CPRI TOOLKIT:

Managing Information Security in Health Care

Table of Contents

Chapter	*Section*	*Title*
Chapter One	1.0	Executive Summary
Chapter Two	2.0	Introduction
	2.1	How to Use This Toolkit
Chapter Three	3.0	Monitoring Laws, Regulations, and Standards
	3.1	Introduction
	3.2	Summary of Proposed DHHS Rules
	3.2.2	Common Elements
	3.2.3.	Proposed Data Security and Electronic Signature Standards
	3.2.4	Electronic Transactions/Code Sets
	3.2.5	Health Care Provider Identifier
	3.2.6	Employer Identifier
	3.2.7	Health Plan Identifier
	3.2.8	Unique Health Identifier-Individuals
	3.3	Final Federal HIPAA Security & Electronic Signature Standard Waiting for Publication
	3.4	Federal Medical Privacy Legislation
	3.4.1	Summary of DHHS Confidentiality Recommendations
	3.4.2	Privacy Notice of Proposed Rule Making Waiting for Publication
	3.5	State Medical Privacy Legislation
	3.6	Setting Standards in Health Care Information
	3.7	JCAHO/NCQA Recommendations for Protecting Personal Health Information
	3.8	Reconciling European and American Approaches to Privacy
Chapter Four	4.0	Developing Policies, Procedures, and Practices
	4.1	Introduction
	4.2	CPRI Guidelines – Information Security Policies
	4.3	Sample Security Policies
	4.3.2.1	Harvard Vanguard Medical Associates
	4.3.2.2	Kaiser Permanente Northern California
	4.3.2.3	Mayo Clinic
	4.3.2.4	Partners Healthcare System
	4.3.2.5	PCASSO, SAIC & UC, San Diego
	4.3.1.6	Project Phoenix, Georgetown University
	4.4	Assigning Roles and Responsibilities
	4.4.1	Introduction

	4.4.2	**CPRI Guidelines for Managing Information Security Programs**
	4.4.3	**Case Study: Immunization Information Systems at University of Pennsylvania**
	4.5	**Health Information Risk Assessment and Management**
	4.5.1	**Case Study: Project Phoenix - Risk Analysis of A Telemedicine System**
	4.5.2	**Case Study: Project Phoenix - Risk Management Plan**
	4.6	**Organizing Security Training**
	4.6.1	**CPRI Guide - Information Security Education**
	4.6.2	**Sample Training Materials**
	4.6.2.1	**Instructor' Guide**
	4.6.2.2	**Slides for Training Program**
	4.6.3	**Conferences on Information Security Training**
	4.7	**Additional Resources**
	4.8	**Enforcing Security Policies**
	4.8.1	**CPRI Sample Confidentiality Statements & Agreement**
	4.8.2	**Case Study: Securing User Agreement at Kaiser Permanente Northern California**
	4.9	**Implementing Information Security Policies**
	4.9.1	**CPRI Guide – Security Features**
	4.9.2	**Special Issues in Electronic Transmission of Confidential Data**
	4.9.2.1	**Fax**
	4.9.2.2	**E-mail**
	4.9.2.3	**HCFA and the Internet**
	4.9.3	**Case Study: PCASSO – Patient Centered Access**
	4.9.4	**Case Study: CHIME PKI**
	4.10	**Business Continuity and Disaster Planning**
Chapter Five	**5.0**	**Enhancing Patient Understanding**
	5.1	**Introduction**
	5.2	**Complying with Consent, Inspection, and Disclosure Requirements**
	5.3	**HelpBot: Complying with Patient Education Requirements**
Chapter Six	**6.0**	**Institutionalizing Responsibility**
	6.1	**Introduction**
	6.2	**Case Study: Trustee/Custodian Agreements at Kaiser Permanente**
Chapter Seven	**7.0**	**Web Sites**
Chapter Eight	**8.0**	**Glossary**
Chapter Nine	**9.0**	**Bibliography**

Toolkit Section 1.0

Chapter One

EXECUTIVE SUMMARY

Introduction

Computer-based patient record systems (CPRS) may potentially achieve greater protection of health information than paper-based records. Ensuring an appropriate and consistent level of information security for computer-based patient records, both within individual health care organizations and throughout the entire health care delivery system, requires organizations entrusted with health care information to establish formal information security programs. Recognizing the importance of information security in managing computer-based patient records, the Computer-based Patient Record Institute (CPRI) chartered the Work Group on Confidentiality, Privacy, and Security to promote this process. Since its inauguration in 1993, the Work Group has developed and published a series of topical guidelines on improving information security for organizations implementing CPRS.

The guideline series addresses individual issues in information security, but, taken as a whole, promotes a comprehensive organizational process. The CPRI believes that managing health care information requires integrating good security processes into the everyday working routines of all staff, not just implementing security measures. Toward that end, the CPRI created a new Task Force to consolidate its guideline series into a toolkit that outlines general principles and provides "best practice" examples of how health care providers should manage the security of their paper and electronic records. The sections of the *CPRI Toolkit* identify key activities that health care providers should initiate as part of managing information security, including:

- Monitoring and adjusting to the changing laws, regulations, and standards
- Developing, implementing, and continuously updating data security policies, procedures, and practices
- Enhancing patient understanding of the organization's information security efforts
- Institutionalizing responsibility for information security

Each section includes an introduction, a copy of the latest edition of the pertinent CPRI guideline, several case studies with sample policies, procedures and forms, and extensive references to print and Internet sources of more information. A consolidated annotated bibliography, a list of Web sites, and a glossary of terms appear at the end of the *CPRI Toolkit*. With this toolkit, any health care provider should be able to plan, implement, and evaluate a security surveillance process scaled to their organizational needs. These resources should aid healthcare organizations in securely managing information, particularly as they develop responses to new federal regulations and laws such as the Health Insurance Portability and Accountability Act of 1996.

Monitoring Changing Laws, Regulations, and Standards

Currently, questions of health information security and medical privacy are of utmost importance in the United States. Hardly a day goes by that *The Washington Post*, *The New York Times*, or *USA Today* do not feature an article about some aspect of medical privacy. Opinion polls document that the American public regards the data management practices of most large organizations with great skepticism. In partial response to these and other expressions of public concern, President Clinton commissioned a task force on medical privacy as part of his health care reform efforts. Although the recommendations of the privacy task force died along with Clinton's plan, federal legislators have incorporated some of their intent, particularly the requirement of federal medical privacy legislation, into subsequent approaches to health care reform. . The Health Insurance Portability and Accountability Act of 1996 (HIPAA))creates specific requirements for the Congress and the Department of Health and Human Services (DHHS). Because of HIPAA, the legal and regulatory environment for managing patient medical records has dramatically changed. DHHS has developed regulations for managing health information security (see below Chapter Three). Efforts to develop federal medical privacy requirements continue in both Congress and DHHS. DHHS led the way on medical privacy by designing model rules to guide Congress and/or its own process of rulemaking if necessary. Meanwhile, many standards-setting organizations are busy addressing the problems of medical privacy and the security of health care information from their own perspectives.

The *CPRI Toolkit* contains summaries of the DHHS rules, the DHHS model medical privacy provisions, information about tracking state laws on medical privacy, and a thorough explanation of the standards-setting process in medical informatics. As an example of how two important standards-setting organizations in health care, the Joint Commission on the Accreditation of Healthcare Organizations and the National Committee on Quality Assurance, are beginning to incorporate demands for adequate data security practices into their evaluation criteria, a copy of the Executive Summary of *Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment* can be found in chapter three of the *CPRI Toolkit*.

Developing Policies, Procedures, and Practices for Information Security

Changes in the regulatory and legal environments, the security risks of distributed networks and systems, ever-changing information technology, and rising patient expectations all require health care organizations to continuously update their data security policies, procedures, and practices. A security team must take primary responsibility for coordinating this effort through careful risk analysis, security policy review, and technical and operational enhancements. The security team's efforts will fail, however, without strong business and clinical leadership from throughout the organization. Even if key leaders accept responsibility for maintaining the confidentiality of patient identifiable information, staff will probably resist taking on new tasks that further complicate their work and compete with current tasks. The security team must recognize that enhancing the organization's security capability requires transforming institutional resistance into a mission-based mobilized security effort. A security team that neglects building support for its efforts risks failure.

Included in the *CPRI Toolkit* are sample documents illustrating approaches to security policies, security risk analyses, patient consent and disclosure documents, and other issues from several organizations including the American Health Information and Management Association, Kaiser Permanente of Northern California, Partner HealthCare System, Inc., Harvard Vanguard Medical Associates, and several NLM-funded sites. These examples should assist any health care program, large or small, in its efforts to enhance the security of its confidential information.

Enhancing Patient Understanding of Information Security Efforts

As the DHHS recommendations on confidentiality make clear, health care providers face new obligations in informing patients about how they manage health information. The DHHS recommendations signal some broad social changes, however, whose significance transcends the narrow legal and regulatory context of their development. Reforms in health care finance (specifically the emergence of managed care) are refocusing some aspects of health care from the doctor-patient relationship to the organization-patient relationship, thus making health care organizations accountable to patients in new ways. In addition to being accountable for health care processes and outcomes, organizations are becoming accountable to patients for their business practices, particularly for what they do with information about their individual cases. These changes, as well as DHHS proposals, will increasingly require health care organizations to obtain new types of consent, provide patients access to information historically reserved for institutional use only, educate patients about their business practices, and extend new services to their patients using electronic media. Patients are also demanding a variety of Internet and web-based healthcare services, including email and access to their medical records. Model examples for how some health care organizations are trying to meet these new obligations are included in the *CPRI Toolkit*.

Institutionalizing Responsibility for Information Security

The well known maxim "Confidentiality is everybody's business" states the basic truth. Transforming this truism into practice requires institutional work and personal commitment. This toolkit provides models and methods for assisting health care providers to manage patient records as a broad institutional process, including the technical protection of the information system. In addition to these concrete methods, however, health care providers should institutionalize a sense of responsibility for maintaining patient confidentiality at all levels, including individual staff, program managers, and organizational administrators. Health care providers should develop methods for binding these levels of responsibility together such as in the illustration of the "Trustee/Custodian Agreements" from Kaiser Permanente explained in the final section of the *CPRI Toolkit*. By creating the trustee/custodian relationship, Kaiser has institutionalized mutual responsibility for secure information control between clinical and information staff, thus integrating it not segregating it from everyday work. Not all health care providers require developing an arrangement as formal as Kaiser's Trustee/Custodian Agreement. Yet, most organizations larger than a single physician office differentiate between clinical and information systems staff. Formulating roles institutionalizing a sense of mutual responsibility for information security among staff operationalizes the idea that confidentiality is everybody's business. Instead of relegating

information security to the domain of the technical specialists and parceling responsibility for managing patients only to clinicians, all staff assumes responsibility for the enterprise, its patients, and the confidentiality of their information.

Chapter Two

INTRODUCTION

Computer-based patient record systems (CPRS) may potentially achieve greater protection of health information than paper-based records. Ensuring an appropriate and consistent level of information security for computer-based patient records, both within individual health care organizations and throughout the entire health care delivery system, requires organizations entrusted with health care information to establish formal information security programs. Recognizing the importance of information security in managing computer-based patient records, the Computer-based Patient Record Institute (CPRI) chartered the Work Group on Confidentiality, Privacy, and Security to promote this process. Since its inauguration in 1993, the Work Group has developed and published a series of topical guidelines on improving information security for organizations implementing CPRS.

The guideline series addresses individual issues in information security, but, taken as a whole, promotes a comprehensive organizational process. The CPRI believes that managing health care information requires integrating good security processes into the everyday working routines of all staff, not just implementing security measures. Toward that end, the CPRI charged the Work Group to consolidate its guideline series into a toolkit that outlines general principles and provides "best practice" examples of how health care providers should manage the security of their paper and electronic records. The sections of the CPRI Toolkit identify key activities that health care providers should initiate as part of managing information security, including:

Monitoring and adjusting to the changing laws, regulations, and standards
Developing, implementing, and continuously updating data security policies, procedures, and practices
Enhancing patient understanding of the organization's information security efforts
Institutionalizing responsibility for information security

Each section includes an introduction, a copy of the latest edition of the pertinent CPRI guideline, several case studies with sample policies, procedures and forms, and extensive references to print and Internet sources of more information. A consolidated annotated bibliography, a list of Web sites, and a glossary of terms appear at the end of the CPRI Toolkit. With this toolkit, any health care provider should be able to plan, implement, and evaluate a security surveillance process scaled to their organizational needs.

The legal, social, and technical environment surrounding CPRS will remain dynamic, thus requiring all health care providers to be vigilant in the years to come. The CPRI has designed this toolkit to assist health care providers in adapting to the changing circumstances affecting management of information security. The CPRI Toolkit contains examples of "best practices,"." but health care providers should consult with their legal departments and assess their own situations before adopting any forms, policies, or procedures contained in the CPRI Toolkit.

How to Use the CPRI Toolkit

Healthcare organizations will find valuable resources in the *CPRI Toolkit* to assist in managing the security of business, clinical and other types of health information, particularly in computer-based record systems. The *CPRI Toolkit* includes guiding principles, case studies and paradigmatic examples of how to build a health information security program, including "hot links" over the World Wide Web to important sites. New regulations on the security of computer-based health information promulgated by the Department of Health and Human Services subsequent to the Health Insurance Portability and Accountability Act of 1996 make accomplishing this task salient and necessary for all healthcare providers, payers and clearinghouses. In order to keep faith with and maintain the trust of patients, clinical and business partners and the general public, nonetheless, healthcare organizations should seek capably to assure the confidentiality, integrity and secure accessibility of their information as a matter of basic business practice. Assuring information security has the reputation of being a highly esoteric technical enterprise. The *CPRI Toolkit* makes the case that maintaining information security should be an aspect of the everyday work of all members of the organization (including its customers), not just of "security specialists" or information technologists alone. The *CPRI Toolkit* offers guidance in accomplishing three basic security program functions, namely:

1) Monitoring changing laws, rules and regulations;
2) Updating information security policies, procedures and practices, and;
3) Enhancing patient understanding and acceptance.

By accomplishing these functions healthcare organizations potentially institutionalize a sense of responsibility for information security throughout their operations thus building the foundations of a competent, defensible information assurance program.

To take best advantage of the resources contained in the *CPRI Toolkit*, healthcare organizations should develop and sustain a security surveillance process that typically includes the following critical steps:

1) Assigning responsibility for managing information security;
2) Developing and implementing a plan for managing risks to the confidentiality, integrity and secure accessibility of an organization's information;
3) Measuring and documenting the impact of administrative and technical countermeasures taken in execution of the information security plan, and;
4) Reevaluating and adapting the plan in light of experience.

As implied by the feedback loop linking experience to the original plan, the security surveillance process never ends but should occur as part of a healthcare organization's regular administrative operations. Such a broad-based, recurrent approach will build administrative support for and enterprise-wide awareness of the importance of information assurance – both of which will be necessary to meet the deadline for implementation of the HIPAA security regulations in early 2002. This approach also shares with the HIPAA regulations a strategy of health information security based on risk

management, not risk avoidance. It thereby should help healthcare organizations comply with HIPAA as it enhances their overall competence in health information assurance.

The organization of the *CPRI Toolkit* encourages healthcare organizations to keep their eyes focused on three broad security functions: monitoring their federal, state and professional regulatory and legal environment, updating their own internal environment of policies, procedures and practices, and communicating with their patients. As healthcare organizations work their way through the critical steps of the security surveillance process, they will find resources in the *CPRI Toolkit* linking the process to these three broad functions. The resources come in several forms.

1) Monitoring Laws, Regulations and Standards: Chapter 3 devotes great attention to the extensive HIPAA-provoked federal activity in health information security and provides extensive materials about state and professional activities in health information assurance. This chapter includes summaries of all the HIPAA electronic transaction and data security regulations and of the Notice of Proposed Rulemaking on medical privacy. A special matrix creates "hot links" between the HIPPA requirements and pertinent sections of the *CPRI Toolkit.* A section on state law includes information on how to investigate legislative action in all fifty states as well as a recent evaluation of the state scene prepared by the Georgetown University Health Privacy Project. The Executive Summary of the JCAHO/NCQA Recommendations for Protecting Personal Health Information is republished with permission in recognition of the central role of these two accrediting bodies for healthcare providers. Finally, DHHS and professional information security specialists regularly refer to and depend upon the work of a range of standards setting organizations, a realm that often remains somewhat obscure to many healthcare professionals. In order to demystify and recognize the importance of standards setting organizations, the editors of *CPRI Toolkit* asked Margaret Amatayakul, former executive director of the CPRI, to write an introduction to setting standards in health care information. Using the resources in this section of the *CPRI Toolkit*, any healthcare organization ought to be able to discover and track the various federal, state, and professional requirements in health information security and privacy to which they must comply. HIPAA gives this section special salience now; but, monitoring laws, regulations and standards for healthcare constitutes work that never ends for healthcare organizations in this and all aspects of their operation.

2) Updating health information policies, procedures and practices: Since its inception in 1993, the CPRI Work Group on Confidentiality, Privacy and Security has published booklets on specific topics in health information security. Each booklet is reprinted in Chapter 4 accompanied by samples and case studies illustrating the critical steps healthcare organizations should take to plan and implement a health information security program. Sample security policies illustrate how eight different healthcare organizations of varying scale have addressed the issues discussed in "CPRI Guidelines for Information Security Policies." Section 4.5 contains an introduction to information security risk assessment and a case study on telemedicine from Georgetown University Medical Center. To learn about "Assigning Roles and Responsibilities" in health information security, consult section 4.4 with the reprinted "CPRI Guidelines for Managing Information Security Programs" and a case study from the University of Pennsylvania. A comprehensive information security training course complete with

"Instructor's Guide", all necessary slides, and pre and posttests accompanies the "CPRI Guide to Information Security Training". Information about organizations that sponsor regular training in information security training and references to other resources complete the section. To learn about how organizations enforce security policies, consult section 4.8, which contains sample confidentiality statements/agreements and a case study on securing user agreement at Kaiser Permanente Northern California. A special section focuses on issues in the electronic transmission of health information such as email, fax and the Internet. HCFA's new Internet Policy appears accompanied by a discussion of PCASSO, an NLM-sponsored project giving patients and providers secure remote access to computer-based patient records at the University of California San Diego Medical Center. This includes discussion of certain information security technologies such as firewalls and encryption.

3) Enhancing patient understanding of an organization's health information security program. In the new millennium, patients will hold healthcare organizations accountable for many aspects of their business practice as well as medical care. As this second edition of the *CPRI Toolkit* goes to press, Congress is debating Patients' Bill of Right legislation to permit suit of managed care companies for denial of service and other business practices. Such bills and supporting anecdotes provide some evidence of public dissatisfaction with the consequences of reforms in healthcare finance during the last decade. Demands for greater accountability in the use of personally identifiable health information reflect distrust of complex organizations and their power over the lives of individuals. The DHHS suggests that federal medical privacy laws or regulations include requiring healthcare organizations to give patients the right to review and propose corrections to their medical record as well as document and permit patients to review lists of disclosures. Chapter 5 of the *CPRI Toolkit* includes procedures and forms from AHIMA illustrating how healthcare organizations might responsibly provide these services. Healthcare providers might actually go one step farther and use the public's concern about medical security and privacy to build trust. Chapter 5 includes a discussion of "HelpBot", Georgetown University Medical Center's web-based explanation of its efforts to assure the confidentiality, integrity and secure accessibility of patient information in telemedicine. Instructions for tailoring "HelpBot" to an organization's own needs are included.

Institutionalizing sound security practices requires creating sustaining structures at all levels of the organization. Security seminars routinely repeat two basic truisms: 1) the CEO should publicly support an organization's information security program, and 2) confidentiality is everybody's business. Questions about how to integrate information security into an organization's life less frequently get posed. Of particular concern is the tendency to isolate information security from clinical and business operations. Through an arrangement called "Trustee-Custodian Agreements" Kaiser Permanente has developed a means of tightly sharing responsibility for information security between information specialists and clinical and business users. Chapter 6 includes a detailed discussion of the process and sample agreement forms.

The *CPRI Toolkit* offers a gateway into thinking about managing information security in healthcare. Because this second edition exists "on the web" as well as on

paper, it literally functions as a means of finding resources beyond its own boundaries. To assist users in this task, Chapter 7 lists all the addresses of references to sites and information on the World Wide Web with activated “hot links”. Chapter 8 includes a glossary of terms updated from the previously published CPRI “Glossary” and a web link to the HIPAA glossary. Chapter 9 lists important references in the field of health information security.

The *CPRI Toolkit* does not contain recipes for compliance with HIPAA or a foolproof security system. Like the very best cookbooks, however, it includes extensive review of policies (what is wanted), procedures (how to do what is wanted) and practices (what actually gets done) which, when thoughtfully deployed, give evidence of due diligence and yield an administratively disciplined, defensible program. Nor will technology alone yield a responsible program. Each healthcare organization must blend technology with policies, procedures and practices to create a mix consistent with its own mission and business philosophy. Information security management in healthcare as elsewhere requires managing risks that cannot be avoided as long as one remains in business. Managing risks requires exercising administrative judgement. The editors of the *CPRI Toolkit* hope that this document will enhance the ability of all healthcare professionals to exercise competent administrative judgement as we work to better the health of our patients, enrich the working lives of our staff and protect our organizations.

In recognition of the projected long term development of the *CPRI Toolkit*, the CPRI created a committee to oversee its content. Its members include the following individuals:

Ted Cooper, MD, Task Force Chair
National Director of Confidentiality and Security
Kaiser Permanente

Jeff Collmann, Ph.D., Editor
Department of Radiology
Georgetown University Medical Center

Barbara Demster, MS, RRA
Comliance Officer
Healtheon Corporation

Kathleen Frawley, J.D.
American Health Information Management Association

Shonna Koss
IBM

Renee Ornes
Webmaster
3Com Healthcare Corporation

Bruce W. Patterson
Director, Healthcare Industry
3Com Healthcare Corporation

Paul Schyve, M.D.
Joint Commission for the Accreditation of Healthcare Organizations

The following members of the Confidentiality and Security Program Task Force, Computer-based Patient Record Institute prepared the first edition of the CPRI Toolkit.

Ted Cooper, MD, Task Force Chair
National Director of Confidentiality and Security
Kaiser Permanente

Jeff Collmann, Ph.D., Editor
Department of Radiology
Georgetown University Medical Center

Barbara Demster, MS, RRA
Health Information Manager

Healtheon Corporation

Keith MacDonald
First Consulting Group

Susan K. Odneal, CISSP
Kaiser Permanente Information Technology

Jeanne Reiners
Information Services
Baptist Healthcare System

The editors also want to recognize and thank the members of the CPRI Work group on Confidentiality, Privacy and Security who prepared the many previously published guideline books that are republished in the *CPRI Toolkit.*

Kathleen Frawley, J.D., Co-chairperson

Dale W. Miller, Co-chairperson

Kenneth Kung, Team Leader, Information Security Management

Carol A. Romano, Ph.D., R.N., F.A.A.N, Team Leader, Information Security Education

Cindy Beery, Team Leader, Model Confidentiality Agreements

Cynthia Miller, Team Leader, Security Features

The CPRI would like to thank the following organizations, investigators, and projects for permission to use or site examples from their work.

Noam H. Artzt, Ph.D., All Kids Count and Leonard Davis Institute of Health Economics, University of Pennsylvania, Philadelphia, Pennsylvania for "Information Security and Immunization Information System."

Dixie B. Baker, Ph.D., Principal Investigator, PCASSO, Science Applications International Corporation (SAIC), San Diego, California for information security policies from PCASSO.

Christopher Chute, M.D., DrPH, Mayo Foundation, Rochester, Minnesota for information security policies from Mayo Clinic.

David Cochran, M.D., Harvard Pilgrim Healthcare and Richard Lopez, M.D., Harvard Vanguard Medical Associates, Brookline, Massachusetts for patient confidentiality policies of Harvard Vanguard Medical Associates

Janlori Goldman, J.D., Health Privacy Project, Georgetown University, Washington, D.C. for executive summary of report on state privacy laws.

Karen Gallagher Grant, R.R.A., Partners Healthcare System, Boston, Massachusetts for information security policies of PartnersS Healthcare Systems, Inc.

The Joint Commission on Accreditation of Healthcare Organizations and the National Committee for Quality Assurance for permission to reprint the executive summary of "Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment."

Linda L. Kloss, R.R.A., Executive Vice President and CEO, American Health Information Management Association, Washington, D.C. for permission to reprint AHIMA's forms.

Seong K. Mun, Ph.D., Principal Investigator, Project Phoenix: telemedicine in hemodialysis, Georgetown University Medical Center, Washington, D.C., for documents from security program of Project Phoenix.

The editors will wish to offer special thanks to the following individuals who prepared new documents for inclusion in the CPRI Toolkit.

Margret Amatayakul, MBA, RRA for "Standards, Processes and Organizations: Developing Standards in Health Care Information Security"."

Dixie B. Baker, Ph.D., Principal Investigator, PCASSO, Science Applications International Corporation (SAIC), San Diego, California for summary of PCASSO Project.

The editors wish to thank the following colleagues without whom neither the *CPRI Toolkit* nor the work on information security in health care would have been possible.

Arwa Al-Ama, George Washington University, Washington, D.C.
Maj. Catherine Beck, TATRC, U.S. Army Medical Research and Materiel Command, Ft. Detrick, Maryland
Glenn C. Graber, University of Tennessee, Knoxville, Tennessee
Lance Hoffman, Ph.D. George Washington University, Washington, D.C.
Anya Kim, George Washington University, Washington, D.C.
Marion C. Meissner, DynCorp I&E, Fairlakes, Virginia
Anna-Lisa Silvestre, Kaiser Permanente, Oakland, California
Willie E. Wright, SRA International, Inc., Fairlakes, Virginia

The National Library of Medicine and the Department of Defense supported some Projects referenced in the *CPRI Toolkit*. Opinions, interpretations, conclusions and recommendations are those of the authors and are not necessarily endorsed by the National Library of Medicine or the Department of Defense.

The editors offer special thanks to Janice Kennedy, Executive Director of Computer-based Patient Record Institute, for shepherding the CPRI Toolkit through the final, onerous stages of editing, printing, and preparation for distribution. Without her patience and sense of detail, the Toolkit would not have ever been completed.

Chapter Three

Toolkit Section 3.0

MONITORING CHANGING LAWS, REGULATIONS, AND STANDARDS

Toolkit Section 3.1

Introduction

Currently, questions of health information security and medical privacy are of utmost importance in the United States. Hardly a day goes by that *The Washington Post*, *The New York Times*, or *USA Today* do not feature an article about some aspect of medical privacy. Opinion polls document that the American public regards the data management practices of most large organizations with great skepticism. In partial response to these and other expressions of public concern, President Clinton commissioned a task force on medical privacy as part of his health care reform efforts. Although the recommendations of the privacy task force died along with Clinton's plan, Federal legislators have incorporated some of their intent, particularly the requirement of Federal medical privacy legislation, into the piecemeal approach to health care reform developed during the last three years. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) creates specific requirements for the Congress and the Department of Health and Human Services (DHHS). Because of HIPAA, the legal and regulatory environment for managing patient medical records has dramatically changed. . DHHA has developed regulations for managing health information security. Efforts to develop federal medical privacy requirements continue in both Congress and DHHS. DHHS led the way by designing model rules to guide Congress and/or implement the laws it passes. Moreover, many standards-setting organizations have been busy addressing the problems of medical privacy and the security of health care information from their own perspectives.

The *CPRI Toolkit* contains summaries of the proposed DHHS rules, the DHHS model medical privacy provisions, information about State laws on medical privacy, and a thorough explanation of the standards-setting process in medical informatics. As an example of how two important standards-setting organizations in health care, the Joint Commission on the Accreditation of Healthcare Organizations and the National Committee on Quality Assurance, are beginning to incorporate demands for adequate data security practices into their evaluation criteria, a copy of the Executive Summary of *Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment* completes this chapter of the *CPRI Toolkit*.

Toolkit Section 3.2

Summary of Proposed DHHS Rules and Regulations

Under the rubric of "Administrative Simplification," HIPAA requires Congress to pass laws that "improve… the efficiency and effectiveness of the health care system by encouraging the establishment of standards and requirements for the electronic transfer of certain health care information" (PL No. 104-191). In sections 261 through 264, HIPAA calls for standards and laws for two circumstances, namely 1) the electronic interchange of financial and administrative data between health plans, health care clearinghouses, and health care providers, and 2) maintaining the privacy of individually identifiable medical information. HIPAA also establishes a timetable by which Congress and DHHS must act. The timeline can be seen in the table below.

The HIPAA Timetable – Enacted

Date	Scheduled Release
August 21, 1996	HIPAA enacted
July 31, 1997	DHHS recommendations on confidentiality
February 28, 1998	DHHS draft transaction standards
August 21, 1999	Deadline for Federal privacy legislation

Under the direction of the National Committee on Vital and Health Statistics, the Healthcare Finance Administration (HCFA) leads the DHHS effort to draft transaction and model privacy standards. HIPAA establishes an aggressive timetable for DHHS to draft, release for comment, and recommend for adoption such a complex, extensive, and important set of regulations. Although currently behind schedule, DHHS is making progress. New regulations are regularly released for comment in the Federal Register. The timetable can be seen in the table below.

The HIPAA Timetable as of February 1, 1999

Date	Actual Release
August 21, 1996	HIPAA
Sept 11, 1997	Released: Confidentiality recommendations
July 6, 1998	Comment Period Closed: Provider Identifier
July 6, 1998	Comment Period Closed: Transaction Standards
July 6, 1998	Comment Period Closed: Code Set Standards
June 16, 1998	NPRM: Employer Identifier
July 6, 1998	White Paper: Unique Health Identifier – Individuals
October 13, 1998	Comment Period Closed: Security Standards
Pending	NPRM: Identifier-Health Plans

Summaries of the proposed DHHS rules follow. To view the text of these recommendations and the existing draft regulations for electronic transactions, please consult the DHHS Web site, http://aspe.os.dhhs.gov/admnsimp/ You may also enroll to receive e-mail notice of newly posted draft regulations and comment on the proposed rules through this same Web site.

Toolkit Section 3.2.2

Common Elements of All Proposed Standards

Standard Definitions for All Proposed Rules

A common set of definitions exists for all rules so far released.

1. **Health care clearinghouse:** a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard elements. Such an entity receives health care transactions from health care providers and other entities, translates the data from a given format into one acceptable to the intended recipient, and forwards the processed transaction to appropriate health plans and other health care clearinghouses for further action, as necessary.

2. **Health care provider:** a provider of medical or other health services and those entities that furnish or bill and are paid for health care services in the normal course of business.

3. **Health information:** any information, whether oral or recorded in any form or medium, that
   a. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
   b. Relates to the past, present, or future physical or mental health of condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

4. **Health plan:** an individual or group health plan that provides, or pays the cost of, medical care
   a. Including group health plans, health insurance issuers, health maintenance organizations, Part A or Part B of Medicare Act, Medicaid, Medicare supplemental policies, long term care policies, employee welfare plans that provide health benefits, the health plan for active military personnel, the veterans health plan, CHAMPUS, the Indian Health Service, the Federal Employees Health Benefits Program, and other plans as designated by the Secretary of DHHS; but
   b. Not including plans such as property and casualty insurance plans or workers compensation plans.

5. **Medical care:** the diagnosis, cure, mitigation, treatment, or prevention of disease or amounts paid for the purpose of affecting any body structure or function of the body; amounts paid for transportation primarily for and essential to these items; and amounts paid for insurance covering the items and the transportation specified in this definition.

6. **Participant:** any employee or former employee of an employer, or any member or former member of an employee organization, who is or may become eligible to receive a benefit of any type or from an employee benefit plan that covers employees of such an employer or members of such organizations, or whose beneficiaries may be eligible any such benefits, including an individual treated as an employee under section 401 (c)(1) of the IRS code.

7. **Small health plan:** a group health plan with fewer than 50 participants.

8. **Standard:** a set of rules for a set of codes, data elements, transactions, or identifiers promulgated either by an organization accredited by the American National Standards Institute (ANSI) or the Department of Health and Human Services (DHHS) for the electronic transmission of health information.

9. **Transaction:** the exchange of information between two parties to carry out financial and administrative activities related to health care.

Implementation Requirements for all Standards

DHHS proposes a common set of implementation requirements for all HIPAA relevant standards and rules. All health care plans and clearinghouse, except small health plans, must implement the standards and code sets within 24 months of their enactment. Small health care plans must adopt the standards within 36 months of enactment. (Only health care providers that transmit health information in the electronic form covered in the rules must implement the rules. Such health care providers must implement the rules within 24 months of enactment.) Once the rules are adopted, health plans may not delay or refuse to process claims submitted in the standardized format. Civil monetary penalties are proposed for violations of the rules. The DHHS rules will supersede any State law contrary to their requirements except where specifically waived. Financial institutions (such as credit card companies) or their agents may but are not required to comply with the rules. For more details on alternatives to the recommendations and the process whereby DHHS developed its proposals, please consult the Federal Register for each proposed set of rules. You may gain access to these documents, by consulting the Administrative Simplification Web site (http://aspe.os.dhhs.gov/admnsimp). (

Penalties for Violations of the Proposed Rules

The Social Security Act establishes a civil monetary penalty for violation of the provisions under which the proposed rules would enter, subject to several limitations. Penalties may not be more than $100 per person per violation and not more than $25,000 per person for violations of a single standard for a calendar year. The procedural provisions in the section of the Act, "Civil Monetary Penalties," are applicable. The Act establishes penalties for a knowing misuse of unique health identifiers and individually identifiable health information: 1) a fine of not more than $50,000 and/or imprisonment of not more than 1 year; 2) if misuse is "under false pretenses," a fine of not more than $100,000 and/or imprisonment of not more than 5 years; and 3) if misuse is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10 years. These penalties do not affect any other penalties that may be imposed by other Federal programs, including ERISA. Under section 1178 of the Act, the provisions of part C of title XI of the Act, as well as any standards established under them, supersede any State law that is contrary to them. However, the Secretary may, for statutorily specified reasons, waive this provision.

Proposed Standards for Data Security and Electronic Signature

Toolkit Section 3.2.3

The DHHS makes general changes in the data security standards that broaden the scope and impact from earlier regulations. The transaction standards apply to electronic transactions between organizations, thus leaving health care providers who do not use electronic transmission media unaffected. In contrast, individualized health information becomes subject to the new rules when it is electronically stored, maintained or transmitted; exists in any format (standard transaction or proprietary); and communicated either internally or externally to a corporate entity. A health care provider who stores patient data on magnetic tape, for example, but sends paper documents to a health plan must comply with the data security rules but is not required to comply with the electronic transaction rules. As with the transaction rules, the data security rules apply to health information on any electronic media except telephone voice and faxback systems.

The proposed rules also address electronic signatures. Although DHHS does not recommend requiring electronic signatures at this time, they specify mandatory rules for implementing an electronic signature if an organization so chooses. Use of this standard would satisfy any Federal or State requirement for a signature, either electronic or on paper.

DHHS firmly places responsibility for determining implementation of specific data security measures with health care providers, plans, and clearinghouses. DHHS defines a standard as "a set of requirements with implementation features that providers, plans, and clearinghouses must include in their operations to assure that electronic health information pertaining to individuals remains secure" (Federal Register, August 12, 1998, p. 43249; see http://erm.aspe.hhs.gov/secnprm). The standard does not require or reference specific technological solutions or address the extent to which a particular entity should implement specific features. The standard does require each affected entity to assess its own security risks and develop methods to manage them. The proposal emphasizes many times that providers, plans, and clearinghouses must create and keep current detailed documentation of their data security assessments, plans, policies, and procedures. The people responsible for maintaining data security should have ready access to the documentation.

For presentation purposes, DHHS groups the security requirements into four categories - administrative procedures, physical safeguards, technical security services, and technical security mechanism. DHHS requires only that the security measures be taken, not necessarily organized according to their groups. A general description and matrix enumerating the requirements and implementation features of each grouping follow.

<u>Administrative Procedures</u>

Administrative procedures to guard data integrity, confidentiality, and availability are documented, formal practices used to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data. Administrative procedures can be seen in the table below.

Administrative Procedures to Protect Data

Requirement	Implementation
Certification	
Chain of trust partner agreement	
Contingency plan *(all listed implementation features must be implemented)*	Applications and data criticality analysis. Data backup plan. Disaster recovery plan. Emergency mode operation plan. Testing and revision.
Formal mechanism for processing records	
Information access control *(all listed implementation features must be implemented)*	Access authorization. Access establishment. Access modification.
Internal audit	
Personnel security *(all listed implementation features must be implemented)*	Assure supervision of maintenance personnel by authorized, knowledgeable person. Maintenance of record of access authorizations. Operating, and in some cases, maintenance personnel have proper access authorization. Personnel clearance procedure. Personnel security policy/procedure. System users, including maintenance personnel, trained in security.
Security configuration management *(all listed implementation features must be implemented)*	Documentation. Hardware/software installation and maintenance review and testing for security features. Inventory. Security Testing. Virus checking.
Security incident procedures *(all listed implementation features must be implemented)*	Report procedures. Response procedures.
Security management process *(all listed implementation features must be implemented)*	Risk analysis. Risk management. Sanction policy. Security policy.
Termination procedures *(all listed implementation features must be implemented)*	Combination locks changed. Removal from access lists. Removal of user account(s). Turn in keys, token, or cards that allow access.
Training *(all listed implementation features must be implemented)*	Awareness training for all personnel (including management). Periodic security reminders. User education concerning virus protection. User education in importance of monitoring log in success/failure and how to report discrepancies. User education in password management.

Physical Safeguards

Physical safeguards to guard data integrity, confidentiality, and availability relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities. Physical safeguards can be seen in the table below.

Physical Safeguards to Protect Data

Requirement	Implementation
Assigned security responsibility	
Media controls *(All listed implementation features must be implemented.)*	Access control. Accountability (tracking mechanism). Data backup. Data storage. Disposal.
Physical access controls (limited access) *(All listed implementation features must be implemented.)*	Disaster recovery. Emergency mode operation. Equipment control (into and out of site). Facility security plan. Procedures for verifying access authorizations prior to physical access. Maintenance records. Need-to-know procedures for personnel access. Sign-in for visitors and escort, if appropriate. Testing and revision.
Policy/guideline on work station use	
Secure workstation location	
Security awareness training	

Technical Security Services

Technical security services to guard data integrity, confidentiality, and availability include the processes that are put in place to protect and to control and monitor information access. Technical Security Services can be seen in the table below.

Technical Security Services to Protect Data

Requirement	Implementation
Access control *(The following implementation feature must be implemented: procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: context-based access, role-based access, user-based access. The use of Encryption is optional.)*	Context-based access. Encryption. Procedure for emergency access. Role-based access. User-based access.
Audit controls	
Authorization control *(At least one of the listed implementation features must be implemented.)*	Role-based access. User-based access.
Data Authentication	
Entity authentication *(The following implementation features must be implemented: automatic logoff, unique user identification. In addition, at least one of the other listed implementation features must be implemented.)*	Automatic logoff. Biometric. Password. PIN. Telephone callback. Token. Unique user identification.

Technical Security Mechanisms

Technical security mechanisms include the processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network.

Technical Security Mechanisms to Protect Data

Requirement	Implementation
Communications/network controls *(If communications or networking is employed, the following implementation features must be implemented: integrity controls, message authentication. In addition, one of the following implementation features must be implemented: access controls, encryption. In addition, if using a network, the following four implementation features must be implemented: alarm, audit trail, entity authentication, event reporting.)*	Access controls. Alarm. Audit trail. Encryption. Entity authentication. Event reporting. Integrity controls. Message authentication.

The Electronic Signature Standard

In the electronic environment, the same legal weight associated with an original signature on a paper document may be needed for electronic data. Use of an electronic

signature refers to the act of attaching a signature by electronic means. DHHS requires electronic signatures to include certain implementation features, specifically:

- Message integrity
- Nonrepudiation
- User authentication

No technically mature techniques provide the security service of non-repudiation in an open network environment, in the absence of trusted third parties, other than digital signature-based techniques. If electronic signatures are employed, DHHS requires that digital signature technology be used. The requirements of the electronic signature standard are defined in the table below.

Electronic Signature Standard Requirements

Requirement	Implementation
Digital signature *(If digital signature is employed, the following three implementation features must be implemented: message integrity, non-repudiation, user authentication. Other implementation features are optional.)*	Ability to add attributes. Continuity of signature capability. Counter signatures. Independent verifiability. Interoperability. Message integrity. Multiple signatures. Non-repudiation. Transportability. User authentication.

Toolkit Section 3.2.4

Proposed Standards for Electronic Transactions and Code Sets

Standardizing the form and code sets of electronic transactions between health care providers, plans, and clearinghouses constitutes a major goal of the Administrative Simplification section of HIPAA. HIPAA requires DHHS to evaluate existing standards, consult with relevant constituencies about their recommendations, and propose rules to impose a uniform set of transaction forms and code sets for use in electronic data interchange. DHHS proposed standards for and the code sets to be used in eight types of transactions, including:

1. Health claims or equivalent encounter information
2. Health care payment and remittance advice
3. Coordination of benefits
4. Health claim status
5. Enrollment and disenrollment in a health plan
6. Eligibility for a health plan
7. Health plan premium payments
8. Referral certification and authorization

Standards for first report of injury and health claim attachments will be treated in the future. The Secretary of DHHS may also adopt standards for other types of transactions as deemed necessary.

The rules apply to health plans and health care clearinghouses for all designated transactions. Health plans that use agents to process their transaction must assure their agents also follow the rules. Transactions within a corporate entity are not subject to the rules. The rules apply to health care providers only when transmitting health information in electronic form in connection with transactions covered under the rules. Health care providers may send and clearinghouses may accept nonstandard data for the sole purpose of having the clearinghouse translate the data into standard form. Electronic transmissions include all media such as magnetic tapes or disks physically transported from one location to another as well as electronic transmission media such as the Internet, dialup lines, and private networks. If adopted, the standards would become part 142 of title 45 of the Code of Federal Regulations entitled "Administrative Requirements."

The table below lists the proposed standards for each type of transaction. "ASC X12N" standards refer to version 4010 of standards developed by the subcommittee of the ANSI X12 Accredited Standards Committee (ASC) for electronic standards in the insurance industry, including health insurance. "NCPDP" refers to the National Council of Prescription Drug Programs Telecommunication Claim version 3.2 or equivalent Batch Standard Version 1. For more details, consult the Federal Register at the Administrative Simplification Web site (http://aspe.os.dhhs.gov/admnsimp). (

Proposed Standards for Electronic Health Transactions

Transaction Type	Transaction Subtype	Standard
Health care claim		
	Retail drug	NCPDP
	Dental claim	ASC X12N 837: Dental
	Professional claim	ASC X12N 837: Professional
	Institutional claim	ASC X12N 837: Institutional
Health care payment		ASC X12N 835: Payment/Advice
Benefit coordination		
	Retail drug	NCPDP
	Dental claim	ASC X12N 837: Dental
	Professional claim	ASC X12N 837: Professional
	Institutional claim	ASC X12N 837: Institutional
Health claim status		ASC X12N 276/277
Plan enroll/disenroll		ASC C12 834
Plan eligibility		ASC X12 270/271
Plan premium payments		ASC X12 820
Referral cert/auth		ASC X12N 278

Implementation guides for the NCPDP Telecommunication Standard Format Version 3.2 and the Batch Standard Version 1.0 are available from the National Council for Prescription Drug Program, 4201 North 24th Street, Suite 365, Phoenix, Arizona 85016. You may contact them by telephone at (602) 957-9105, by fax at (602) 955-0749, or through their Web site at http://www.ncpdp.org.

Implementation guides for the ASC X12N standards are available from Washington Publishing Company, 806 W. Diamond Ane, Suite 400, Gaithersburg, Maryland, 20878. You may contact them by telephone at (301) 590-9337, by fax at (301) 869-9460, or through their Web site at http://www.wpc-edi.com/HIPAAa/.

The table below lists recommended code sets for different types of medical data. "ICD-9-CM" refers to the International Classification of Diseases, 9th edition, Clinical Modification as maintained and distributed by the National Center for Health Statistics, CDC, DHHS. CPT refers to the Current Procedural Terminology as maintained and distributed by the American Medical Association. "CDT" refers to the Current Dental terminology maintained and distributed by the American Dental Association. "NDC" refers to the National Drug Code maintained and distributed by the Food and Drug Administration. HCPCS refers to the Health Care Financing Administration Procedure Coding System (levels 1, 2, and 3) as maintained and distributed by the Health Care Financing Administration, DHHS. The proposal requires modifications to the current HCPCS, including eliminating the CDT from level 1 and developing a national process for reviewing and approving health insurer codes currently met by local codes in level 3.

Toolkit Section 3.2.5

Proposed National Standard for Health Care Provider Identifier

Medical Data Types	Medical Data Subtypes	Recommended Code Set
Diseases and causes of injury		ICD-9-CM, Vol 1 & 2
Procedures		
	Physician services	CPT
	Dental services	CDT
	Inpatient hospital services	ICD-9-CM, Vol 3
Other health-related services		Modified HCPCS
Drugs		NDC
Other substances and equipment		Modified HCPCS

Proposed National Standard for Health Care Provider Identifier

HIPAA mandates developing a single, national provider identifier for use in all electronic transactions as a major element in its administrative simplification effort. DHHS proposes adopting the National Provider Identifier (NPI) as the standard in conjunction with a central electronic enumeration method to be designated the National Provider System (NPS).

The NPI includes the following characteristics:

- ASC X12N compliant
- Eighth-position alphanumeric identifier
- Eighth-position functions as a check digit following the ISO standard
- Intelligence free(that is, identifier contains no empirical signifiers subject to change)
- Universal identifier for use in all health care transactions
- Under final testing for use in HCFA transactions
- Not proprietary
- Widely available to health care industry
- Maintained by HCFA
- Safeguarded under Federal Privacy Act
- Supports approximately 20 billion unique identifiers

DHHS discusses two options for enumerating providers, that is, assigning them NPI. Option 1 creates a new Federally-directed registry for enumerating all providers. Option 2 designates a combination of Federal programs named as health plans, Medicaid State agencies, and a Federally directed registry. DHHS recommends Option 2 for financial reasons. Although less centralized, Option 2 would cost less because 85% of providers already participate in Federal or State health plans. Enrollment and enumeration can thus be accomplished in the same process. The enumeration process would begin with providers participating in Medicare followed by Medicaid and non-Medicare Federal health plans. If providers conduct business with more than one Federal or State health plan, they may select any one for enumeration. The Federal registry would enumerate only those providers who do not conduct business with Federal or State health plans. DHHS expects this phase of the enumeration process to require two years. The NPS would extend NPI to providers who do not conduct any business using electronic transactions only after enumerating all other providers and identifying funds to support the process.

DHHS proposes creating two levels of access to information about providers in the National Provider database. Level I grants enumerators only access to all the information. Level 2 grants access to selected data elements to the general public. For the details of restricted and unrestricted data elements, please consult Federal Register, Vol. 63, No.88, Thursday, May 7, 1998, page 25338 using the Administrative Simplification Web site, (http://aspe.os.dhhs.gov/admnsimp) . You may also consult the same location (pages 25340-54) for a detailed analysis of financial and administrative impacts of the NPI.

Toolkit Section 3.2.6

Proposed National Standard for Employer Identifier

HIPAA mandates developing a single employer identifier for use in all electronic transactions as a major element in the administrative simplification effort. DHHS proposes adopting as the standard the Employer Identifier Number (EIN) assigned by the Internal Revenue Service and as defined in the Code of Federal Regulations. The EIN is the taxpayer identifying number of an individual or other person (whether or not an employer) that is assigned pursuant to 26 U.S.C. 60011 (b) or corresponding provisions of prior law, or pursuant to 26 U.S.C. 6109, and in which nine digits are separated by a hyphen, as follows: 00-0000000.

Toolkit Section 3.2.7

Proposed National Standard for Health Plan Identifier

(Notice of Proposed Rule Making pending.)

Toolkit Section 3.2.8

Proposed Unique Health Identifier for Individuals

Although the DHHS has not released a Notice of Proposed Rule Making for the Unique Health Identifier for Individuals (UHI), a White Paper exists outlining the various options currently under consideration including strengths, weaknesses, supporters, and cost. You may consult the White Paper using the Administrative Simplification Web site, http://aspe.os.dhhs.gov/admnsimp/nprm/noiwp1.htm. Opposition to the implementation of a UHI has emerged from many quarters thus encouraging officials to delay action.

Toolkit Section 3.3

(Waiting for Final Security and Electionic Signature Standard)

Toolkit Section 3.4

Federal Medical Privacy Legislation

Information on Federal Legislation on Medical Privacy

HIPAA requires the passage of Federal medical privacy legislation by August 21, 1999. Several legislators including Senator Leahy and Congressman McDermott have introduced bills but none has yet passed. To consult the text and follow the legislative status of each bill, go to the Federal legislation Web site, http://thomas.loc.gov and search on "medical privacy." The American Health Information and Management Association (AHIMA) maintains a Web site that tracks the progress of Federal privacy bills at http://www.ahima.org. For more information and summaries of all bills related in any way to the general issue of privacy, consult the Web site of the Electronic Privacy Information Center (EPIC) at http://www.epic.org and http://www.epic.org/privacy/bill_track.html. If Congress fails to pass medical privacy legislation by the HIPAA deadline, the DHHS recommendations on maintaining confidentiality of individually identifiable information will take effect. The DHHS recommendations also constitute a model for Federal legislation. For these reasons, a summary of the DHHS recommendation follows.

Toolkit Section 3.4.1
Recommendations on Confidentiality of Individually Identifiable Information

The DHHS begins discussion of its recommendations on the confidentiality of individually identifiable information by addressing the scope of coverage—that is, to whom, to what activities, and to what information should the recommendations apply.

To whom do the recommendations apply? All health care providers, payers, and others who receive health information without authorization (such as health oversight, public health, and research organizations) should be subject to the new privacy legislation. Health service organizations are third parties who process health information from providers and payers as part of services rendered. The recommendations should apply to deceased persons for two years after death with specified rights being exercised on deceased's behalf. Conventional rules apply to minors, people with power of attorney, and people unable to act on own behalf. The recommendations should not apply to self-pay patients, prison inmates or detainees, liability insurers, life insurers, workers' compensation carriers, or employers unless acting as payers or providers. Federal departments responsible for members, civilian employers, and contractors of the military should develop their own regulations. The Department of Veteran's Affairs should have the right to release information without authorization for internal departmental use only.

To what activities should the recommendations apply? The recommendations should apply to three general types of activities:

- Any preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure with respect to the physical or mental condition or functional status of a patient or affecting the structure or function of the body
- Any sale or dispensing of a drug, device, equipment or other item pursuant to a prescription
- Procurement or banking of blood, sperm, organs, or any other tissue for administration to patients

To what information should the recommendations apply? The recommendations should apply to any information, oral or recorded, in any form or medium, including demographic information that has the following characteristics:

- Relates to past, present, or future physical or mental health or conditions of a patient, the provision of health care to a patient, or the past, present, or future payment for the provision of health care to a patient
- Is received, created, used or maintained by a health care provider in the ordinary course of business or practice of a profession, or by a health care payer, or received by entities receiving information under the provisions of the legislation without authorization
- Identifies the individual, or with respect to which there is reasonable basis to believe that the information can be used to identify the patient

The recommendations should apply to most people working in the health care business, to most of their patients, to almost everything they do that involves patients and almost all the information created, interpreted, and stored thereby as a matter of Federal

law. Although important, the exceptions to coverage underscore rather than minimize the change we face in the health care business.

The DHHS articulates five basic principles and makes specific recommendations implementing each basic principle of confidentiality. In general, the recommendations increase restrictions on the release of information to third parties, expand obligations to explain and document information management practices to patients, and impose new penalties for breaches of patient confidentiality. The DHHS also tries to balance patients' rights to confidentiality with society's need for knowledge derived from aggregating confidential information in the context of public health efforts. Five principles underlie the DHHS recommendations:

1. **Boundaries:** an individual's health care information should be used for health purposes and only those purposes, subject to a few carefully defined exceptions
2. **Security:** organizations to which we entrust health information ought to protect it against deliberate or inadvertent misuse of disclosure
3. **Consumer Control:** patients should be able to see what is in their records, get a copy, correct errors, and find out who else has seen them
4. **Accountability:** those who misuse personal health information should be punished, and those who are harmed by its misuse should have legal recourse
5. **Public Responsibility:** individual's claims to privacy must be balanced by their public responsibility to contribute to the common good, through use of their information for important, socially useful purposes, with the understanding that their information will be used with respect and care and will be legally protected

In order to implement these principles, Federal law should accomplish the following tasks:

- **Impose a legal duty of confidentiality on those who provide and pay for health care and on other entities who receive health information from them.** This duty has an affirmative and a negative component. An affirmative duty should exist only to use or disclose health information as authorized by patient or required by law. No duty should exist to disclose information except to patients. The Federal laws, moreover, should provide only a privacy floor, thus supporting and maintaining other laws providing greater protection for patient confidentiality to remain in effect. Health information should moreover be used only for purposes compatible with and directly related to the original purposes for obtaining the information and for which health entities are authorized to disclose it. (The DHHS directly addresses in this context the release to and use of health information by employers.)
- **Require security measures.** The DHHS recommends requiring by Federal law that health providers, payers, and service organizations maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of health information and protect it against threats, hazards, or unauthorized disclosures.

The DHHS synthesizes the boundary and security principles in what one might call "The Rule of Minimum Disclosure." Instead of releasing whole chunks of a patient's record without regard to a requestor's required use, organizations should in the future restrict all uses and disclosures, as practicable, to the minimum amount of information necessary to accomplish the purpose for which it is requested. This recommendation virtually requires adoption of the computerized patient record with its automated indexing and segmenting capabilities.

The DHHS recommends a complete overhaul in how health care providers and payers manage their patients' access to and control over personally identifiable health information. Health care providers must strengthen the ability of consumers to understand and control what happens to their information by:

- Providing written explanation of the organization's information practices and patient's rights with respect to their health information
- Granting patients access to their own records for the purpose of inspecting and/or copying them
- Permitting patients to seek correction and/or amendment of health information under certain conditions

- Maintaining records of most disclosures of information

The DHHS recommends allowing organizations to deny patients access to their records when access might cause grave harm to a third person or jeopardize an oversight activity, legal proceeding, or clinical trial. In the event that an organization refuses a patient's request to correct and/or amend health information, it must inform the patient of the refusal and allow the patient to file a concise statement explaining the requested correction and reason for disagreeing with refusal to change. The patient's statement should be included in the record, but the burden of proof for correction lies on the patient. None of these recommendations should abrogate existing reporting laws about such things as vital statistics and infectious disease or abrogate existing State or Federal laws that impose greater restrictions on use of private information.

The DHHS recommends providing new sanctions and new avenues for redress for consumers whose privacy rights are violated, including:

- **Civil proceedings:** actual and equitable relief including physical, mental and pecuniary losses. Attorney's fees should be paid in cases of knowing violation of confidentiality.
- **Criminal proceedings:** criminal penalties for obtaining health information under false pretenses and knowing and for unlawfully obtaining, using, or disclosing health information.

In an acknowledgment of its own interests in the debate about patient confidentiality, the DHHS recommends identifying those limited arenas in which public responsibilities warrant access to individual medical information but sharply limiting uses and disclosure of information. The issue in this case affects the ability of NIH and other public health research agencies to aggregate data originally obtained from the records of individual patients into large databases that could potentially reflect broad trends. The problem requires simultaneously stripping aggregate records of individual identifiers while maintaining the ability to trace the original sources.

Toolkit Section 3.4.2

(Waiting for publication of notice of proposed rule making on privacy of health care information)

Toolkit Section 3.5

State Medical Privacy Legislation

Sources of Information about State Laws on Medical Privacy

Federal legislation and the DHHS rules will eventually set minimum standards for medical privacy and the management of health care information. Many State legislatures actively address these issues with laws and rules of their own. Health care providers should track developments in their own states as well as at the Federal level. Some sources of information about State legislative activities follow.

1. The National Conference of State Legislatures maintains a rich Web site about major issues confronting the legislatures of all 50 United States. The web address is http://www.ncsl.org. The NCSL Web site includes hotlinks to the Web sites of all State legislatures some of which track bills under review. To gain access to the State Web sites, go to http://www.ncsl.org, then click on "Legislative Policy Issues," and then click on "Sites of State Legislatures."

2. Most medium-to-large universities subscribe to the Lexis/Nexis service. Lexis/Nexis recently introduced a new service entitled Lexis/Nexis Academic Universe that includes detailed information about case law and statutory law in all states. Many university libraries allow visitors to use their resources with permission.

3. Westlaw is another subscription service available through university law libraries. Access to this resource is limited.

4. All 50 United States track legislation by publishing an administrative bulletin. If you cannot find the information you need with the sources listed above, contact your State legislator and ask to receive the bulletin.

5. Under the direction of Janlori Goldman, PhD, The Health Privacy Project at the Institute for Health Care Research and Policy of Georgetown University has produced a detailed report privacy and state law - *The State of Health Privacy: An Uneven Terrain.* Its executive summary is reprinted with permission below, and the entire report is available at http://www.healthprivacy.org/resources/statereports/contents.html.

HEALTH PRIVACY PROJECT

Institute for Health Care

Research and Policy

Georgetown University

The State of Health Privacy: An Uneven Terrain

Executive Summary

There is no comprehensive federal law that protects the privacy of people's health information. The U.S. Congress is moving ahead to meet a self-imposed deadline to enact a broad health privacy statute by August 1999. If the deadline is not met, the Secretary of Health and Human Services must issue regulations by February 2000. At this time, people must rely on whatever health privacy protections are built into their state's statutes.

As the congressional debate over health privacy heats up, there is a question that is always asked but— until now— has been impossible to answer. "What state laws exist in this area? How have states responded to the health privacy needs of their citizens?"

This report is the first-ever comprehensive 50-state survey of health privacy statutes. In our experience, the hallmarks of researching state health privacy laws have been that: 1) nothing is simple; and 2) nothing is predictable. In the process of researching, analyzing, and summarizing the statutes, we reached a number of conclusions and made a few surprising discoveries. But in many more ways, the states defy categorization.

State laws relating to health privacy have been enacted at different points in time, over many years, and to address a wide variety of uses and public health concerns. One must approach each state on its own terms and attempt to understand the protections as a unique whole within the state. In striving for precision and nuance, our labels of state laws are accompanied by qualifiers and explanations.

Laws relating to health privacy can be found in nearly every nook and cranny of a state's statutes – in obvious and obscure sections of a state's code, buried in regulations, developed in case law, and detailed in licensing rules. Florida, for example, has more than 60 statutes that address health privacy, and the state is not unique.

A number of initial observations emerge from the state summaries:

States legislate and regulate health privacy by entity.

There is little mystery about why state health privacy laws are so extensive, vast, and detailed: the statutes reflect the diverse users of health information. Consider the following four types of users: physicians, schools, insurers, and state agencies. Each has a specific function in the state and a legal and regulatory structure specific to its roles. Thus, the statutory requirements for how they handle medical information are different.

To understand what confidentiality protections do exist at the state level, one must first begin by examining the laws applying to the different entities that collect, use, maintain, and distribute health information. Even states that attempt to handle health privacy in a comprehensive fashion ultimately establish unique rules for different entities. In looking at a state's laws and determining what kind of privacy protections exist, one must always ask, "Who's holding the data?" and "What is the medical condition at issue?"

The end result of this legislating by entity is that state laws – with a few notable exceptions – do not extend comprehensive protections to people's medical records. Thus, a state statute may impose privacy rules on hospitals but not dentists. The state may restrict the use and disclosure of information derived from a genetic test but not information obtained in a routine physical. Or just the opposite may be true in a neighboring state.

The cumulative effect of these various statutes might appear erratic, but so many of the laws that do exist provide meaningful protections for consumers and speak to the specific needs of the organizations and citizens of the state. For instance, a nursing home may have different information needs than a public hospital, and state laws attempt to accommodate these differences.

The vast majority of state statutes were never intended to be comprehensive.

Virtually every state has some law aimed at the confidentiality of patient information, but very few states have anything approaching a comprehensive health privacy law. Three notable exceptions are Hawaii, Rhode Island and Wisconsin, each of which has comprehensive health privacy laws. Many states have health privacy laws governing certain health care entities, such as hospitals or clinics, but no privacy protections regulating health plans and HMOs.

State confidentiality requirements are part and parcel of larger statutes that provide consumer protections or regulate persons or entities. Many of the statutes, for example, are imbedded within licensing requirements. In this context, the provider is required to maintain health information in confidence in order to obtain and maintain a license to practice from the state. One must read all of the statutes together in order to glean an understanding of how health information is protected as it moves between persons and entities.

An ethical duty to maintain confidentiality is often assumed.

Most states appear to presume an ethical duty on the part of health care providers to keep information confidential. Many statutes, for instance, do not explicitly impose a duty of confidentiality, but they do stipulate a penalty for breaching patient confidentiality. It seems that in these instances, the states did not see a need to legislate the ethical duty. Unfortunately, the users of health information have extended well beyond those who may be bound by professional codes of ethics.

State laws have not kept pace with changes in health care delivery and technology.

Most state laws do not reflect the dramatic changes in the health care environment or the dramatic changes in information technology. Today, for instance, the majority of health care is not delivered by physicians. Integrated delivery systems (such as HMOs and provider networks) and the establishment of statewide health information databases have created new demands for data that push well beyond the limits originally anticipated by the states. The variety of people and entities collecting, receiving and using health information has also extended far beyond the health care environment. A physician, for example, may be obligated to report a person with epilepsy to the Department of Motor Vehicles, which in turn may revoke a driver's license.

Therefore, in many ways, the state laws defy summarization – they are detailed, specific, and intricate. Nevertheless, we have attempted to bring some coherence to this report. The summaries are arranged in four broad categories: Patient Right of Access, Restrictions on Disclosure, Privileges, and Condition-specific Requirements. Our major findings in each category are listed below.

Key Findings

Patient Access

States vary widely in the rights they grant to patients to receive and copy their own medical records. Some states have no statutory right of access, such as Kansas and North Dakota. Three states – Alabama, Idaho, and New Mexico – and the District of Columbia, only have a statutory right for patients to access their own mental health records.

On the opposite end of the continuum, a few states – such as Connecticut and Minnesota – grant access to records maintained by nearly all of the potential sources of patient data, i.e. government agencies and entities, hospitals, physicians, insurers, schools, and even non-traditional health care providers such as natureopaths. Maine and South Dakota, for example, have cast a particularly wide net with respect to providing access to records maintained by health care providers by using broad definitions that anticipate future users and holders of medical information, such as those performing in vitro fertilization and blood banks.

Most states fall somewhere in the middle of these two extremes. Forty-four states provide some right of access, but this figure is a bit misleading. The right of access quickly breaks down:

33 states provide a right of access to hospital records;

13 states provide a right of access to HMO records; and

16 states provide a right of access to insurance records.

Many additional statutes cover specific providers – such as physicians, psychiatrists, and pharmacists. However limited the right, the impact of providing the right should not be underestimated. For example, in response to the public's desire to utilize alternative sources for contact lenses, Colorado and a few other states require optometrists to disclose prescriptions to their patients.

All state statutes that grant people a right to see and copy their own medical records limit that right with a set of exceptions. The most common exception is that a patient can be refused access to his or her own medical record if the record holder believes that the release of the information could endanger the life and safety of the subject of the information or another person.

Many states have also granted patients the right to amend or correct their medical information, particularly when the records are held by insurance companies. In Illinois, New Jersey and Ohio, for example, the statute includes a detailed procedure for resolving a patient's challenge to the accuracy or completeness of the record. Where the provider and the patient disagree, for example, the patient may be able to insert a statement of his or her position in the record.

Most states allow a person or entity to charge patients for copies of their medical record. Some states specify a cost in the statute – in Kentucky, for example, a health care provider or hospital must provide a patient with a free copy of their medical record. A patient may be charged for additional copies, but not more than $1 per page. Other states require that the fee be waived if the patient is contesting an adverse underwriting decision. The most common approach is to stipulate that an entity may charge a "reasonable" fee.

Restrictions on Disclosure

States vary widely in terms of the restrictions or prohibitions they impose on disclosures of medical records and medical
information. The restrictions tend to be triggered in two instances: by the entity holding the data, and the kind of information
being held.

For the most part, the state statutes prohibit a person or entity from disclosing information unless certain conditions are met. The most notable impact of this approach is that it may limit the actual protections afforded the data. Once the information is disclosed, it may or may not be afforded the same protections by the receiving entity. For instance, the state laws may not place limits on the re-disclosure patient data, or the receiving entity may not be under any legal obligation to adhere to the privacy rules imposed on the disclosing entity.

In comparison, a few states – such as Wisconsin and Rhode Island – have statutes that prohibit medical information from being disclosed, regardless of the entity holding the record.

Overall, the most common restriction found in state statute is that patient authorization must be secured prior to health information being disclosed. Some states specify the format and content of the authorization form in statute. Many states allow patients to revoke authorizations.

At the same time, these statutes all specify numerous exceptions to this general rule in which a person or entity may disclose information without patient authorization. The most common instances include: for purposes of treatment; to secure payment for healthcare; for auditing; and for quality assurance activities. Most statutes allow access to patient data for research purposes, without any patient notification or authorization. (See later discussion on research.)

Also of note is that some states do prohibit the re-disclosure of medical information. In such instances, an entity that receives medical information is prohibited from re-disclosing the information unless a separate authorization is secured, or the disclosure is in keeping with the statutory requirements imposed on the original disclosure. Other states do not statutorily restrict the re-disclosure of medical information. In Montana, for instance, the state has adopted a public policy that recognizes that a patient's interest in the proper use of health care information survives its initial release by a health care provider. The state, however, has decided not to statutorily regulate subsequent disclosures because a person's expectation of privacy changes when the information is held by a non-health care provider.

Privileges

We have included a survey of states' statutory privileges for two reasons: 1) to date, all of the proposed federal health privacy legislation leave state privilege law intact; and 2) many states' statutes governing the confidentiality of health care information maintained by HMOs provide that an HMO is entitled to claim any statutory privilege against disclosure that the provider of the information is entitled to claim. Thus, in order to understand what privilege an HMO might be able to exercise, it is necessary to know what statutory privileges exist.

A common misconception about the physician-patient privilege is that it is a general prohibition against a health care provider sharing information about his or her patients. However, it is important to recognize that in legal terms, there is a distinction between "privilege" and "confidential." The law of privilege is generally seen as a rule of evidence which is limited in scope. It allows a patient in a legal or quasi legal proceeding to refuse to disclose, and to prevent others from disclosing, certain confidential information (usually communications) obtained during the course of diagnosis and treatment. In contrast, a health care provider's duty of confidentiality to her patients, arising from a code of ethics, by regulation, or otherwise, is a broader duty not to disclose to the public information obtained in a professional capacity.

That being said, it must be noted that even legal professionals often use the terms interchangeably. We have attempted to note where a state has worded its statutory privilege in such a way as to extend it beyond a legal or quasi legal proceeding.

It must be emphasized that this is a summary of statutory rules of privilege. Many more providers and entities may be covered by a state's common law privilege. The summaries do not include a discussion of when privilege may be waived. State law is detailed and voluminous on this subject, and we chose simply to indicate to whom the statutory privilege applies.

Condition-specific Requirements

Nearly all states have laws that impose condition-specific privacy requirements, most often to shield people with mental illness, communicable diseases, cancer, and other sensitive, stigmatized illnesses from broad disclosures. Many of these laws were passed to respond to public fear that certain health information would be widely disclosed and used to deny patients benefits or result in other harm. Where this fear acted as a barrier to seeking health care, treatment, or counseling, states have moved to bolster public trust and confidence in the health care system by enacting heightened privacy rules in these specific areas. The protections tend to attach to the information at the point of collection, before the information is disclosed. These requirements may, for example, direct a provider, hospital, or laboratory to obtain a particular kind of authorization from the patient.

In some circumstances, the condition-specific requirements allow for greater disclosure of the information. Some mental health statutes, for example, explicitly allow family members to access the mental health records of a family member who has been committed. Other statutes allow employers to share medical information about an employee if it affects her performance on the job.

Most of the condition-specific requirements that exist at the state level, however, were enacted hand-in-hand with mandatory reporting laws. For instance, essentially all states require that health care providers report to governmental health authorities the identity of persons suspected or diagnosed as having specified contagious diseases, such as tuberculosis. Many states require providers to report the identity of children born with birth defects to a central registry. The statutes then limit how the health authorities or registry can use or disclose the information which has been collected. In most cases, however, the protections do not apply to any other entity holding the same information -- such as the provider, hospital, or insurance company. While the summaries note the protections afforded the data, it is important not to lose sight of the fact that these privacy laws were enacted on the backend of laws requiring doctors and other health care providers to report to state officials identifiable patient data related to certain illnesses and conditions. Clearly, state lawmakers viewed such privacy protections as a necessary balm to quiet public fears of the government developing health information databases on vulnerable citizens. Our inclusion of the public health reporting requirements and related privacy protections are not comprehensive, but we point out that many states' reporting requirements are aimed beyond communicable or infectious diseases. Many states collect health information to study costs, outcomes, and quality – all of which rely on extensive patient data. In turn, there is a great demand – often answered in the affirmative – for access to this data.

Remedies and Penalties

Most state health privacy statutes contain some form of remedies and penalties that are triggered by violations of the law. Commonly found are private right of action provisions granting people the ability to bring lawsuits when the statute has been violated, without first having to meet any additional standard of proof, i.e. that the violation was willful or intentional. It is enough that the law was violated. A full range of damages, remedies, and attorney's fees and costs are usually available, however the monetary damages are often set quite low. In some cases, these statutory remedies may be construed as exclusive, thereby barring people from raising other claims, such as privacy torts or other common law claims.

Government-maintained Records

Across the board, records held by government agencies and officials are treated differently – and are usually more protected – than the medical information collected and held by the private sector. In some instances, the medical records held by the government are the only records protected in statute. In effect, a state statute may impose confidentiality requirements only on public hospitals, leaving people who are treated in private hospitals without the same legal safeguards. In Oregon, for example, the statutory prohibitions on disclosure, including authorizations, apply only to public providers of health care. Private health care providers are simply "encouraged, but not required, to adopt voluntary guidelines limiting the disclosure of medical records..."

Although this legal distinction – between public and private holders of medical information – is rooted in the constitutional principle that there must be limits on government action vis-a-vis the individual, it may not be particularly meaningful to health care consumers. Therefore, privacy protections for other personal information have been extended in a number of federal and state privacy statutes to restrict the private sector's collection and use of personal information.

Research

Again, there is little uniformity in how state statutes regulate researcher access to people's medical information. The vast majority of laws, however, do allow researchers broad access to patient records. As the laws apply to private entities, researcher access is almost always built in as an exception to a statute's patient authorization requirements. What limits do exist usually speak only to specific information – such as genetic information or HIV/AIDS information.

On the other hand, researcher access to patient data held by government entities, i.e., agencies or registries, is in some instances more detailed. Some registries, for example, have strict conditions that must be met before researchers can access data and may require that personal identifiers be removed before a researcher can access information.

Conclusion

Again, there is no comprehensive federal law protecting the privacy of people's medical records. Congress has acknowledged that such a law should be passed and imposed a deadline on itself to do so by August 1999. If Congress fails to meet the deadline, the Secretary of Health and Human Services is required to issue regulations by February 2000.

Health privacy is not a new issue to the U.S. Congress. Each year over the past decade, as debate has resumed over how to best craft a health privacy law, the question is inevitably raised, "What have the states done? What are the state health privacy laws? What will be the impact on the states of any federal preemption of state law? What negative and positive models exist for us to learn from?" For the most part, these questions have gone unanswered. Until now, no comprehensive compilation of state health privacy laws existed.

As this report documents, there is little probability that any federal law could match the breadth and scope of the existing state laws. As such, any federal law that fully preempted state law would eliminate some of the rights and protections consumers currently enjoy and disrupt current state legal and regulatory structures. Here's why –

States have been the first to respond to concerns about health privacy and they have enacted many strong protections.

State health privacy statutes cover a broad range of entities and, not surprisingly, are both weak and strong. In terms of broad consumer protections, one can identify many significant gaps and weaknesses in most state statutes: such as a limited right for a patient to access his or her own medical record; little ability for patients to limit disclosure of their medical records; and little recourse when the laws are violated.

On the other hand, state laws enacted in response to a particular public concern, or a public health threat– such as in the areas of mental illness, communicable disease, cancer, and genetic testing – are often strong, detailed, and aimed at the states' unique experiences with their citizens.

State laws address a level of detail not considered in any of the federal proposals.

The importance of the detail in state health privacy law should not be underestimated. Because the states legislate by entity, they are often able to craft laws that speak to the unique needs of the patient population

and the information needs of particular entities. An HMO, for example, has very different needs than a family planning clinic.

State law is extensive – it is impossible to predict the full impact of full federal preemption.

Most importantly, it is almost impossible to predict the full impact of federal preemption on state laws relating to health privacy. Remember that these summaries are only the tip of the iceberg in terms of relevant state statutes. Many more laws govern areas such as adoption, workers compensation, public health reporting, civil, judicial and administrative procedures, fraud and abuse, and law enforcement access.

There is widespread consensus that a federal law could help to provide significant new protections and to establish some basic rules about the use and disclosure of health information. However, until this point, the policy debate about preemption tended to be based on rhetoric, not fact. There is a large body of law before us now. While many of the facts are reassuring, it does not lend itself to easy answers.

A significant challenge is before us. There is no doubt that such a comprehensive federal health privacy law could be beneficial in many ways. But while a federal law could substantially benefit people by establishing a baseline of consumer protections, a federal law that ignored the significant role states have played in protecting health information could disrupt the legal and regulatory structures at the state level and, in turn, some of the protections currently afforded to consumers.

Our hope is that this report will serve as the factual basis upon which to proceed, providing us with a true opportunity to move beyond the rhetoric that has so far defined this debate.

Toolkit Section 3.6

Setting Standards in Health Care Information

By: Margret Amatayakul, MBA, RRA

Security Standards

This section provides an introduction to standards development, an overview of information systems standards in general and as they relate specifically to health care, a summary of the frameworks under development for health care information systems security standards, including HIPAA regulations, and brief descriptions of the major information system security standards efforts and standards themselves which may be applicable to the health care industry. See the glossary of acronyms and Internet addresses at the end of the toolkit for additional information on all organizations referenced in this section.

Introduction to Standards

A standard is defined as "something established by authority, custom, or general consent as a model or example." When used as an adjective, the definition includes "conforming to a standard as established by law or custom [which is] sound and usable." These definitions suggest that standards establish a set of requirements, processes, procedures, terms, options, or arrangements of objects that come into existence by common usage or a formal process and provide uniformity and constancy at a baseline level of acceptance.

The American National Standards Institute (ANSI) is a private, non-profit organization that coordinates formal voluntary consensus standards activities in the United States and approves American National Standards. Members of ANSI include over 1,000 companies, 30 government agencies, and over 250 professional, technical, trade, labor, and consumer organizations. The organization ensures that a single set of nonconflicting American National Standards are developed by ANSI-accredited standards development organizations (SDOs) and that all interests concerned have the opportunity to participate in the development process. All ANSI approved standards also must undergo regular review and revision. ANSI has approved over 11,000 standards in five major categories: dimensions, ratings, terminology and symbols, test methods, and performance and safety requirements. (For more information about ANSI, see www.ansi.org/.) ANSI is the sole representative and member of the two major non-treaty international standards organizations: the International Organization for Standardization (ISO) (see: www.iso.ch) and the International Electrotechnical Commission (IEC).

Standards may also be developed in professional societies, trade associations, government agencies, and industry consortia or may simply come about by common usage. The American Medical Association's CPT-4 procedural descriptions and codes is an example of a standard developed by a professional society. Microsoft has dominated the personal computer operating system market to such an extent that its product has become a standard through common usage.

Information Systems Standards

For information systems in general, the Open Systems Interconnection (OSI) reference model (shown in Figure 1) is designed to organize standards within seven layers to ensure that devices and software from different suppliers work together. Standards address many functions such as capacity, transmission rates, protocols, and security. While very few systems are fully OSI compliant, the model is useful for the structure of layers it introduces. Standards at the lower layers are not industry specific. For example, hardware encryption devices may be used in banking and health care. Standards become more specific to the industry as they address the higher layers, especially the applications layer. As security standards are more fully described in this section, the reference model will be used to identify where each type of security standard is applicable.

Health Care Information Systems Standards

In health care, several organizations develop standards relating to the health care information application level. Some of these are ANSI-accredited and others are professional societies, trade associations, industry consortia, etc. The ANSI Healthcare Informatics Standards Board (HISB) has been created within ANSI to help coordinate and promote adoption of standards relating to health care information system applications. (see: web.ansi.org/gtests/hisb/) Examples of organizations that participate in ANSI HISB are depicted in Figure 2. (A web site that serves as a link to many of the standards

developed by ANSI HISB members and other organizations is the Duke University Medical Center Healthcare Informatics Standards Site: www.mcis.duke.edu/standards/guide.htm.)

On August 21, 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) which included an Administrative Simplification section requiring the use of standards for electronic health care transactions, addressed the need for privacy legislation, and called for recommendations concerning standards for medical record information. Specifically, HIPAA required Health and Human Services to adopt standards that have been developed by an ANSI-accredited SDO, unless no standard had been developed or another standard would significantly reduce administrative costs and `as promulgated in accordance with "negotiated rulemaking" procedures. (Information about the administrative simplification requirements can be found at http://aspe.os.dhhs.gov/admnsimp/.)

Health Care Information Systems Security Standards Frame Works

Health care information systems security standards are critical for ensuring the confidentiality and integrity of private health information.

Privacy determines who should have access, what constitutes the patient's rights to confidentiality, and what constitutes inappropriate access to health records. In the United States today, privacy law exists in state statutes, but there is no Federal comprehensive privacy law. HIPAA called for the Secretary of Health and Human Services to submit recommendations to Congress "on standards with respect to the privacy of individually identifiable health information," and that was done on September 11, 1997. (The recommendations are available at http://aspe.os.hhs.gov/admnsimp/pvcrec0.htm.) Congress has until August 21, 1999 to pass privacy legislation pursuant to HIPAA, otherwise the Secretary is mandated to issue privacy regulations by August 21, 2000.Will need to be updated near the time the web site goes live.

Security is embodied in standards and technology that enable confidentiality of health care information and health data integrity policies to be carried out. Figure 3 demonstrates the relationship among the concepts of privacy, confidentiality and data integrity, and security and their embodiment in law, policy, and standards.

Several health care informatics SDOs are developing frameworks for health care security service mechanisms to protect against security threats.

Security Threats

ASTM was organized in 1898 as the American Society for Testing and Materials and has grown into one of the largest SDOs in the world. It is a not-for-profit organization that provides a forum for producers, users, ultimate consumers, and those have a general interest to meet on common ground and write standards for materials, products, systems, and services. ASTM Committee E-31 on Healthcare Informatics was established in 1970 as an ANSI-accredited committee to develop standards for health information and health information systems. Current standards address architecture, content, portability, format, privacy, security, and communications of health care information. ASTM's Provisional Standard (PS 101) "Guidelines for a Technical Security Framework for Transmission and Storage of Healthcare Information" identifies the following security threats relative to health care information:

- Masquerade - one entity pretending to be another entity, facilitating the following other attacks.
- Modification of information - including message or data content, destruction of messages, data or management information.
- Message sequencing threats - including replay, pre-play, and delay of messages.
- Unauthorized disclosure - reveals to an unauthorized user message content, information derived from observing message flow, and information held in storage on an open system.
- Repudiation - a user or system denies having performed some action, such as modification of information.
- Denial of service - prevents the systems from performing its functions.

HL7 Security Exposures

HL7 (Health Level Seven) was founded in 1987 to develop standards for the electronic interchange of clinical, financial, and administrative information among independent health care oriented computer systems (e.g., hospital information systems, clinical laboratory systems, enterprise systems, and pharmacy systems). In June of 1994, HL7 was designated by ANSI as an ANSI-accredited standards developer. HL7 in its draft *Security Services Framework* categorizes health care information security exposures in the following manner:

Disclosure
- Exposure
- Interception
- Inference
- Intrusion

Deception
- Masquerade
- Falsification
- Repudiation

Disruption
- Incapacitation
- Corruption
- Obstruction

Usurpation
- Misappropriation

Misuse

HL7 further references the Crisis Emergency Response Team (CERT) for specific instances of some of these security failures (see: www.cert.org/).

Security Services

Security services are defined in the HL7 and ASTM references as:

- Identification and Peer Entity Authentication - provides proof of the identity of communicating parties, primarily through digital signatures or other cryptographic integrity mechanisms.
- Data Origin Authentication - provides corroboration that the source of data is received as is claimed, and is also provided using digital signatures or other cryptographic means.
- Authorization and Access Control - supports the granting of rights to access and the prevention of unauthorized use of resources. This is accomplished through digital signatures and access control lists which identify entities and their access rights which may be context-based, role-based, and/or user-based and provide for mandatory, discretionary, time-of-day, classification, and/or subject-object separation access.
- Confidentiality - ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes. Encryption is used to provide this service and may include selective field confidentiality, which generally requires modification of existing message structures or encapsulation of the entire message for complete confidentiality. Key escrow also provides for confidentiality.
- Integrity - ensures that data or system software have not been undetectably altered or destroyed in an unauthorized manner or by unauthorized users. This can be provided by various integrity check values.
- Non-repudiation - provides proof of origin or receipt which will protect against an originator or recipient falsely denying responsibility for the action. This protection is afforded through use of a digital signature and encryption.

Security Mechanisms

HL7 also identifies additional security mechanisms relating to administrative and physical aspects of security:

- **Accountability** - refers to tracing of actions of an individual or entity so that responsibility can be determined. Audit trails, logs, and receipts are examples of means to provide accountability.
- **Availability** - ensures that information is accessible and useable upon demand by an authorized entity. Availability is the result of appropriate security services and data capture policies.
- **Administration** - is the management of security policy, including the existence of physical and environmental security, disaster planning and recovery, personnel security, training and awareness, information technology facilities management, authentication and access control, database security, system maintenance, and legislation compliance. These guidelines were drawn from the Computer-based Patient Record Institute's *Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Records* (CPRI, January 1996 and see Chapter 4 below) and *Security Features for Computer-based Patient Record Systems* (CPRI, September 1996 and see Chapter 4 below) (www.cpri.org), as well as work performed by the Secure Environment for Information Systems in Medicine (SEISMED) project (see: www.semper.org/sirene/projects/seismed/).

Security Service Standards

The table below summarizes the standards that exist for the technical security services identified by ASTM (from ASTM's Provisional Standard [PS 101]) *Guidelines for a Technical Security Framework for Transmission and Storage of Healthcare Information*).

Many of the standards that supply the health care specific information security service framework were not developed for health care specifically, and few health care security standards have been written until recently. While confidentiality of private health information has always been a concern in health care, special measures were not considered necessary when it was believed that only authorized personnel had access to paper records.

ASTM Health Care Information Security Framework

	Link	Subnetwork	End-to-end	Application (Session-oriented)	Application (Store and forward)

Authentication (peer entity)	None	IPSEC	IPSEC	FIPS 196, SPKM	PKCS-7
Authentication (data origin)	SILS	IPSEC	IPSE	SSL, SPKM	PKCS-7
Authorization and access control	N/A	IPSEC	IPSEC	Draft standard in ASTM E31	Draft standard in ASTM E31
Integrity	SILS	IPSEC	IPSEC	SSL, SPKM	PKCS-7
Confidentiality	SILS	IPSEC	IPSEC	SSL, SPKM	PKCS-7
Non-repudiation	N/A	N/A	N/A	ASTM E1762, Draft standard in ASTM E31 S-HTTP	ASTM E1762 Draft standard in ASTM E31

National Research Council Findings

In 1995, the National Library of Medicine, as one of the lead agencies within the government for facilitating health care applications of the national information infrastructure, identified privacy and security as primary issues that needed to be addressed in order to facilitate greater use of information technology within health care. As a result, the National Research Council (NRC) initiated a study to observe and assess existing technical and nontechnical mechanisms for protecting the privacy and maintaining the security of health care information systems. The report, *For the Record: Protecting Electronic Health Information,* published by the National Academy Press in 1997, revealed serious inadequacies in how health care providers were safeguarding their health care information. It recommended several security procedures for immediate adoption, including:

- Individual authentication of users - in which every individual has a unique username/password for access and is held accountable for all actions taken while logged on.
- Access controls - to allow viewing of clinical information on a need-to-know basis.
- Audit trails - log all accesses to information and should be available for patient and clinician review on demand.
- Physical security and disaster recovery - encompassing positioning of computer terminals where unauthorized users cannot view displays, denial of access to paper printouts and electronic storage by unauthorized personnel, use of frequent backup tapes housed off-site.
- Protections of remote access points - that firewalls should be implemented and all remote accesses protected by single session or encrypted passwords.
- Protection of external electronic communications - requiring all patient-identifiable data transmitted over public networks to be encrypted.
- Software discipline - installation of virus checking programs and limitations on downloads from the Internet on all servers.
- System assessment - audits should be performed on a monthly basis to examine vulnerability to password cracking programs and to verify procedures implemented to detect system vulnerabilities.

For future adoption, the NRC report recommended:

- Strong authentication - in the form of “hardware tokens.”
- Enterprise-wide authentication - wherein users may authenticate once and have access to all relevant systems in an enterprise.
- Access validation - both system function and content detail should be controlled by role.
- Expanded audit trails - that provides a consolidated audit for all software.
- Electronic authentication of record - electronic signature for “signing” medical records and cryptographic digital signature for retrieving records.

For the Record: Protecting Electronic Health Information is available on line at http://www.nap.edu/books/0309056977/html/index.html

HIPAA's Security Regulations

HIPAA's security regulations reflect the recommendations of the NRC report and the work of the SDOs to establish a security framework. Security regulations will apply to claims clearinghouses, health plans, employers, and health care providers that maintain or transmit automated health information. A draft security matrix and proposed rules that capture the requirements and implementation features that the health care industry will be expected to meet were published on August 12, 1998 (see: http://erm.aspe.hhs.gov/erm/secnprm). The standards to safeguard data integrity, confidentiality, and availability of a health care entity's electronic data are categorized in HIPAA's security matrix as:

- Administrative procedures - documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relationship to the protection of data.
- Physical safeguards - protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Covers use of locks, keys, and administrative measures to control access to computer systems.
- Technical security services - processes to protect and to control and monitor information access.
- Technical security mechanisms - processes to prevent unauthorized access to data that are transmitted over a communications network.

Recognizing that an industry consensus on security standards does not yet exist, the regulations are trying to establish a flexible framework for security practices that meet the goals of security without prescribing the means. Definition and penalties for wrongful disclosure of individually identifiable health information were also included in the proposed rules, as was a section on electronic signature which requires use of a digital signature if an electronic signature is to be used.

Security Standards for Health Care Information Systems

The HIPAA Security Matrix maps some 55 documents to the various security requirements and methods of implementation in the proposed regulations. While the documents are illustrative and not all standards, the documents are an appropriate starting point for summarizing the standards that may be appropriately applied to protect health care information. The following list of standards and other documents has been arranged in general by OSI level and then by organization. It should be understood, however, that a number of the standards have evolved from proprietary standards, to ANSI-accredited (United States) standards, to international standards. Every effort has been made to categorize the standard according to the organization currently responsible for its maintenance as well as to reference it to other designations. Also included are works that are not standards, but which are applicable reference material for the domain.

United States General Security Standards

There are a number of standards groups, industry consortia, government agencies, and vendors that have developed security standards at the lower OSI layers. The following are referenced in the proposed HIPAA Administrative Simplification security matrix and/or other standards:

ANSI X3S3.3 - An ANSI-accredited standards committee for the development of standards for lower layers, **X3.92 Data Encryption Standard (DES)**, is its most well-known in the security arena.

DES - Data Encryption Standard was developed by IBM in the 1960s for the U.S. Department of Defense and was subsequently published as ANSI X3.92. It is also available as **NIST, FIPS PUB 46-2**. It is sometimes referred to as **DEA** (data encryption algorithm). It is a symmetrical key system for use at the physical, or data link (for LANs) layer over asynchronous lines. DES has generally been considered adequate for most practical commercial purposes, but not sufficiently secure for top secret applications. As computer power increases, however, the length of the key has become an issue. (See discussion under RSA.) The main drawback of DES, however, is in exchanging the keys and keeping them secure because the same key is used to encrypt and decipher the message, thus it is unsuitable for communicating with

unidentified, untrusted parties. Public key algorithms that are asymmetrical are more suitable for such communications.

ANSI X9F1 - ANSI has approved as American National Standards a number of standards for the Public-Key Infrastructure (PKI). Many of these had their origins in proprietary standards developed by industry. Many of the these standards have also been approved as ISO standards. (For information about X9F1, see www.csrc.nist.gov/pki).

ANSI X9.17 - Cryptographic Service Messages - describes a multilayer key management scheme used in interbank communications, and in other applications for communicating between trusted hosts.

ANSI X9.26 - Secure Sign-On Standard - provides a simply implemented, challenge and response password system many times more secure than a normal ID/password combination.

ANSI X9.30 Part 1: Public Key Cryptography Using Irreversible Algorithms: Digital Signature Algorithm, 1995. Also available as NIST, FIPS PUB 186.

ANSI X9.30 Part 2: Public Key Cryptography Using Irreversible Algorithms: Secure Hash Algorithm (SHA-1)

ANSI X9.31 Reversible Digital Signature Algorithms

ANSI X9.42 Management of Symmetric Keys Using Diffie-Hellman

ANSI X9.44 Key Transport Using RSA

RSA - (Rivest-Shamir-Adleman) - is an asymmetrical algorithm named after the mathematicians who described it in 1978. It is proprietary (although subject to U.S. government regulations) and commercially available (e.g., PGP), having been implemented in a number of products. It is cumbersome to use for encryption of data streams and is being replaced by newer schemes with larger, and possibly variable, key sizes that incorporate key management and key transmission. Some of the contenders include Clipper, which is a hardware-based encryption scheme supported by the U.S. Department of Defense, the Japanese-invented Fast Encryption Algorithm (FEAL), the Australian LOKI, and the International Data Encryption Algorithm (IDEA).

ANSI X9.45 - Enhanced Management Controls Using Digital Signatures and Attribute Certificates

ANSI X9.52 - Triple DES Modes of Operation

ANSI X9.55 - Extensions to Public Key Certificates and Certificate Revocation Lists

ANSI X9.57 - Certificate Management

ANSI X9.62 - Elliptic Curve Digital Signature Algorithm (draft)

ASC X12- Accredited Standards Committee X12 - The Data Interchange Standards Association (DISA) (see www.disa.org) is the not-for-profit organization that supports X12. X12 develops, maintains, interprets, publishes, and promotes the proper use of American National and UN/EDIFACT International Electronic Data Interchange Standards. Its main objective is to facilitate electronic interchange relating to business transactions such as order placement and processing, shipping and receiving information, invoicing, and payment and cash application data, and data to and from entities involved in finance, insurance, education, and state and federal governments. X12N addresses health insurance specifically, and its transaction standards are being proposed under HIPAA. The following X12 standards address security:

ANSI X12 .42 Cryptographic Service Message (815) - provides the data format required for cryptographic key management, including automated distribution and exchange of keys.

ANSI X12.58 - Security Structures (version 2)

ANSI X12.376 Secure Authentication and Acknowledgment (993) - used by the recipient of a transaction set to authenticate and acknowledge the origin, content, or sequence of data received with the originator of the transactions.

IEEE - Institute of Electrical and Electronics Engineers - is an industry consortium (see: www.ieee.org) that has developed the Medical Information Bus (MIB) standard, IEEE 1073, for automated data capture from bedside patient medical devices. In the security arena, the following standard has been developed by this group:

IEEE 802.10 - Standard for Interoperable Local Area Network Security (SILS), Draft 1992 - 1996 - IEEE 802.10 is seeking to expand the ISO 7498-2 Security Architecture so that security services (i.e., authentication, access control, and data integrity) can be provided at layer two. The document has eight parts, including a model, secure data exchange, key management, security management, Ethernet, sublayer management, SDE security labels, and protocol information conformance statement (PICS) proforma. X3S3.3, the ANSI-accredited standards committee for lower layers has not supported this project because it departs from the familiar ISO Security Architecture and because it incorporates material subject to copyright protection.

IETF - Internet Engineering Task Force - (see: www.ietf.cnri.reston.va; ftp://ds.internic.net/) is a large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. IETF standards are created by committees that are submitted to the networking community through a set of documents called Requests for Comments (RFCs). All RFCs are considered draft documents because any document can be superseded by a newer RFC. IETF provides a suite of protocols under **IPSec** to secure communication at the network layer between communicating peers. The following are applicable standards from IETF:

IETF ID Combined SSL/CPT Transport Layer Security Protocol

SSL - Secure Socket Layer Protocol - is a programming interface developed by Netscape for World Wide Web applications and is currently undergoing standardization through IETF. It augments the sockets programming interface, which in turn is an interface to TCP. SSL ensures that eavesdroppers cannot read data, allows either side to verify the identity of the other side, and assures data integrity because any change to a byte will invalidate the check sum on each SSL chunk. SSL solves the problem of authentication and privacy between two sites using TCP, but is not a good choice for “store and forward” environments because once data is read all proof of origin is lost.

IETF ID FTP Authentication Using DSA

IETF ID Secure HyperText TP Protocol (S-HTTP)

S-HTTP - Secure HyperText Transfer Protocol - defines a request/response protocol on top of the HTTP protocol used in the World Wide Web. This protocol can secure each request/response pair separately, and provides data origin authentication, integrity, and confidentiality. It also provides non-repudiation of responses. It emphasizes record or document level protection rather than session-level protection.

IETF RFC 1422 Privacy Enhanced Mail: Part 1: Message Encryption and Authentication Procedures

IETF RFC 1424 Privacy Enhanced Mail: Part 2: Certificate-Based Key

Management

IETF RFC 1423 Privacy Enhanced Mail: Part 3: Algorithms, Modes, and Identifiers

S/MIME - Secure Multi-purpose Internet Mail Extensions - is public key encryption protocol originally developed by RSA Laboratories for secure e-mail.

IETF RFC 1510 - Kerberos Authentication Service

IETF RFC 1825 - Security Architecture for the Internet Protocol
IETF RFC 1826 - Internet Protocol Authentication Header
IETF RFC 1827 - Internet Protocol Encapsulating Security Payload (ESP)
IETF RFC 1828 - Internet Protocol Authentication using Keyed MD5
IETF RFC 1829 - The ESP DES-CBC Transform

IETF RFC 2025 - Simple Public Key Mechanism

SPKM - Simple Public Key Mechanism - is designed for use with any session-oriented application, providing confidentiality, integrity, entity and origin authentication, and (optional) non-repudiation. It also handles all peer-to-peer and client-server applications, is designed for use with GSS-API, and is recommended for use in CORBA applications.

IETF RFC 2104 HMAC: Keyed-Hashing for Message Authentication

NIST - National Institute of Standards and Technology - through its Computer Security Resource Clearinghouse (CSRC) (see: http://csrc.nist.gov) is taking a leadership role in the development of a Federal Public Key Infrastructure (PKI) that supports digital signatures and other public key-enabled security services. NIST is coordinating with industry and technical groups such as the Federal PKI Steering Committee and its Technical Work Group (TWG) that has developed initial versions of a requirements document, a concept of operations, a technical security policy, an **X509 v3** certificate profile, and an interoperability report.

NIST, FIPS PUB 112 - Password Usage

NIST, FIPS PUB 196 - Entity Authentication Using Public Key Cryptography

PKCS #7 Cryptographic Message Syntax Standard, Version 1.5, November 1993, from RSA Laboratories - supports encryption and signature of arbitrary data, including support for multiple signatures. PKCS #7 is used as the basis for the S/MIME secure e-mail standard, S-HTTP, and the ANS X9.45 authorization certificate originator to encrypt a message and by the recipient to decrypt a message.

PKCS #11 Cryptoki B - A Cryptographic Token Interface

TCSEC - Trusted Computer System Evaluation Criteria ("The Orange Book") - DOD-5200.28 STD, U.S. Department of Defense - originally published in 1983, TCSEC provides categorization of security products by seven classes (from the lowest level D to the highest A1). A similar body exists in Europe (the European Information Technology Security Evaluation and Certification Scheme (ITSEC). Products are tested on identification and authentication, access control, accountability, audit, object reuse, accuracy, reliability of service, and data exchange.

United States Health Care Security Standards and Guidelines

Security standards and guidelines specific to health care information systems applications have also been developed by ANSI-accredited SDOs, such as ASTM, DICOM, HL7, and NCPDP and industry consortia such as the Object Management Group (CORBAsec and CORBAmed), American Medical Informatics

Association (AMIA), American Health Information Management Association (AHIMA), and the Computer-based Patient Record Institute (CPRI).

American Health Information Management Association (AHIMA) - (see: www.ahima.org) is the professional membership organization of health information management professionals. As the official custodians of medical records and health information within health care providers, health information management professionals have long focused on protecting the confidentiality of patient information. AHIMA has developed a number of Practice Briefs on:

- Authentication of Medical Record Entries
- Confidential Health Information and the Internet
- Destruction of Patient Health Information
- Disaster Planning for Health Information
- Disclosure of Health Information
- Electronic Signatures
- E-mail Security
- Facsimile Transmission of Health Information
- Managing Health Information Relating to Infection with HIV
- Managing Multimedia Medical Records
- Patient Anonymity
- Patient Photography, Videotaping, and Other Imaging
- Protecting Patient Information After a Closure
- Release of Information Laws and Regulations (by State)
- Release of Information for Marketing Purposes

American Medical Informatics Association (AMIA) - is a professional association intended to advance the public interest in medical informatics through charitable, scientific, literary, and educational activities. It promotes the development and application of medical informatics in the support of patient care, teaching, research, and health care administration. In 1997 it published *Guidelines on the Use of Electronic Mail with Patients***,** which provides communication, technical, and administrative and medicolegal guidelines on communicating with patients via e-mail.

ASTM, Committee E31 - Healthcare Informatics - includes subcommittees addressing privacy (E31.17) and data and system security (E31.20). These committees have produced the following standards:

ASTM E1762 - Standard Guide for Electronic Authentication of Health Care Information - Defines a document structure for use by electronic signature mechanisms; describes the characteristics of an electronic signature process; defines signature attributes for use with electronic signature mechanisms; describes acceptable electronic signature mechanisms and technologies; defines minimum requirements for user identification, access control, and other security requirements for electronic signatures; and outlines technical details for all electronic signature mechanisms in sufficient detail to allow interoperability between systems supporting the same signature mechanism.

ASTM E1869 - Standard Guide for Confidentiality, Privacy, Access and Data Security Principles for Health Information Including Computer Based Patient Records - This proposed standard works toward achieving consensus on the issues of confidentiality, access, and privacy of patient records; and recommends standards, policies, procedures, and other safeguards for computer-based patient records and the secondary databases that are related to the patient record. The goals are to recognize the patient's right to privacy, to preserve the confidentiality of the data, and to provide appropriate access.

ASTM E1902 - Standard Guide for the Management of the Confidentiality and Security of Dictation, Transcription, and Transcribed Health Records - This standard identifies the steps that must be taken to assure that dictation, transcription, and handling of the transcribed health records protect patient privacy.

ASTM PS100 - Provisional Standard Specification for Authentication of Healthcare Information Using Digital Signatures - This specification describes the use of digital signatures to provide authentication of health care information as described in ASTM E1762, Standard Guide for Authentication of Health Care Information. It includes specification of allowable signature and hash algorithms, management of public and private keys, and specific formats for keys, certificates, and signed health care documents.

ASTM PS101 - Provisional Standard Guidelines for a Technical Security Framework for Transmission and Storage of Healthcare Information - (As previously described under "Security Service Standards," this guidelines describes a framework for the protection of health care information both in storage and transmission.

ASTM PS102 - Provisional Standard Guide for Internet and Intranet Security - This guide describes security mechanisms that can be used to protect health care information which is being transmitted over networks using the Internet Protocol Suite (IPS). This includes the Internet as well as corporate intranets constructed from off-the-shelf components implementing these protocols. This standard describes relevant security standards and recommends, where needed, particular options such as cryptographic transformations to be used with the standards.

ASTM PS103 - Provisional Standard Guide for User Authentication and Authorization - This document describes mechanisms that may be used to authenticate users to computer systems as well as mechanisms to authorize particular actions by users. These actions may include access to health care information documents as well as specific operations on those documents. It addresses both centralized and distributed environments by defining the requirements that a single system must meet and the kinds of information which must be transmitted between systems to provide distributed authentication and authorization services.

ASTM PS105 - Provisional Standard Guide for Amendments to Health Information - This addresses the criteria for amending individually identifiable health information. Paper-based and computer-based amendments to health care records must have comparable methods, practices, and policies in order to ensure an unambiguous representation of the sequence and timing of documented events. Original and amended health information entries and documents must both be displayed, and must be consistent across both domains.

ASTM PS106 - Provisional Standard Specification for Security Audit and Disclosure Logs for Use in Health Information Systems - This draft standard identifies the data to be recorded in an audit log that serves to document and maintain a permanent record of all authorized and unauthorized access to confidential health care information so that providers and organizations and patients can retrieve evidence of that access to meet clinical, organization, risk management, and patient rights needs. The draft also describes the functionality needed for audit log management and the use of audit logs as tools by organizational managers.

ASTM PS107 - Provisional Standard for Information Access Privileges to Health Information - This document addresses the process of granting and maintaining access privileges to health information. It directly addresses maintenance of confidentiality of personal, provider, and organizational data in the health care domain. It addresses a wide range of data and data types, not all of which are traditionally defined as health care data. They are, however, elemental in the provision of data management, data services, and administrative and clinical health care services.

ASTM PS108 - Provisional Standard Guide for Individual Rights Regarding Health Information - This guide outlines the rights of individuals, both patients and providers, regarding health information and recommends procedures for the exercise of those rights.

ASTM PS109 - Provisional Standard Guide for the Training of Persons Who Have Access to Health Information - This standard addresses the privacy, confidentiality, and security training of employees, agents, and contractors who have access to health information.

ASTM Draft Standard Specification for Transmission of Healthcare Information Using Secure Messaging Protocols - This standard will describe the use of existing standard secure messaging protocols to convey health care information over store-and-forward communications networks (e.g., E-mail). The standard will address point-to-point transmission of health care information from a single originator to one or more recipients, and secure encapsulation of health care information and associated access control information that is used to determine which users can access the information. The standard is based on the S/MIME specifications produced by IETF.

ASTM Draft Standard Privilege Management Infrastructure - This standard will define interoperable mechanisms to manage privileges in a distributed environment.

Computer-based Patient Record Institute - CPRI was founded in 1992 as a result of recommendations in the Institute of Medicine patient record study report, *The Computer-based Patient Record: An Essential Technology for Health Care* (National Academy Press, 1991). The not-for-profit organization is committed to advancing improvements in health care quality, cost, and access through routine use of information technology. It has performed extensive work in the area of security for organizations using computer-based patient records:

CPRI - Glossary of Terms Related to Information Security - this is a compilation of terms and their referenced definitions that seek to establish consistency in use of contextually rich and complex terms associated with privacy, confidentiality, and security. The glossary provides context, demonstrates interrelationships among terms, and guides interpretation of terms. (See herein.)

CPRI - Guidelines for Electronic Signature Policies - provides guidance to developers and implementers of computer-based patient record systems relative to understanding the scope of electronic signature technologies and development and implementation of electronic signature policies. The work distinguishes between electronic signature as a broad class and digital signature as special type. (See herein.)

CPRI - Guidelines for Establishing Information Security Policies - based on the premise that computer-based patient records offer the potential for achieving greater protection of health information over paper-based patient records, this work introduces the concept of a complete information security program consisting of policies, standards, training, technical and procedural controls, risk assessment, auditing and monitoring, and assigned responsibility for management of the program. Information security policies are the basis for all other aspects of effective information security programs and this work facilitates the development of policies within an organization. (See herein.)

CPRI - Guidelines for Managing Information Security Programs - essentially a job description for an information security manager, this work fosters the recognition of the need to establish an organizational infrastructure to implement and maintain an information security program and serves as a reference document for information security management. (See herein.)

CPRI - Guidelines for Information Security Education Programs - provides a curriculum for an information security educational program for health care providers and suppliers, including goals and objectives, content outline, instructional methodologies, methods of program implementation, and evaluation guidance. (See herein.)

CPRI - Sample Confidentiality Statements and Agreements - fosters the recognition of the need for all employees, students, volunteers, physicians, and vendors who access information systems to sign confidentiality agreements, and provides model agreements that organizations can adopt for their own use. (See herein.)

CPRI - Security Features for Computer-based Patient Record Systems - essential a checklist for developers to ensure they have adequately incorporated security features in their product designs, for purchasers to use in specifying security requirements, and for auditors and consultants to use in evaluating the existence of security features in provider settings and supplier products. (See herein.)

Three State Health Information Planning Project - Three consortia – the Washington-based Foundation for Health Care Quality, the Minnesota Health Data Institute, and the Massachusetts Health Data Consortium – have joined together to address a security and risk management framework that reflects HIPAA, Joint Commission on Accreditation of Health Care Organizations, and other requirements. Backed by funding from The Robert Wood Johnson Foundation and the John A. Hartford Foundation, the three groups formed a technical advisory committee in 1997, then selected the San Diego-based technology company Science Applications International Corp. (SAIC) to assist them. Their report issued in June 1998, "Security and Risk Management for Business-to-Business Health Information Networks," enumerates a security policy and a technology plan to help organizations transfer information securely.

U.S. Department of Health and Human Services, Health Care Financing Administration - HCFA released its **Internet Security Policy on Authentication and Identification Procedures** in 1998 which provides policy and guidelines for the security and appropriate use of the Internet to transmit HCFA Privacy Act-protected and other sensitive HCFA information (see Chapter Four)

International General Security Standards

ISO/IEC has developed a Security Architecture and promulgated a number of security protocols for use at various layers. Figure 5 provides a summary of how security services are allocated to the OSI layers in the ISO 7498.2 framework for security architecture.

Allocation of Security Services to OSI Layers per ISO 7498.2 Framework for a Security Architecture

	OSI Reference Model Layer						
Security Service	1 Physical	2 DataLink	3 Network	4 Transport	5 Session	6 Presentation	7 Application
Peer entity authentication			Y	Y			Y
Data origin authentication			Y	Y			Y
Access control service			Y	Y			Y
Connection confidentiality	Y	Y	Y	Y		Y	Y
Connectionless confidentiality		Y	Y	Y		Y	Y
Selective field confidentiality						Y	Y
Traffic flow confidentiality	Y		Y				Y
Connection integrity w/recovery				Y			Y
Connection integrity wo/recovery			Y	Y			Y
Selective field connection integrity							Y
Connectionless integrity			Y	Y			Y

Selective field connectionless integrity							Y
Nonrepudiation of origin							Y
Nonrepudiation of delivery							Y

Other applicable ISO/IEC standards include:

- **ISO/IEC 9798-1: Information Technology - Security Techniques-Entity Authentication Mechanisms - Part 1: General Model**
- **ISO/IEC 9798-2: Information Technology - Security Techniques-Entity Authentication Mechanisms - Part 2: Entity Authentication Using Asymmetric Techniques**
- **ISO/IEC 10164-4 Information Technology - Open Systems Connection - System Management: Alarm Reporting Function**
- **ISO/IEC 10164-5 Information Technology - Open Systems Connection - System Management: Event Report Management Function**
- **ISO/IEC 10164-7 Information Technology - Open Systems Connection - System Management: Security Alarm Reporting Function**
- **ISO/IEC 10164-8 Information Technology - Open Systems Connection - System Management: Security Audit Trail Function**
- **ISO/IEC 10164-9 Information Technology - Open Systems Connection - System Management: Objects and Attributes for Access Control**
- **ISO/IEC 10181-2 Information Technology - Security Frameworks in Open Systems - Authentication Framework**
- **ISO/IEC 10181-3 Information Technology - Security Frameworks in Open Systems - Access Control Framework**
- **ISO/IEC 10181-4 Information Technology - Security Frameworks in Open Systems - Non-repudiation Framework**
- **ISO/IEC 10181-5 Information Technology - Security Frameworks in Open Systems - Confidentiality Framework**
- **ISO/IEC 10181-7 Information Technology - Security Frameworks in Open Systems - Security Audit Framework**
- **ISO/IEC 10736 Information Technology - Telecommunications and Information Exchange Between Systems - Transport Layer Security Protocol (TLSP)**
- **ISO/IEC 11577 Information Technology - Telecommunications and Information Exchange Between Systems - Network Layer Security Protocol (NLSP)**

Other International Security Standards Efforts

A new international standard for evaluating the security features of computer products has been developed through ISO. The *Common Criteria for Information Technology Security Evaluation* (ISO FDIS 15408) is in final draft stage and is expected to be published as an ISO standard in spring 1999. The Common Criteria builds upon previously developed security evaluation criteria for health information technology of the U.S. (Trusted Computer System Evaluation Criteria [TCSEC], "The Orange Book," U.S. Department of Defense, 1985), Canada, and some members of the European Union. The Common Criteria are based on three major components: The Protection Profile, which is a statement of security needs for information technology products; The Security Target, which is a statement of security claims for a particular information technology security product or system; and a combination of security requirement components (see: http://csrc.nist.gov/cc).

The European committee for standardization Technical Committee 251 - Medical Informatics (CEN TC251) (see: www.centc251.org) has a working group on security, privacy, quality, and safety. A pre-standard on Security Categorization and Protection of Healthcare Information Systems (COMPUSEC) and a digital signature standard have been developed.

In July 1995, the European Union's Council of Ministers adopted the "Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data." The

European Privacy Directive, as it became known, became effective October 25, 1998. U.S. businesses are expected to understand the Directive in order to provide the means in their systems to comply, if they are selling abroad. The Department of Commerce is working with the European Union to define a "safe harbor" approach for American companies that would require them to self-certify that they are in compliance with the Directive.

Standards development organizations and governmental entities in Japan, Singapore, Australia, and New Zealand are also currently developing standards to insure the security, confidentiality, and privacy of health care data as it resides in systems or as it is being passed in message transactions between systems.

Updates, Additions, and Corrections to this Work

This work was developed in January 1999 and reflects what is believed to be the most current information on security standards and other related documents. Standards development, however, is an ongoing process. Updates, additions, and corrections to this work are most welcome and should be addressed to the Computer-based Patient Record Institute (www.cpri.org).

Margret Amatayakul, MBA, RRA, a health information management professional and former executive director of the Computer-based Patient Record Institute, compiled this work. She may be contacted through margretcpr@aol.com

Toolkit Section 3.7

JCAHO/NCQA Recommendations

Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment

By the Joint Commission on the Accreditation of Healthcare Organizations and the National Committee on Quality Assurance

Developed with generous support from the W.K. Kellogg Foundation and the Agency for Health Care Policy and Research

Executive Summary

One of the touchstones of our health system is the deep trust that patients place in their providers. Patients entrust to their doctors information they share with few other human beings. They know that this openness and honesty is essential to obtaining appropriate and effective health care. Increasingly, however, some patients may pause before sharing certain information with their providers. They may wonder who in addition to their doctor will become privy to highly personal details. They are aware that some of their information must be shared with unknown individuals who handle reimbursement insurance and quality of care issues. However, they may wonder who else has access to their information, or how well is its privacy protected when transmitted electronically among these parties. To the extent that individuals needing health care withhold vital information because of these fears, potential complications could arise in relation to their treatment, and their very lives could be endangered.

Today's uncertainty about access to personal health information is sustained by the lack of consistent policies and practices for protecting the confidentiality of personal health data. Fair information practices that define individual rights and protections for other types of personal information, such as financial data, are not formally and uniformly applied to personal health information. Most stakeholders-provider organizations, practitioners, health plans, deliverers of specialty services (carve-out providers), claims administrators, and others-are generally committed to protecting the confidentiality of personal health information. In one form or another, all have policies and practices intended to protect confidential information. However, each group is left to its own best judgment as to the policies adopted and how they are applied when facing numerous demands for sharing sensitive information in order to accomplish routine management tasks related to oversight of care, reimbursement, utilization review, disease prevention, and resource management. Unfortunately, the framework or standards against which to evaluate these practices is often missing.

NCQA and JCAHO believe that concerns about confidentiality of personal health information seriously threaten the quality of health care. As accrediting organizations, NCQA and JCAHO believe that they can contribute to the development of a common framework to guide the protection of personal health information. Recognizing the societal importance of sharing personal health data in certain circumstances, this joint effort focused on the nature of the special concerns, problems, and strategies for addressing patient confidentiality issues in today's complex health care environment, where managed care organizations (MCOs), providers, employers, oversight organizations, regulators, and researchers require increased access to personal health information.

This paper presents an overview of the issues that were considered through the NCQA/JCAHO joint project, and identifies actions that can be taken to address the confidentiality of personal health information. This report is intended to inform legislators, policy makers, managed care plans, providers, and the public. Funding for this project was received from the W.K. Kellogg Foundation and AHCPR in the Dept. of Health and Human Services.

NCQA and JCAHO have incorporated requirements for the protection of patient information into their standards and practices for evaluating health care organizations. Today's accreditation standards address requirements for health organizations to: obtain patient consent for release of information; treat patient medical records as confidential; incorporate confidentiality requirements into contractual agreements with third parties; and inform patients of their rights regarding access to their medical record information. The accreditation review process also includes a contractual agreement that holds reviewers accountable for the confidential treatment of any patient data that is accessed during a review. As a result of the issues addressed and the recommendations developed in this report, NCQA and JCAHO will consider

where these recommendations extend beyond current standards and practices and how they might influence modifications to their accreditation standards.

Throughout the health care system, among legislators, and across the general public there is consensus on the need to improve the protection of the confidentiality of personal health information. The recommendations presented in this report are a starting point to enable all participants to evaluate their policies and procedures and move forward with increased protections. Many of the actions described in this report can be implemented in a near-term timeframe and will significantly improve the protection of personal health information. The recommendations are divided into six major areas:

- Ensuring accountability
- Dealing with consent in an evolving health care delivery and financing system
- Educating about policies, practices, rights, and responsibilities
- Using technology as a solution
- Providing legislative support
- Guiding research

Recommendations

The recommendations present the positions of NCQA and JCAHO. They are derived from discussions during work sessions convened with numerous experts on this topic. However, they do not represent a consensus of the participants from those sessions, nor should they be attributed to any member or groups of members who participated in this project.

Ensuring Accountability

Managed Care Organizations (MCOs) should have clearly defined policies and procedures for dealing with confidentiality issues. The MCO policies and procedures should be built upon an understanding of stakeholders' views and values.

Accountability is enhanced by having focal points who are responsible for assessing compliance with policies and procedures, and addressing new requests for data-for example, a security officer and a data disclosure board.

MCOs should have a program of periodic audits to ensure compliance by staff and contractors with MCO policies and procedures. Audits should also include a determination of the accuracy of personally identifiable health data and should determine the rate, type, and source of errors.

All contracts, carve-outs and carve-ins should be held to the same standard of accountability as the MCO. If an MCO shares patient data with these parties, such as for managed behavioral health care services, access to personally identifiable data for the patient's care by those services should be provided as needed. Accountability should be on (1) the MCO and (2) the contracted provider, so that protections are in place to allow access only by the appropriate caregiver.

Oversight organizations, including accrediting bodies, states, and Federal agencies, should include in their contracts terms that describe their responsibility to maintain the confidentiality of any personally identifiable health information that they review. To the extent possible, these organizations should minimize their access to personally identifiable health information. Aggregated and/or deidentified data should be used whenever feasible.

MCOs must verify that personally identifiable health information shared with external organizations is used only for the purposes that were specified in the patient's consent, and that the external organization will comply with the MCO's policies.

There must not be any commercialization of patient identifiable information by MCOs or any organization handling patient data, without specific patient consent for this purpose.

Licensed, independent practitioners responsible for direct patient care should have access to all relevant personal health information on the patients they are treating.

As part of their assessment of managed care organizations competing for their business, employers should include requirements for the protection of personally identifiable health information. These criteria should also be incorporated into employer and other purchaser contracts with MCOs and applied in monitoring the performance of a managed care organization.

Employers should not have access to personally identifiable health information about their employees without consent or unless mandated by law. MCOs should not share personally identifiable

health information with employers without consent. Self-insured employers should adopt technical and operational practices that protect personally identifiable health information from unauthorized access and meet the same standards of protection as required for MCOs.

Dealing with Consent in an Evolving Health Care Delivery and Financing System

Use of an individual's personally identifiable health information for any purpose must be authorized by a clear and specific consent provided by the patient unless the release of the information is required by law. Consents should be truly informed, specific, and voluntary. The language of the consent must be written in a manner that can be understood by the patient. Consents should specify the information to be shared, with whom, and for what purposes it will be used.

Providers and MCOs should have policies and procedures that can alert them to the need to reobtain patient consent.

Educating about Policies, Practices, Rights, and Responsibilities

MCOs should provide their members with a detailed understanding of what personally identifiable health information is maintained, how it is kept, how it is used, who has access to it for clinical, reimbursement, or for quality oversight purposes, and any releases of information that are required by law. MCOs should make their policies and procedures known at the time of marketing and enrollment and reinforce them at the time of care delivery. These efforts should be continuous and multi-pronged.

Practitioners and provider organizations should inform patients of their rights and responsibilities regarding the confidentiality of their information at the time of their initial encounter. This should be reaffirmed at other appropriate intervals, such as when there is a significant change in health status or in the use of their personal health information.

MCOs should inform their members of their rights to review and comment about their personal health information and to review transaction logs that record accesses and/or changes to their personally identifiable health information.

MCOs should routinely provide training to their employees and contracted providers on how to be sensitive to confidentiality concerns and how to comply with confidentiality policies.

Using Technology as a Solution

As MCOs acquire information systems, they should require capabilities that provide a high level of security and confidentiality protection, including encryption, detailed user access controls, transaction logs, and blinded files

MCOs and providers should leverage the sophistication of technology to solve special privacy issues, such as restricted access. Existing technology can set levels of authorization for access to patient data according to the role the user plays in a patient's care.

MCOs should maintain and routinely analyze records of all accesses and/or modifications to personal health information. Modifications or changes to data should be disseminated in a timely way to all other legitimate users to ensure data accuracy. To the extent possible, this tracking should be incorporated into computerized systems.

Providing Legislative Support

Federal and State legislation should strive to provide consistency across jurisdictions: at minimum, in all areas germane to patients' rights. States should have the flexibility to implement Federal protections through regulations that address special considerations in their jurisdictions.

Legislation should provide equally high levels of confidentiality protection for all personally identifiable health information.

State and Federal penalties for misuse that are meaningful deterrents should be designed and enacted in a way that is relevant to and reinforced by today's level of technical uses and capabilities.

Legislation should mandate that law enforcement officials must provide evidence of credible and compelling need for access to personally identifiable health information. Federal law should protect as confidential any quality improvement or risk-reduction information gathering done in response to a requirement by an accrediting or oversight body as part of its oversight activities.

In the absence of specific legislation, MCOs should have policies and procedures for determining when patient information should be turned over to law enforcement officials and conditions for doing so.

Guiding Research

When MCOs disclose personally identifiable health information to health service researchers, they should ensure that the intended research has had appropriate reviews for, and contains necessary controls to protect the confidentiality of the patient.

When MCOs share personally identifiable health information with researchers for record review or data linkages, anonymizing protections such as encryption and or de-identification techniques should be used whenever possible. Designated security/privacy personnel should protect any "keys" and these keys should be destroyed as soon as possible.

When MCOs agree to share identifiable information with researchers, they should include in their contracts or collaborative agreements, penalties for any unauthorized use or disclosure of the data.

The research community, in collaboration with DHHS, should develop principles to guide Institutional Review Boards (IRBs) when approving the use of personally identifiable health information. These principles should be used consistently across IRDs.

Introduction

Changes in the regulatory and legal environments, the security risks of distributed networks and systems, especially the Internet, ever-changing information technology, and rising patient expectations all require health care organizations to continuously update their data security policies, procedures, and practices. A security team must take primary responsibility for coordinating this effort through careful risk analysis, security policy review, and technical and operational enhancements. The security team's efforts will fail, however, without strong business and clinical leadership within the organization. Even if key leaders accept responsibility for maintaining the confidentiality of patient identifiable information, staff will probably resist taking on new tasks that further complicate their work and compete with current tasks. The security team should recognize that enhancing the organization's security capability requires transforming institutional resistance into a mission-based, mobilized security effort. A security team that neglects building support for its efforts risks failure.

This chapter includes discussions, CPRI guidelines, sample documents and case studies illustrating issues in establishing a health information security program. As a healthcare organization builds its security effort, it must develop and enforce security policies, conduct risk analyses, stage employee training sessions, assign roles and responsibilities for information security and deploy security technology. Sample material from the American Health Information Management Association, Kaiser Permanente of Northern California, Partners HealthCare System, Harvard Vanguard Medical Associates and several NLM-funded sites provide rich resources to help sustain this important effort. A special section explains regulations and approaches to using the Internet in transmitting healthcare information.

Developing Security Policies

Establishing comprehensive, detailed security policies constitutes the cornerstone of good information security practice. Security policies guide an organization's appropriate use of data and explain security risks and sanctions to employees. Although healthcare organizations must all comply with a common set of federal regulations, no two security policies will be the same because of variations in mission, business practices and local regulations. Indeed, as the HIPAA regulations emphasize, each organization must exercise administrative judgement in building its information security policies, an opportunity that poses challenges as well as creates flexibility. Information security policies must begin at the enterprise level. When programs pose special risks, however, an organization should examine the necessity of developing local security policies to manage the novel risks. Because security risks, technologies, and organizational missions change, security managers, in collaboration with senior management and representative users, should regularly review and update security policies.

CPRI has produced a document entitled "Guidelines for Establishing Information Security Policies" that outlines steps organizations can take to establish their confidentiality and security policies. It describes the following subject areas that should be included in any policy:

1. Philosophy for the Protection of Information
2. Patient Rights with Respect to Information Security
3. Protection of Caregiver Information
4. The Privileges and Obligations of Researchers
5. The Rights of Society
6. Collection of Information
7. Retention and Destruction
8. Information Security Program
9. Accountability and Responsibilities
10. Access to Information
11. Classification of Information
12. Records of Access
13. Disaster Recovery/Business Resumption Plans
14. Information Security Awareness Training
15. Monitoring and Auditing

According to the Guidelines, security policies should have the following general characteristics:

1. Originate from the highest level of an organization
2. Apply to all employees, independent contractors, and agents throughout all units of the organization
3. Cover the following types of information: patient health, patient demographics, patient financial, research, clinician, peer review, payer, business records, and computer software
4. Cover uses of information for all of the following activities: patient care, public health, quality of care, management, research, payment, insurance eligibility, and any other relevant purpose
5. Apply to all information regardless of its form or storage media

Comply with all legal, industry, and professional requirements

Reconciling European and American Approaches to Privacy
Toolkit Section 3.8

Jeff Collmann, Ph.D.
Georgetown University

The European Privacy Directive (the Directive) threatens the flow of personal information and jeopardizes business transactions of many types (particularly so-called "business to business" transactions) from European Union member states to the United States. The United States has reason to worry. Its privacy regime differs substantially from European approaches. The terms of the Directive fail, moreover, either to match the reality of information flows or the development of information technology (Swire and Liton 1998). Representatives of the European Union and the United States Department of Commerce have entered into negotiations about the terms of a "Safe Harbor" Agreement that potentially provides a means to avoid these undesirable consequences. Negotiations about details of language continue with controversy and areas of disagreement remaining between the EU and the USA representatives as well as among US commentaries on the draft agreement.

Passed on October 28, 1995 and taking effect on October 28, 1998, the Directive seeks to promote the free flow of personal information within the European Union while assuring a common, high level of privacy protection. The Directive also seeks to prevent the flow of personal information from the EU to third countries lacking "adequate" privacy protection. Implementation of these lofty goals, particularly with respect to transfers to third countries such as the United States of America poses interesting questions for reflection on the privacy issue as well as troubling problems for international social policy. Personal information transfers underpin many routine business transactions. Hence, while the Directive appears to focus its attention on protection of individual citizens or employees in Europe, many of its consequences affect European and international enterprises. "Business to business" transactions question the boundaries between an individual's private and public identities. The Directive expresses an expectation that third countries would change their privacy regimes better to conform with European assumptions thus joining other questions such as human rights and genetically engineered products in the list of social issues linked to trade and national sovereignty in international discourse. The "Safe Harbor" negotiations may create conditions maintaining flows of personal information from the EU to the USA but leave many of these broader questions open for continued debate. We may thus achieve an instrumental but not a cultural reconciliation of European and American approaches to privacy.

Requirements for EU Members

The Directive applies to "personal data", a general category covering information about individual natural human beings without regard to the sector of its use. "Personal data" includes information relating to an identified or identifiable natural person ("data subject"), using direct or indirect means such as an identification number or one or more factors specific to the data subject's physical, physiological, mental, economic, cultural

or social identity. This definition intends to cover all "reasonable and likely" means of identifying an individual including advanced statistical methods that are making identifying an individual easier and easier with less and less information[i]. The Directive applies to processing of personal data primarily using automated means. It applies to manual means if used in a structured filing system that allows easy access to personal data. The Directive does not apply to personal data under several conditions including, for data rendered anonymous, for uses by purely domestic or personal purposes by a natural person, for activities outside the scope of EU law and for processing related to EU Members' public security, state security, defense or criminal law.

For American businesses, the Directive's provisions about processing and reprocessing data pose among the most rigorous and difficult of conditions. Processing may occur only if the following conditions have been met, including:

1. data processing must be "adequate, relevant and not excessive" with respect to purposes of the processing;
2. purposes of processing must be explicit, legitimate and determined at the time of processing;
3. strict limitations imposed on reprocessing of data for purposes incompatible with original purposes, but;
4. reprocessing permitted for historical, scientific or statistical purposes if not used in measures or decisions regarding the data subject.

Moreover, processing of personal data may occur only with the permission of the data subject except under the following circumstances, including:

1. when necessary to conclude or perform a contract in the interests of the data subject;
2. in case of a legal requirement;
3. when required by a task in the public interest or by an official authority;
4. when in the legitimate interests of a natural person if not overridden by data subject's rights and freedoms, or;
5. when necessary to protect an interest "essential for the data subject's life".

The Directive prohibits the processing of "sensitive personal data" that is, information "capable by (its) very nature of infringing upon fundamental freedoms or privacy" such as racial or ethnic origin, political opinions, religious beliefs or philosophical beliefs, trade union membership, health or sex life. Exceptions to this prohibition include the following conditions, namely:

1. with explicit consent of data subject;
2. when authorized in employment law as part of controller's rights;
3. when necessary to protect incapable subject's vital interests;
4. with regard to an association's own members or regular contacts;
5. data already made public by the data subject or in legal claim;
6. in health care when subject to professional/ legal obligation of secrecy;
7. when required by important interests of Member States' public interest, or;
8. in exercise of journalistic or literary freedom of expression.

The Directive creates rights for Europeans that few Americans take for granted with respect to use of personal data. Data subjects have the following rights with respect to processing of personal data about themselves, namely the right to:

1. know the controller, purpose, types and proposed recipient;
2. gain access to the data to verify its truth and legality;
3. know the "logic" of automated processing;
4. rectify, erase or block processing of inaccurate data;
5. object to processing of data, especially for marketing purposes;
6. not be subject to decisions based on automated data processing;
7. have access to judicial remedy for failure to respect their privacy rights.

The Directive creates obligations for controllers (the natural or legal person or agency that determines the purposes and means of data processing) and processors (the natural or legal person or agency processing data on controller's behalf) in the EU incumbent upon few American counterparts. These include requirements for controllers to notify supervisory authorities of data processing, for processors to act only upon instructions from controllers, and for both controllers and processors to adopt technical and organizational safeguards for data security. [ii] European Member States must identify and examine risky data processing operations and publicize information about processing operations within their individual jurisdictions.

Transfer of Personal Data to Non-EU Countries

EU member states must meet two basic conditions before authorizing transfer of personal data to countries outside its boundaries. They must determine that the country in which the proposed recipient resides maintains "adequate" safeguards for the privacy of personal data. Or, they must determine that at least one of a set of "derogations" listed in Article 26 applies to the specific transfer under consideration. Preliminary drafts of the Directive required non-EU countries to maintain "equivalent" privacy safeguards; but, the less stringent if ambiguous "adequacy" language now governs personal data transfers out of Europe. How shall Member States assess "adequacy"? Article 25 states that "adequacy" of privacy protection shall be assessed "in light of all the circumstances surrounding a single or set of data transfers such as the nature of the data, the purpose and duration of the data processing operations, the country of origin, the country of final destination, and the general and sectoral rules of law as well the professional rules and security measures effective in third country. The Directive provides for findings of adequacy or inadequacy. When a finding of inadequacy occurs, the Directive permits EU Member States to take measures preventing data transfers and/or to begin negotiations to remedy the adverse finding. As explained below, the United States could reasonably expect a finding of "inadequacy" with respect to its privacy safeguards. Negotiations to create a "Safe Harbor" agreement to avoid the consequences of such a finding have been underway for several years.

Article 26 permits transfers of personal data to third countries with "inadequate" privacy safeguards under certain stringent conditions, including:

1. unambiguous consent of the data subject;
2. performance of a contract between data subject and controller;

3. execution precontractual measures at data subject's request;
4. performance of contract in data subject's interest;
5. legally required for public interest or defense of legal claims;
6. protect the vital interests of data subject;
7. information exists in public registry;
8. adequate specific safeguards such as contractual clauses assuring protection.

For many reasons, the EU does not encourage third countries to rely on the derogations contained in Article 26 as a standard approach to receiving approval for data transfers. Controversy particularly exists about the utility of "contractual clauses" in obtaining adequacy findings. While the provision clearly exists in Article 26, the EU has acknowledged its willingness to permit only sparing use of contractual solutions.

Why the United States should be worried?

Transactions in personal data lie deeply embedded in business and trade between EU Member States and the United States of America. As Swire and Linton (1998) make clear, global corporations move personal data all over the world in the course of their business ranging from trade transactions, to clinical and pharmaceutical research, to routine human resource management. A finding of inadequacy jeopardizes all these transactions when personal data must flow from the EU to the United States. The US faces a finding of inadequacy for many reasons, including a sectoral not comprehensive approach to privacy rule making, a reputation for fragmented, capricious and inadequate privacy practices that frequently do not meet EU requirements. Moreover, as Swire and Linton (1998) explain, the EU Directive poses major problems of interpretation when applied to the United States. The assumptions of the Directive do not match the real world of data transactions and emerging information technology. The Directive's language contains important ambiguities and EU authorities do not always agree on the relative importance of various mechanisms of compliance such as self-regulation and contractual clauses.

US Sectoral Privacy Rules: The United States historically approaches privacy on a sector by sector basis instead of comprehensively as in the Directive's provisions for personal data. The US has federal laws covering privacy for federal agencies and credit. Much American privacy legislation exists at the state level providing for variable and inconsistent protections. From the perspective of the Directive, US sectoral approaches permit if not encourage privacy-related laws in one sector to undermine laws in other sectors as almost happened with respect to medical privacy during 1999 federal banking legislation.

Fragmented and capricious practices: The US has a dubious reputation for privacy approaches that provide harsh punishment for disclosure of video rental lists but not of individual health care information. Europeans find particularly distasteful American practices of disclosing and selling personal data to third parties for marketing and other "incompatible" uses such as CVS pharmacy providing information to a pharmaceutical company about patients' prescriptions. American data security policies, procedures and practices range widely from good (banking) to poor (health care).

US regime does not meet basic EU requirements: Some US industries could present themselves as compliant with the basic privacy practices enshrined in the Directive but not many. Americans rarely receive clear explanations of how personal data they surrender to commercial, service or government organizations might be used. Current practices in health care, for example, ask patients to permit release of information for treatment and payment. Few patients understand the scope of that permission let alone know the range or purposes of enterprises that will receive data under their authorization. American data subjects also have few ways of determining if companies surrender or process an "adequate, relevant and not excessive" amount of information. Reprocessing and selling personal data for purposes "incompatible with the original purpose" seems a fact of life in some industries with such practices receiving unfavorable scrutiny only recently in others. The debate about medical privacy has raised the question of reuse of personal health data for epidemiological analysis and public health. Controversy exists demonstrating a general lack of awareness and consensus about this issue in the USA.

Assumptions of Directive do not match real world: Swire and Linton (1998) make a compelling case that the Directive assumes a world dominated by main frame or client-server network architectures and person to business transaction. Terms such as "controller" imply fixed, easily identifiable points of authority. In a web-enabled Internet world, however, users may not know who operates or the "location" in real space of a particular web-site's "controller". Holding such obscurely placed individuals accountable for their privacy practices poses difficult logistical to say nothing of genuine legal problems. Moreover, laptop technology makes everybody more mobile users and controllers as well as processors. In the course of one business trip, personal data on a laptop hard disk may cross borders between EU and non-EU countries many times. The Directive also focuses on the rights of "natural persons" envisioning individuals in their private capacity as consumers in an information exchange. The vast majority of transactions entailing use of personal data, however, occur in business to business exchanges. Privacy laws may increase consumer confidence in certain types of electronic transaction. Their relevance to business-to-to business transactions is more questionable.

Intrinsic ambiguities of the Directive: The language of the Directive, particularly in Article 26: Derogations, leaves much room for interpretation and debate. Basic terms such as "unambiguous consent," "in the interest of the data subject", or "necessary for the conclusion of a contract" pose difficulties when examined from an implementation perspective. Disagreement potentially exists about the breadth of such terms and their relevance to particular situations.

Dispute over mechanisms of compliance: As mentioned above, disagreement exists over the relative importance and efficacy of certain mechanisms such as the "contract clause" and "self-regulation". Given the background of concern about US privacy practices, in particular, one might expect caution in depending on mechanisms that rely on self-policing. The Safe Harbor negotiations between US and EU representatives center on terms for establishing a privacy regime for handling personal data from the EU that

depends on practices of self-regulation coupled with enforcement powers in US trade law.

The Safe Harbor Negotiations

The Safe Harbor negotiations seek to create an agreement to which companies could comply as a means of achieving a presumption of "adequacy" in their privacy practices and thus maintain flows of personal data from EU Member States to the USA. Ambassador David L. Aaron, Department of Commerce, negotiates on behalf of the USA. The latest draft of the Safe Harbor agreement was released on November 15, 1999. Consult the World Wide Web (http://www.ita.doc.gov/ecom/Principles1199.htm) to view the latest and all previous drafts with FAQ and public comments. Adherence to the Safe Harbor Agreement once adopted will be voluntary and does not preclude using other mechanisms. In all cases, organizations will self-certify to the Department of Commerce who will maintain a list of participating organizations. Organizations may qualify for the Safe Harbor in many ways, including a self regulatory privacy program, developing their own policies that comply with the Principles, adhering to relevant statutory, regulatory or administrative law or possibly including the Principles in contracts per Article 26[iii]. When relying on self-regulations, failures to comply must be actionable under Section 5 of the Federal Trade Commission Act that outlaws unfair and deceptive acts or other similar acts. Organizations benefit from safe harbor beginning upon the date of self-certification and must apply the Principles to all covered information from that date. The terms of the agreement include both the Principles and the FAQ. The Department of Commerce will encourage organizations to participate in the Safe Harbor because it provides speedier transfer, lighter administrative burdens and greater legal certainty than alternatives.

Debate continues over details of language but seven topics have remained constant as the focus of discussion, namely Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement. Please note: the principles of Notice, Choice, Onward Transfer and Data Integrity focus particularly on the reuse and/or disclosure of personal data for purposes other than or incompatible with the original purpose of collection. The following bullets summarize not reproduce the proposed text.

1. Notice: organizations must inform individuals about purposes for collection and use of personal data, how to contact the organization and types of third parties to whom it discloses information. When using or disclosing personal data for a purpose other than that for which it was originally collected, the organization must explain data subject's choices and means for limiting such uses and disclosures.
2. Choice: When a use or disclosure is incompatible with purpose of original collection, data subjects have the right to opt out of such disclosure or use. Data subjects must choose to opt in for such uses of sensitive personal data.
3. Onward Transfer: An organization may only disclose personal data to third parties consistent with the principles of Notice and Choice.
4. Security: Organizations must take reasonable precautions to protect personal information in their control from loss, misuse and unauthorized access, disclosure, alteration and destruction.

5. Data Integrity: Consistent with the principles, an organization may not process personal information for purposes incompatible with original purposes. Organizations must also take reasonable steps to ensure the data's reliability.
6. Access: Individual should have access to inspect and correct, amend or delete inaccurate information except where burden or expenses would be disproportionate to risks to individual's privacy.
7. Enforcement: Effective privacy protection should include mechanism for assuring compliance, recourse for affected individuals in cases of non-compliance, and consequences for non-compliant organizations.

Negotiations are continuing on the precise text of the Safe Harbor Agreement.

Conclusion

The Safe Harbor negotiations cannot necessarily nor do they claim to reconcile basic differences in the European and American approaches to privacy. Indeed, the text overtly limits the Safe Harbor language to the task at hand, developing ways to permit continuing flow of data from the EU to the US with privacy protections that meet the European "adequacy standard". Developments in some arenas are pushing American privacy protections closer to the Safe Harbor and Directive's requirements. Proposed medical privacy rules under HIPAA, for example, would limit reuse and disclosure of personal health information in ways echoing the Notice, Choice, Onward Transfer, Data Integrity, and Access principles. Proposed HIPAA data security rules would have a similar effect for the Security Principle. The sectoral approach nonetheless seems well entrenched in American culture; but, as Swire and Linton observed, the development of the Internet may force Europeans and Americans to rethink their basic privacy assumptions.

---

[i] The definition of "reasonable and likely" varies with the sophistication of the data processor in draft rules for medical privacy recently proposed by the United Sates Department of Health and Human Services.

[ii] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the United States Department of Health and Human Services to establish regulations concerning data security in electronic patient records systems. Although proposed rules now exist with final rules expected by summer 2000, they will affect only personal data in the health care sector, not all sectors processing personal data as assumed by the Directive.

[iii] As of November 15, 1999, the EU had still not agreed to use of principles in model contracts.

Guidelines
For
Establishing Information Security Policies
At
Organizations Using Computer-based Patient Record System

Prepared by
CPRI Work Group on
Confidentiality, Privacy & Security

February 1995

Computer-based Patient Record Institute
Advancing health care through information technology

Guidelines
For
Establishing Information Security Policies
At
Organizations Using Computer-based Patient Record System

Prepared by
CPRI Work Group on
Confidentiality, Privacy & Security

February 1995

Computer-based Patient Record Institute
Advancing health care through information technology

Computer-based Patient Record Institute
Advancing health care through information technology

Guidelines for Establishing Information Security Policies
At Organizations Using Computer-based Patient Records

© Copyright 1995, by the Computer-based Patient Record Institute. All rights reserved.

No part of this publication may be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without permission in writing from the publisher.

Printed in the United States of America

This book was prepared camera-ready.

Guidelines for Establishing Information Security Policies at Organizations with Computer-based Patient Record Systems

Overview

The Computer-based Patient Record Institute (CPRI) has recognized the importance of providing for information security in the implementation of computer based patient records. Therefore, the Work Group on Confidentiality, Privacy, and Security was established as one of the four original work groups of the CPRI. This work group was chartered to encourage the creation of policies and mechanisms to protect patient and caregiver privacy and ensure information security. It is developing a series of security guidelines for organizations implementing computer-based patient record (CPR) systems.

The first in the series is this:

- *Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Record Systems*

The remaining guidelines will address:

- Information security education programs.
- Information security manager responsibilities and procedures.
- Methods to identify and authorize access to computer-based patient record systems.
- Assignment and control of user access identifiers.
- Security audit functions and processes.
- Application and system security functions.

Need for Security Guidelines

Computer-based patient records (CPRs) offer the potential for achieving greater protection of health information over paper-based patient records. However, to ensure an appropriate and consistent level of information security for computer-based patient records, both within the individual health care organizations and throughout the entire health care delivery system, formal information security programs must be established by each organization entrusted with health care information. The first component of an information security program is information security policies which incorporate all applicable laws and regulations, but which are designed by the organization to meet specific needs.

A complete information security program consists of policies, standards, training, technical and procedural controls, risk assessment, auditing and monitoring, and assigned responsibility for of the program. Information security policies are the basis for all other aspects of effective information security programs.

Acknowledgments

This document was prepared by members of the Work Group on Confidentiality, Privacy, and Security, Kathleen Frawley and Dale W. Miller, Co-Chairs. The co-chairs are indebted to the many volunteers who participated in the work group meetings, provided input, and prepared and reviewed the drafts of this document.

Table of Contents

Overview iii

Acknowledgments iv

Introduction 1

The Need For Security Policies 1

Objectives 2

Scope 2

Relationship to Legal and Regulatory Requirements 3

Distribution and Promulgation 3

Policy Subjects 4

- Philosophy for the Protection of Information 4
- Patient Rights with Respect to Information Security 4
- Protection of Caregiver Information 5
- The Privileges and Obligations of Researcher 6
- The Rights of Society 7
- Collection of Information 7
- Retention and Destruction 8
- Information Security Program 8
- Accountability and Responsibilities 8
- Access to Information 9
- Classification of Information 9
- Records of Access 10
- Disaster Recovery/Business Resumption Plans 10
- Information Security Awareness Training 10
- Monitoring and Auditing 10

Suggested Method for Policy Development 10

References 11

Glossary 13

Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Record Systems

Introduction

Computer-based patient records (CPRs) offer the potential for achieving greater protection of health information over paper-based patient records. However, *to* ensure an appropriate and consistent level of information security for computer-based patient records, both within the individual health care organization and throughout the entire health care delivery system, formal information security programs must be established by each organization entrusted with health care information. The first component of an information security program is information security policies which incorporate all applicable laws and regulations, but which are designed by the organization *to* meet specific needs.

The Need for Security Policies

In order to receive and pay for health care, people entrust health care providers with private information. Most people believe and expect that the privacy and integrity of health information will be preserved by all who use and maintain that information. Every organization, which creates, uses, stores, and communicates health care information, has a legal and ethical responsibility to honor this trust. Organizations are also required to protect sensitive and private records about physicians, nurses, staff members and employees, and other caregivers. These obligations and responsibilities to protect information must be considered and fulfilled the implementation of computer-based patient records.

Public policy, laws, accrediting and regulatory requirements, and patient expectations require a certain standard for information security. However, the policies developed by a specific health care organization to protect the confidentiality, integrity, and availability of patient and administrative information is significantly influenced by the organizations unique mission, culture, and management.

The foundation for a successful information security program is comprehensive information security policies. These policies should define the organization's philosophy and direction for the protection of information. The policies must be documented and promulgated throughout the entire organization.

While the majority of the information maintained by health care organizations consists of patient records, these organizations also maintain sensitive and valuable business records. The confidentiality, integrity, and availability of these business records must be protected to enable the continued successful functioning of the organization. Therefore, the recommendations in this document apply to all information created, maintained, and used by organizations utilizing computer-based patient records.

Objectives

The objectives of these guidelines are to:

- Encourage and facilitate the use of CPR systems providing for the effective development of info

-

- complying with requirements for confidentiality and privacy established by applicable state and Federal laws, the Joint Commission on Accreditation of Health care Organizations, and regulatory agencies.
- Promote consistent protection of information throughout the entire health care delivery system.
- Communicate the responsibilities for the protection of information and foster information security awareness.
- Foster good business practices related to protecting health care information.
- Provide the basis for information security standards and procedures and standards for the management, storage, and distribution of health care information.

Scope

This document is designed to be used primarily in the establishment of information security policies at all types of organizations implementing and utilizing computer-based patient records. While it may be helpful in specifying security controls, features, and functions, it is primarily intended to be used to define management policies. These management policies will form the basis for the development of the standards and procedures that dictate the specific security controls to be implemented.

Hospitals, academic health centers, health care networks, home health agencies, health care group practices, long-term care facilities, ambulatory care facilities, mental health facilities, dental practices, transcription services, pharmacies, chain drug stores, research facilities, insurance companies, caregivers and operators of health care information systems and networks, government agencies, and any other organization with access to the computer-based patient record should develop information security policies. While, larger, multi-functional organizations with more diverse information needs may require more extensive policies than organizations making more limited use of the information, basic information security policies are required for every organization.

For maximum effectiveness, these policies should be issued at the highest level of the organization and should apply to all employees, independent contractors, and agents, and to all units of the organization. The policies should define the obligations for protection of information to be included in the agreements with all payers, contractors, vendors, accreditation organizations, and all other outside agencies who will be granted access to the information owned by, or in the custody of, the organization.

Policies should be established for the release and use of information for providing patient care, protecting the public health, ensuring quality of care, managing the organization, supporting research activities, paying for care, obtaining insurance coverage, and any other purpose.

Because the security of the information maintained on computer-based patient record systems is partially dependent upon the security of information maintained in other forms, the information security policies should apply to all information owned by, or in the custody of, the organization regardless of its form or storage media. The policies established by individual organizations should be applicable to all types of information used by the organization, including but not limited to:

- Patient health information
- Patient demographic information
- Patient financial information
- Research information
- Information about physicians, nurses, and other caregivers
- Peer review information
- Information about payers
- Business records including financial records, personnel records, practice patterns, quality assurance statistics, strategic plans, and similar information.
- Computer software

Relationship to Legal and Regulatory Requirements

The information security policies should specify the organization's complete policy for information protection. The policies should include all measures necessary for the organization to comply with all legal and regulatory requirements.

The policies must be sufficiently comprehensive so that all users who adhere to the policies and properly use the systems designed, implemented, and managed in accordance with the standards and procedures derived from these policies will be in full compliance with all legal, industry, and professional requirements including:

- Federal and state laws pertaining to the protection of health care information
- Federal regulatory requirements
- Joint Commission on Accreditation of Health care Organizations accreditation requirements
- State licensure and regulatory requirements
- Laws and procedures for protecting public health
- State computer crime laws
- State business practice laws
- Professional ethics

Distribution and Promulgation

The policies must be made available to all employees, professional staff members, faculty, students, volunteers, vendors, contractors, researchers, and others who may be granted access to information by the organization. All persons being granted access to the organizations information should formally acknowledge an understanding of the policies and make a formal written commitment to comply with those policies prior to being entrusted with access to the information. Provisions should be made for periodic renewal of these agreements.

The policies should not be confidential and may be made available to the public. Policies may be distributed via computer-based systems or as paper documents.

Policy Subjects

The following sections identify the topics for which the organization should consider developing policies. Individual policy statements addressing these subjects should be combined to comprise the contents of the organization's information security policy document. The subjects are listed solely as guidelines to assist in developing policies for the organization. Legal counsel, applicable statutes, the Joint Commission on Accreditation of Health care Organizations, relevant regulations, and other official sources should be consulted for detailed, specific requirements.

Philosophy for the Protection of Information

Each organization using a computer-based patent record system must define its philosophy for the protection of information. Although much of the information maintained by health care organizations represents patent information**,** most organizations also create and maintain business records for the enterprise. These business records are a primary asset of the organization and must be protected in a manner commensurate with their value. Therefore the philosophy statements for the protection of information should be applicable to all information created, collected, stored, and processed by the organization. This includes all information that is the property of the organization, the patient, caregivers, researchers, or any other party, and has been- entrusted to the institution for use and safekeeping.

Patient Rights with Respect to Information Security

The policies should define how the organization will respect the rights of the patient with regard to information. In addition to the rights preserved by law and regulatory requirements, the organization may wish to grant additional rights to the patient based on its mission and philosophy.

Areas for consideration in developing the policies are:

- Right to be informed of their rights. Responsibilities for implementing procedures for ensuring that the patient is informed of the policies related to patient information should be defined.

- Right to privacy. Relevant patient information may only be disclosed to those directly involved in the care of the patient, for the protection of the public health as provided by law, for the payment of services as authorized by the patient, to assist researchers as authorized by the patient, or for any other purposes required by law or authorized by the patient.

- Right to review information. Patients are entitled to know which information about them is in the possession of the organization and are entitled to review that information. Any category of information that may be withheld from the patient in accordance with the law should be defined in the policies.

- Right to clear and complete presentation of information. Policies related to making information from the computer-based patient record available to the patient in a clear, logical, understandable format should be developed. Any policies for presenting information in a format not maintained by the organization should be defined. The organization's policies related to the costs associated with presentation of information should also be defined.

- Right to append correct information. Information cannot be deleted, but erroneous information can be marked as such and correct information appended. The rights of the patient to provide supplemental information or an appendix should also be defined.

- Right to block release of specific information. The patient's rights to segment information and block the release of specific information should be clearly stated. The rights of the organization to identify and explain any consequences of such blockage should also be included.

- Right to notification of disclosure of information. The patient's rights to know which individuals, organizations, and government agencies have authority to access, and have actually gained access to, specific information identified with the patient should be clearly defined in the policies.

- Right to protection of information released to third parties. The policy should define the commitment for protection required from a third party prior to the release of information to that organization. The policy may also specify the responsibility for monitoring these commitments.

- Right to integrity and availability. Records must be protected from unauthorized modification and destruction. The patient has the right to expect that the organization will take reasonable precautions to protect the information from destruction by accident or vandalism, and by fire, flood, earthquake, or other disasters. Policies requiring that provisions be made for the patient records to survive the organization in the event of mergers, bankruptcy, and similar events should be established.

Protection of Caregiver Information

The organization's policies should define how information related to caregivers is to be protected. Because caregivers may be employees, independent contractors, and agents of the organization, applicable good business practices and laws pertaining to employee records and contractual agreements should be considered in addition to the requirements for protecting health information. Areas for consideration include:

- Privacy. The caregivers' personal privacy should be preserved. Relevant caregiver information may only be disclosed for the protection of the public health as provided by law, for any other purposes as required by law, or as authorized by the caregiver.

- Review of information. The caregiver is entitled to know which information about the caregiver is in the possession of the organization. Caregivers' are also entitled to know which information they have a legal right to review. Caregivers should have the right to review information they have placed in the patient's record.

- Clear and complete presentation of information. Information about the caregiver and patient information authorized to the caregiver should be made available in a clear, logical, understandable format.

- Appendment of corrected information. The caregivers' rights to identify erroneous information and append correct information pertaining to their employment or contractual arrangements should be defined.

- Release of specific information. The caregiver may be granted the right to segment information and block the release of specific information where permitted by law.

- Notification of disclosure of information. The caregiver is entitled to know which individuals, organizations, and government agencies have authority to access and have actually gained access to information about the caregiver.

- Protection of information released to third parties. The policy should define the commitment for protection required from a third party prior to the release of information to that organization.

- Integrity and availability of records. Records must be protected from unauthorized modification and destruction. The caregiver has the right to expect that the organization win protect the information from destruction by accident or vandalism, and by fire, flood, earthquake, or other disasters. Provisions must be made for the records to survive the organization in the event of closure, mergers, bankruptcy, and similar events.

- Responsibility to protect information. The caregivers' responsibility for the protection of the information to winch the caregiver has access should be stated

The Privileges and Obligations of Researchers

Whether or not patient or caregiver identifiable information will be made available for research, and how that access to information will be authorized, should be included in the policies. The policies should define the role of the institutional review board with respect to information protection. Some of the topics to consider related to the use of computer-based patient record information for research are:

- Opportunities for access to information. Policies for granting access as authorized by the appropriate party or as permitted by law should be established.

- Obligation to protect the information. Researchers' responsibilities to protect the information in their custody should be included in the policies. This includes information that may be removed from the organizations' premises. If researchers are authorized to release information, the policies should define researchers' responsibilities to notify recipients of information of the protection requirements,

- The researchers expectation of accurate information. The policy for ensuring that researchers are made aware of the sources and the accuracy of information being provided should be considered.

- Right to control disclosure of information. The researcher or organization generally has the right to control which individuals and organizations have authority to access information resulting from the research provided the information does not identify specific patients or caregivers, and cannot readily be used to do so.

- Right to integrity and availability. Records must be protected from unauthorized modification and destruction. Within the provisions of any agreements with the organization, the researcher has the right to expect that the organization will protect the information from destruction as a result of accidents, vandalism, fire, flood, earthquake, or other disasters. Provisions must be made for the records to survive the organization in the event of closure, mergers, bankruptcy, and similar events.

The Rights of Society

Although the requirements for release of some patient information are defined by law, organizations using the computer-based patient record should develop policies addressing the responsibilities and determining the methods of complying with these laws.

The organizations policies related to complying with the law for the release of patient, caregiver, and institutional information to public health authorities should be defined.

The policy for the release of information for criminal proceedings, and civil and administrative litigation should be defined. The policies should state how the institution will resolve conflicts in the rights of the patient, the caregiver, and society.

Factors to consider in the release and sharing of information include:

- Which information may be released?

- To whom may information be released?

- Who authorizes release or is responsible for ensuring that the appropriate person has authorized release?

- Who is responsible for developing procedures for release?

- What responsibility does the institution have regarding the protection of information it has released from its custody?

- Who is responsible for managing shared databases and networks?

Collection of Information

Each organization should define its policies for collection and authentication of information. The policy should specify who is responsible for determining which information is to be collected and retained. Responsibilities for the review of information collection policies and retention periods should be specified. Responsibilities and provisions for verifying the accuracy of information should be defined.

Retention and Destruction

Business and patient records must be readable and usable for the life span of the records. The policies should define the necessity and responsibility for developing procedures to ensure that the records are maintained and are accessible for the minimum lifetime of the record as required by law or by business and patient care requirements. Policies specifying the responsibilities for determining the time periods for retention should be included.

Policies to ensure that the organization provides for preservation of the records during the migration to new technologies are essential. Policies defining the responsibilities for destruction of information should be included.

Information Security Program

Every organization should, as a matter of policy, maintain a formal information security program. The responsibility for management of the program and the functions of the program should be described in the policy document.

Responsibilities for the periodic review and maintenance of the information security policies should be specified.

Accountability and Responsibilities

Specific responsibilities and accountability for information security should be defined in the policies. Factors to consider are:

Board of directors/trustees responsibilities including recognizing the importance of information security, establishing policies, establishing the information security program, and authorizing funding.

- Managers' responsibilities including ensuring appropr
-
-
-
-
-
-
- rs, vendors, contractors, temporary employees.
- Responsibility for reporting of violations.
- Responsibility for determining and administering discipline and penalties.

- Responsibility for assessing and accepting risk.
- Patient responsibilities.

Penalties and sanctions for failure to comply with the policies and to fulfill responsibilities should be specified.

Access to Information

Access to information should be defined as a matter of policy. Access should be limited to those entitled to access on the basis of a specific patient care, business need, or research requirement for access as authorized by the patient for patient information and as authorized by the caregiver for caregiver information. Access to patient-specific information, caregiver-specific information, and organization information by those with authority to protect the public health should be granted as provided by law, or to a greater extent, as authorized by the patient or caregiver.

Access to information for law enforcement, litigation, or other purposes not authorized by the patient or caregiver should be granted only to the extent required by law.

The organization should establish policies specifying that access to the organizations business records will be based on assigned job responsibilities.

Responsibility for verifying the legitimacy of requests for access, granting access, and revoking access should be specified. The responsibilities for establishing procedures for resolving disagreements, and for actually resolving disagreements, related to access to information should be defined.

The extent and policy for enforcement of individual accountability for the creation, modification, deletion, or disclosure of information should be defined.

Classification of Information

The policy of the organization with regard to the classification of information on the basis of its sensitivity to disclosure should be defined. The classification categories should be consistent with legal requirements and industry standards. Categories to consider are:

- Information which may be made public.
- Information internal to the organization which may be disclosed to anyone within the organization.
- Information that must be protected from disclosure to anyone other than those specifically authorized access to the information by job function.
- Information that may be disclosed only to certain identified individuals and for which a record of disclosure is maintained.

Records of Access

The policy of the organization to maintain records of access to information should be defined. Policies should specify in general how long records of access should be maintained and who is responsible for determining which records of access must be preserved. The policies should also be applicable to third parties who have access to the organization information or to which information has been released.

Disaster Recovery/Business Resumption Plan

This policy should specify the organizations requirement for developing and maintaining business resumption plans to ensure that the health care organizations information remains available for use in the event of a natural disaster, vandalism, or system failure. The policy should define the responsibility for developing, maintaining, and testing the plans, and define responsibilities for actual recovery.

Information Security Awareness Training

The policies should define a formal information security awareness-training program to be established in the organization. Responsibilities for determining training requirements and conducting training should be defined. The content, frequency of training, and specific training programs and material should be defined in the organizations information security standards. Policies for documentation of attendance at training sessions should be established.

Monitoring and Auditing

Responsibilities and objectives for monitoring of the information security program and for auditing for compliance with the information security policies, standards, and procedures should be specified in the policy document.

Suggested Method for Policy Development

Information security policy development should be accomplished as a formal project, fully sanctioned, and supported by senior management. The following are recommended steps for policy development:

- Establish a formal, fully funded project to develop the policies.
- Assign responsibility for the project and appoint an information security manager.
- Use the topics in these guidelines as the basis for writing policy statements.
- Submit the proposed policies to the organizations legal counsel for review.
- Submit the draft policies to the management of the organization for review.
- Submit the document to the board of trustees or board of directors for approval.

References

Dick, R. S. and Steen, E. B., editors *7he Computer-based Patient Record: An Essential Technology for Health Care.* Washington, DC: National Academy Press, 1991.

Donaldson, M.S. and Lohr, K.N., editors *Health Data in the Information Age: Use, Disclosure, and Privacy.* Washington, DC: National Academy Press, 1994.

Kunitz and Associates, Inc. *Final Report of the Task Force on the Privacy of Private-Sector Health Records.* Contract HHS- 100-91-0036. Rockville: KAL September 1995.

Louis Harris and Associates. *Harris-Equifax: Health Information Privacy Survey 1993.* New York: Louis Harris and Associates, 1993.

Louis Harris and Associates. *Equifax-Harris: Consumer Privacy Survey 1994.* New York: Louis Harris and Associates, 1994.

Madsen, W. *The Handbook of Personal Data Protection.* New York: Stockton Press, 1992.

System Security Study Committee, National Research Council. *Computers at Risk: Safe Computing in the Information Age.* Washington, DC: National Academy Press, 1991.

US Congress, Office of Technology Assessment. *Protecting Privacy in Computerized Medical Information.* OTA-TCT-576. Washington, DC: Government Printing Office, September 1993.

Glossary

Most terms in these guidelines are intended to be interpreted according to their generally accepted usage and meaning. The following terms have been defined to help add clarity to their usage in this document.

Access to Information - The ability to store, retrieve, or make use of information. Access includes the ability to reproduce and disseminate the information.

Caregiver - An individual who directly or indirectly provides health services, the goal of which is to heal, promote health, and improve the well being of another individual.

Confidentiality - The act of limiting disclosure of private matters; maintaining trust that an individual has placed in one which has been entrusted with private matters.

Information Security - The process of safeguarding information; generally refers not only to safeguarding confidentiality but integrity of data, unauthorized disclosure, modification, or destruction.

Information Security Manager - The person assigned responsibility for management of the organization's information security program.

Information Security Program - All activities of the organization related to information security. A complete information security program consists of policies, standards, training, technical and procedural controls, risk assessment, auditing and monitoring, and assigned responsibility for management of the program.

Integrity - The state of being whole; unimpaired. Integrity of data refers to its accuracy and completeness.

Organization - Anyone or any entity who collects, stores, transmits, or otherwise processes health care information.

Patient Information - Refers to data collected about or related to the health status and health care of a specific identifiable individual.

Privacy - That which is not open to or controlled by the public; of or concerning an individual; that which is secret and not shared.

CPRI Members

3M Hlth Info Sys
Adventist Hlth Sys/Sunbeft
ALLTEL Info Svcs - Hlthcare Div
Amer Acad of Family Physicians
Amer Acad of Pediatrics
Amer Assn for Med Transcription
Amer Board of Family Practice
Amer College of Physicians
Amer Hlth Info Mgmt Assn
Amer Hospital Assn
Amer Mad Informatics Assn
Amer Medical Assn
Amer Org of Nurse Executives
Andersen Consulting, LLP
Arkive Information Systems
Assn of Operating Rm Nurses
Chi Systems
Coll of Amer Pathologists
Coll of Hlth care Info Mgmt Execs
Columbia/HCA Hlth care
Ctr for Hlth care Info Mgmt
Ctrs for Disease Control & Prev
Dept of Veterans Affairs
Dynamic Hlth care Tech
Eli Lilly and Company
Ernst & Young, LLP
Glaxo Wellcome
Group Hlth Assn of Amer
Harvard Comm Hlth Plan
HBO & Company
Hlth Industry Mnfrs Assn
Hlth Level Seven
Healthdyne
HealthVISION Corp
Inst for Clin Sys Integ
InterPractice Sys
JCAHO
Kaiser Permanente
Management Systems Assoc
Mayo Foundation
Medic Alert Fnd US
Medical Connections
Medical Records Inst
MedicaLogic
Medicus Systems
Motorola
Natl Assn of Chain Drug Stores
Natl Cncl for Pres Drug Progs;
NC Hlth Care Info & Comm AlInce
NEON Hlth care Softmre
Northwestern Memorial Hosp
Oceania
PHAMIS
Physician Micro Systems
Prudential Insurance Co
SIDOCI Enr
Sisters of Mercy Hlth Sys
SoftMed/HIS
Systems Plus
The Permanente Med Group
ThetaPro
Unitron Mad Comm
Univ Hlth System Consortium
Univ of IA Hosp & Clinics
Univ of VA Hlth Sci Ctr

CPRI is a nonprofit membership organization committed to advancing improvements in health care quality, cost, and access through routine use of information technology. CPRl serves as a neutral forum for bringing the diverse interests of all health care stakeholders together to develop common solutions.

CPRI functions primarily through the voluntary work of its work groups. All individuals are invited to participate in one of the following:

- Work Group on Codes & Structures
- Work Group on Confidentiality, Privacy & Security
- Work Group on CPR Description
- Work Group on CPR Systems Evaluation
- Work Group on Professional & Public Education

Toolkit Section 4.3

Sample Security Policies

The sample security policies provided are from organizations that have agreed to share their work with CPRI so that colleague organizations may benefit from their experience and advance the state of health care information security. Health care organizations may use the samples to assist in developing their own policies, but may not publish them elsewhere without the expressed written consent of the original institution or use them verbatim as their own policies. Contributors include the following organizations:

1. Harvard Vanguard Medical Associates, Brookline, MA
2. Kaiser Permanente Northern California
3. Mayo Clinic, Rochester, MN
4. Partners Healthcare System, Boston, MA
5. PCASSO, SAIC, and the University of San Diego Medical Center

Project Phoenix, Georgetown University Medical Center, Washington, DC

Patient Confidentiality Policies & Manual

Opening Statement **1**

Harvard Vanguard Policy on Confidentiality of Clinical Information **2**

Confidentiality Guidelines

Regarding Medical Information **7**

Regarding Appointments **8**

Regarding Employee Patients **8**

Confidentiality Safeguards **9**

Release of Information (ROI)

Requests for Medical Information **9**

Sensitive and Legally Protected Medical Information **10**

Minors and the Release of Medical Information **11**

Emancipated Minor **12**

Mature Minor **12**

Medical Record System Audit **13**

Documentation Guidelines for Clinicians

Introduction **14**

General Guidelines **14**

Sensitive Medical Information **15**

Corrections/Addenda **16**

Documentation Method **16**

Policy Regarding the Use of E-mail for
Patient-Specific Clinical Information **18**
Background & Content **18**
Policy on the Disciplinary Process for Breach
of Patient Confidentiality **20**
Introduction **20**
Procedures **21**
Self Assessment **27**
Resource List
If you want to do more **29**
Contacts **29**

As a multi-specialty group practice, Harvard Vanguard Medical Associates (Harvard Vanguard) has special concern for confidentiality in the work place. Safeguarding patients' medical information is not only a legal requirement, but also an important ethical obligation. In the pages that follow, we provide a copy of Harvard Vanguard's policy on the confidentiality of patient information. Every Harvard Vanguard manager and supervisor is responsible for educating his or her staff about these policies. The need for adherence to this policy should be continually reinforced. Violation of these policies may be grounds for disciplinary action, including termination for serious cause.

Harvard Vanguard Policy on Confidentiality of Clinical Information

Introduction

The clinical information contained in the medical record has been entrusted to us by our patients. This information is highly sensitive and requires thoughtful and attentive management by those who have access to it. All Harvard Vanguard staff are committed to protecting our patients' right to privacy and safeguarding the clinical information contained in their medical records.

We recognize that there will be situations in which the patient's need for privacy will conflict with the clinician's "need to know". In those situations, we seek to balance the conflicting needs, protecting the patient's right to privacy, without compromising our ability to provide safe and effective medical care. We do this by:

- Ensuring that the medical record contains only information which is essential to the clinical practice.
- Ensuring that the information is objectively and sensitively documented.
- Ensuring that access to the medical record is restricted based on a "need to know" basis, narrowly defined in terms of who needs to know what, when, and for how long.
- Ensuring that access to the medical record can be managed through real-time controls and retrospective auditing in order to safeguard the information which it contains.

To guarantee that the medical record for each patient contains only information that is clinically appropriate, and to ensure that access to this information is tightly managed, the following policies were developed. Violation of these policies will be grounds for disciplinary action, up to and including termination for serious cause.

Responsibility

Responsibility for the content and administration of this policy resides with the Harvard Vanguard Medical Director's Office.

Harvard Vanguard Policy on Confidentiality of Clinical Information

Patient Medical Information

All Harvard Vanguard staff have a responsibility to recognize the special relationship of trust between us and our patients and must safeguard all medical information and/or personal information about patients. Harvard Vanguard staff may use or disclose medical information only as necessary in the delivery of patient care, for authorized administrative purposes and in formally approved research. Medical information may also be disclosed if authorized by the patient or when required by law.

Medical information is considered to be any patient-specific information gathered as part of the patient care process, including, but not limited to encounter descriptions, referrals, requisitions and results of ancillary services, diagnoses, treatment and appointment information. This policy does not cover aggregated data on utilization and patient demographics.

Staff should be sensitive to the fact that fellow employees often obtain their health care at Harvard Vanguard. It is never appropriate for employees to reveal information, including incidental observations, about fellow employees receiving care at Harvard Vanguard.

Staff should be aware of the following:

- Staff may not gain access to information concerning patients, including both medical and enrollment information, except for legitimate clinical and business purposes. Any uncertainty about what constitutes such purposes should be discussed with your supervisor.
- Patient information must never be discussed in public areas.
- Medical records may not be released to anyone (including but not limited to employers, insurance companies, relatives or friends) without the written consent of the patient or when required by law. The only exception is that clinical staff may release clinical information, including medical records when appropriate to facilitate the care of patients, including care by non-Harvard Vanguard providers. All release of medical records must be handled by the site's medical records department.

Harvard Vanguard Policy on Confidentiality of Clinical Information

Patient Medical Information *(continued)*

- Medical records (including all documents containing medical information about an identifiable patient) may only be disposed of by means that assure that they will not be accidentally released to an outside party. Managers must assure that appropriate means of disposal are reasonably available.
- Employees who are patients of Harvard Vanguard must follow standard procedures to obtain or view their own medical records.
- Staff may not attempt in any way to alter information in any medical records, except in accordance with Harvard Vanguard policy. (A copy of the record prior to alteration must always be retained.)

Harvard Vanguard Policy on Confidentiality of Clinical Information

Medical Record Access and Release of Information

Access to a patient's medical record must be treated with utmost respect and confidentiality. Staff with access to the automated medical record will be trained in the standards and behaviors incumbent with this privilege. Responsibility for monitoring and enforcing these policies rests with local site management.

Access to the general medical record is obtained via a coded password which uniquely identifies the user. Passwords may not be disclosed or shared.

Access to mental health session notes in the Mental Health paper chart is limited to mental health clinicians and selected staff. Primary care clinicians may contact the treating mental health clinician to obtain information necessary for the design of a medical treatment plan for the patient. Mental Health patients are informed of Harvard Vanguard's mental health documentation and access policies upon their first visit to Mental Health (see *"Information Concerning Confidential Communications and Record keeping in Mental Health Departments"* available through Central Mental Health).

Patient information should be released only to the patient, unless otherwise authorized by the patient or required by law. This includes medical records, appointment information and test results. In addition:

- Patient information cannot be released to a patient's spouse or other family member without the patient's consent.
- Patient information regarding an adult child cannot be released to a parent without the patient's consent.
- If the patient is a minor, patient information cannot be released without the consent of the parent or the patient's legal guardian.
- There are conditions when clinical or appointment information on an adolescent cannot be released to the parent or legal guardian without the patient's consent. State regulations and Harvard Vanguard's *Consent Guidelines for Treatment of Minors* (available from the Legal Department) should be followed in these cases.
- Detailed clinical information should not be left on an answering machine or voice mail.

All requests for release of medical information to persons/institutions/agencies outside of Harvard Vanguard should be referred to the Medical Records Department.

Harvard Vanguard Policy on Confidentiality of Clinical Information

Medical Record Content

The Harvard Vanguard Medical Record includes the general automated medical record, the automated mental health session notes, and the hard chart, a paper record on file in Medical Records which generally contains pictorial information and clinical information from institutions other than Harvard Vanguard sites.

All patient interactions regarding care and treatment, including phone calls, should be documented in the patient's medical record.

Documentation should be objective and sensitive to the patient.

Certain information has been designated as sensitive and has been assigned specific "restricted" codes to protect it from accidental outside release, unless authorized by the patient or required by law. This statutorily protected and sensitive information is detailed under **"***Sensitive and Legally Protected Medical Information*" (*see page 10)*.

The general automated medical record will include only the following mental health information, unless the patient has consented to include more detailed mental health information in his/her record:

Diagnosis Code
Visit Dates
Active Medications
Clinician Name

All other mental health information will be contained in the Mental Health paper chart, with access restricted to mental health clinicians and selected department staff.

Confidentiality Guidelines

Patient information of any nature is confidential. This includes information from or about medical records, test results, appointments, and referrals. A patient's presence at a Harvard Vanguard site is also confidential.

Regarding Medical Information

Harvard Vanguard staff are obligated to make sure that medical information is not disclosed *inappropriately*, *accidentally* or *negligently*. In order to do this we must take appropriate precautions to safeguard medical information.

- Do not allow medical information on terminals to be visible to patients.
- Keep patient charts and encounter forms face down. Never leave them out where others can see them.
- Use confidential trash bins when disposing of medical information. Any documents with a patient's name, insurance number or medical record is considered medical information.
- Place medical record charts and other medical information outside exam rooms or clinical offices so that they face the door or wall.
- Speak softly over the phone and try to avoid excessive use of the patient's name.
- Do not discuss patient information with anyone in a social conversation.
- Make a habit of speaking to patients in private offices and exam rooms only.
- Do not discuss the reason for a patient's visit in the waiting area or in front of others.
- Anticipate patient privacy needs when giving out test results, setting up appointments and referrals.

Confidentiality Guidelines

Regarding Appointments

A patient's presence in a Harvard Vanguard medical office is itself a piece of confidential information.

Unless you are absolutely certain that you have the patient's permission to do so:

- Never reveal to a third party that a patient is, has been, or will be present at a Harvard Vanguard site.

  Third parties can include spouses, employers, friends or strangers. Inquiries can occur by telephone or in person.

- Never leave a detailed message with a third party when calling to confirm an appointment. If the patient is not available, leave a generic message. Do not leave your name and number on an answering machine.

Ask patients at the time of their appointment how they would prefer to get messages. Make a note of it in the appointment schedule.

Regarding Employee Patients

There are several ways Harvard Vanguard protects the confidentiality of employees who are patients.

- Employees' and their family patients' records are restricted. This means that access to these computerized medical records is restricted to a limited number of employees, i.e., clinicians and other Medical Records staff.

- Restricted medical records are transported between departments in a grey or orange envelope. Restricted records are to be opened *only* by a clinician.

- Employee patients do not need to give a reason for their appointment. This applies to both scheduling the appointment and checking in.

Confidentiality Guidelines

Confidentiality Safeguards

- Each employee is required to read and sign the Harvard Vanguard Confidentiality Policy at their initial orientation.
- Passwords are *strictly confidential*. Employees may not divulge their passwords to anyone.
- All staff are obligated to notify their supervisors in the event that any of these policies are violated.
- Both Automated Medical Record System (AMRS) and EpicCare keep an "Audit Trail" showing a history of inquiry by medical record number and password.

Release of Information (ROI)

Requests for Medical Information

Medical records may be released only by the Medical Records Department in accordance with ROI policies and procedures. Harvard Vanguard Medical Records Departments receive requests for medical information each month. These requests come from many sources:

- Patients
- Family member
- Attorneys
- Insurance Companies
- Employers
- Other Health Facilities

There are many Harvard Vanguard policies and state and federal statutes involved in the release of medical information. (These are outlined in the *Release of Information Participant Guide* and the *Release Of Information Reference Tool*.) The most important is that a signed authorization from the patient is usually necessary to release information. The release form or letter is placed in the patient's hard chart to be kept permanently on file.

- Any patient requesting a ROI must do so through the Medical Records department at their home site.
- Processing time is 7 working days.

Release of Information (ROI)

Sensitive and Legally Protected Medical Information

There are two categories of information which require specific authorization prior to releasing a record: statutory (state or federal law) and sensitive (information deemed particularly personal by the patient). Statutorily protected information includes:

- Sexually transmitted diseases
- HIV testing & AIDS
- Alcoholism/Drug abuse treatment
- Abortion
- Sexual assault counseling
- Mental health treatment and counseling
- Domestic and violence counseling

Information about these diagnoses should be documented under special "protected" codes in the medical record. Harvard Vanguard will not release any information in these categories unless the patient or court order specifically authorizes it by name ("any and all records" is not acceptable). Clinicians may obtain these "protected" codes from the Medical Records Department.

In addition, certain medical information may be specified by the patient as sensitive. (Examples might include treatment for infertility, genetic testing, or child, elder, physical or sexual abuse.) In most circumstances, Harvard Vanguard will not release specified sensitive information without the patient's consent, but may be required to do so by law (for example, in response to a valid records subpoena).

Release of Information (ROI)

Minors and the Release of Medical Information

Minors are defined by Massachusetts law as individuals who are less than eighteen years of age. For most issues, parents have the right to know about care provided for their minor children. It is important, however, to remember that minors are entitled to confidentiality of their medical records in some cases.

When dealing with the medical information of minors remember:

- Access and authorization to release the medical record of a minor usually resides with the minor's natural parents (including noncustodial parents) or legal guardians.
- There are two situations in which parental consent is not required for a minor: when the patient is determined to be either an ***emancipated*** or ***mature*** minor. If parental consent is not necessary, then the minor controls the record (or relevant entries) and it cannot be released to the parents unless the minor consents, or a court order states the contrary.

Release of Information (ROI)

Minors and the Release of Medical Information *(cont'd)*

Emancipated Minor

The following is a list of specific situations where the patient is legally, as defined by the statute, considered an emancipated minor:

1. the patient is married, widowed, or divorced;
2. the patient has a child (patient can also consent for the child);
3. the patient is a member of the armed forces;
4. the patient is pregnant or believes herself to be pregnant;
5. the patient is living away from his/her parents and is managing his/her own finances; or
6. the patient reasonably believes he/she has come in contact with a disease listed by DPH as dangerous (note that consent to treatment in this case is limited to care relating to the particular disease on the list).

If the patient falls into one of the above categories, parental consent is not required and the medical records cannot be released without patient consent—unless a court order states the contrary. (***Note that consent for abortion or sterilization does not apply to paragraphs 2 through 6.***)

Mature Minor

If a patient is under 18, not in an emergency situation, and not emancipated under the law, there still may be situations where the law allows the patient to consent to treatment and where the record reflecting that treatment is kept confidential unless the minor patient consents to its release. These situations are when the clinician determines that the patient is a "mature minor", capable of consenting to treatment. This is a clinical decision requiring careful analysis for each patient in a given clinical situation.

The provider must consider the nature of the proposed treatment, the likely benefit to the patient and the capacity of the particular minor to understand what the medical treatment involves. Where the best interests of a minor will be served without notifying his or her parents and where the minor is capable of giving informed consent to the proposed treatment, the clinician may treat the minor as a mature minor for that particular encounter. Remember to document that the patient is a mature minor

Harvard1.doc

Anyone involved in the care of an adolescent must thoroughly understand and follow state law and organizational policy regarding confidentiality of minors. The laws are complex, requiring careful thought and a sensitive approach to each patient and parent encounter. When in doubt, seek legal advice.

Medical Record System Audit

Both EpicCare and the Automated Medical Record System (AMRS) track the activity of each user on the system and can generate audit reports to detail this activity. Each user's inquiry into a medical record is dated and recorded. Because it is important to demonstrate to our patients that we have confidence in the integrity of our confidentiality policies and procedures as they relate to medical records access, any patient may request an audit be conducted.

At any time, patients may ask that we conduct an audit to determine who has accessed their medical record. Patients should be directed to Medical Records to initiate an audit. Any questionable access flagged by the Medical Record Coordinator will be referred to the site Administrator for follow-up.

Documentation Guidelines for Clinicians

Introduction

The following guidelines are compiled based on State law, risk management guidelines, professional society recommendations and Harvard Vanguard organizational policy in order to assist clinicians with medical record documentation. If you have questions regarding these guidelines, consult your clinical chief or site manager.

General Guidelines

These guidelines define a protected channel in which it is appropriate for clinicians to document confidential patient medical information in the medical record. It is important for clinicians and all other staff to know that these medical records can always be seen by the patient upon the patient's request and also, under certain circumstances, are subject to subpoena and review in legal action. Consequently, it is the responsibility of all clinicians to include only clinically relevant information in the patient's medical record and to document this information in language that is objective, accurate and concise.

It is also important for clinicians to document with precision all patient interactions and all essential clinical information.

All patient interactions regarding care and treatment should be documented in the patient's medical record including:

- Encounters (medical visits)
- Telephone calls and attempts to return phone calls
- Letters
- Clinician/patient conversations
- Test result notifications
- Refusals by patients to comply with therapy
- Visit cancellations and "did not keep" appointments

Documentation Guidelines for Clinicians

General Guidelines *(continued)*

The following essential information should be collected at each patient visit and documented in the patient's medical record:

- Patient's name and date of visit
- Pertinent medical history as appropriate for each visit:
  - -chief complaint
  - -hx of present illness
  - -past medical history
  - -allergies
  - -social/personal hx
  - -family history
  - -review of systems
  - -vital signs
- Normal and abnormal physical examination findings
- Differential diagnosis
- Results of diagnostic tests
- Diagnostic decisions based on the history, examination and test results
- Treatment plan and rationale
  - -medications prescribed, with dosage and regimen
  - -immunizations (include signed consent forms in the "hard chart")
  - -planned diagnostic studies
  - -planned additional medical evaluations
  - -internal or external referrals
  - -recommendations for further treatment or observations
- Follow-up instructions to the patient
- Anticipated patient return
- Documentation of patient education or Instruction

Sensitive Medical Information

Statutorily protected and sensitive medical information should be documented and referenced only under protected codes. This includes information on:

- Sexually transmitted diseases
- HIV testing
- Abortion
- Mental health treatment
- Infertility
- HIV & AIDS
- Alcoholism/drug abuse treatment
- Sexual assault counseling
- Child, elder, physical or sexual abuse

Documentation Guidelines for Clinicians

Corrections/Addenda

Corrected information and addenda should be input into the AMRS or EpicCare record by Medical Records, according to defined policies and procedures.

If information is mistakenly left out of the chart or if a patient wishes to make an addendum, and the clinician deems it appropriate, an addendum to the record can be made. However, the information should be recorded chronologically and dated as to when the information is actually entered into the chart.

If a patient requests that the clinician makes a substantive change to the record, and the clinician has questions, s/he should contact the Legal Department.

Documentation Method

Streamline your record entries; keep them complete, but concise and to the point.

Include only information that is relevant to the patient's clinical care. Do not include commentary on systems issues or administrative detail.

Omit personal opinion and subjective judgment about the patient or the patient's behavior. Keep in mind that patients may access and review their own medical record upon request.

Do not document opinions about treatments rendered by other clinicians.

Document patient complaints about previous treatment by noting that the patient states the outcome of the treatment was undesirable.

Documentation Guidelines for Clinicians

Documentation Method *(continued)*

Avoid documenting statements that might be misconstrued as a promise of a certain outcome or result.

Document undesired outcomes of care:

- Be objective and emphasize how best to correct or manage the undesired outcome
- Include a record of the conversation with the patient informing him/her of the undesired outcome

Update the AMRS or EpicCare record frequently. Clearly identify active problems and medications. Use “inactive” and “omit” codes to designate diagnoses or treatments that are inactive or not currently relevant.

Harvard Vanguard Policy Regarding the Use of E-mail For Patient-Specific Clinical Information

Note: ***The following statement applies to the use of internal e-mail communication systems only. The use of external e-mail systems, like the Internet for patient-specific clinical communication, is prohibited by organization policy, although these protocols will be revisited in the upcoming year. Also note that EpicCare, our new Clinical Information System, will have internal messaging capabilities so that clinicians can communicate with each other electronically within the security of the medical record system itself.***

Background & Content

E-mail is a valuable means of communication which helps to facilitate the coordination and integration of patient care. The current alternatives to e-mail are, at times, problematic as many clinicians practice in multiple centers and not all clinicians have access to a single voicemail box. Clear and detailed communication between clinicians can occur via e-mail within a relatively short period of time, even when both clinicians are not simultaneously available. Harvard Vanguard's major hospital partners use their own internal e-mail systems for clinical communication. We believe that this communication can contribute to efficient and effective coordination of clinical care and will be increasingly important for Harvard Vanguard clinicians in the future.

In order to minimize breaches of confidentiality, the following policies must be adhered to when using e-mail for patient-specific communication:

Internal Communication Via E-mail

Specific patient names may be used in an internal e-mail message, provided the following circumstances are met:

- Clinical messages with confidential content must be transmitted only from one clinician to another clinician for purposes related to patient care and not broadcast to a list distribution.
- Patient-specific messages which reference highly sensitive information, e.g., information relating to mental health or HIV diagnoses, must not contain the patient's name. Patient identification must be limited to the patient's Medical Record number.

Harvard Vanguard Policy Regarding the Use of E-mail For Patient-Specific Clinical Information

Background & Content (*continued*)

Clinical e-mail messages must be promptly deleted after they are read. E-mail messages should not be saved or archived on a PC for any length of time. Note that any retained e-mail messages are discoverable in medical/legal circumstances.

- Patient-specific e-mail communications between clinicians should be documented in the patient's record just as other means of clinician-to-clinician communication would be. For example, if in certain circumstances a non-encounter is entered into AMRS to document clinician-to-clinician telephone consultations, then a non-encounter should be used to document similar e-mail consultations.

External Communication via E-mail

- E-mail may be used securely to communicate patient-specific clinical information within Harvard Vanguard or Harvard Pilgrim, but not with other institutional systems since communication outside of Harvard Vanguard or Harvard Pilgrim uses the Internet which is not considered secure. For example, a patient-specific e-mail message transmitted via Goldmail or cc:Mail to a Brigham and Women's Hospital or other non-Harvard Vanguard clinician travels over the Internet. This type of inter-institutional communication is not secure and will be considered a breach of confidentiality.

Violation of these policies will be considered a breach of confidentiality, subject to the Harvard Vanguard *Policy on the Disciplinary Process for Breach of Patient Confidentiality*.

Harvard Vanguard Policy on the Disciplinary Process for Breach of Patient Confidentiality

Introduction

Harvard Vanguard Medical Associates' policy regarding confidentiality of clinical information reflects its strong commitment to protecting the confidentiality of its patients' medical records and clinical information. To ensure compliance with the policy by all staff and to ensure that the disciplinary actions taken as a result of breach of patient confidentiality by an employee are applied consistently, Harvard Vanguard has adopted the disciplinary process set forth below.

Policy

As a health care provider, Harvard Vanguard and its staff are entrusted with clinical information regarding our patients. As set forth in Harvard Vanguard's *Policy on the Confidentiality of Clinical Information*, we recognize that the medical record is highly confidential and must be treated with great respect and care by all staff with access to this information. Any breach in patient confidentiality by a staff person is subject to formal discipline as set forth in this policy. A breach of patient confidentiality occurs when any Harvard Vanguard staff person (i) accesses or reviews patient clinical information for any reason not related to the provision of care and treatment or another authorized purpose (e.g. research, QA, & UR); (ii) discusses with or reveals to any individual(s) clinical information for purposes not related to patient care and treatment or another authorized purpose; or (iii) violates the provisions of Harvard Vanguard's Policy on the Confidentiality of Clinical Information. For any breach in patient confidentiality the involved employee shall be subject to the disciplinary actions set forth in the "*Procedures*" section below.

Applicability

This policy applies to all Harvard Vanguard staff.

Exception

For Harvard Vanguard employees covered by a collective bargaining agreement, any portion of this policy that is inconsistent with the applicable collective bargaining agreement shall be governed by such collective bargaining agreement.

Harvard Vanguard Policy on the Disciplinary Process for Breach of Patient Confidentiality

Procedures

A. Level of Breach

Breaches in patient confidentiality have been divided into the following three levels with the corresponding disciplinary action for each level of breach.

Level 1. Carelessness – This level of breach occurs when a Harvard Vanguard employee unintentionally or carelessly accesses, reviews or reveals patient information to him/herself or others without a legitimate need to know the patient information. Examples include, but are not limited to: employees discuss patient information in a public area; employee leaves a copy of patient medical information in a public area; employee leaves a computer unattended in an accessible area with a medical record unsecured.

- Disciplinary Sanctions:

  Depending upon the facts, counseling, oral warning, written warning, final written warning or suspension, documented in writing and maintained in the employee's personnel record, or termination. Except in the case of termination, the employee shall be required to repeat the confidentiality training module on his/her own time.

- Level 1 Disciplinary Sanctions shall be administered in a progressive manner. Disciplinary sanctions shall be reported to the applicable professional licensing board as appropriate[1]

Level 2. Curiosity or Concern (no personal gain) – This level of breach occurs when an employee intentionally accesses or discusses patient information for purposes other than the care of the patient or other authorized purposes but for reasons unrelated to personal gain. Examples include but are not limited to: an employee looks up birth dates, address of friends or relatives; an employee accesses and reviews a record of a patient out of concern or curiosity; an employee reviews a public personality's record.

[1]*Disciplinary sanctions, other than counseling and oral warnings, may be reportable to the Massachusetts Board of Registration in Medicine and other professional licensing boards.*

Harvard Vanguard Medical Associates

Harvard Vanguard Policy on the Disciplinary Process for Breach of Patient Confidentiality

Procedures *(continued)*

- Disciplinary Sanctions:

  First offense: Depending upon the facts, oral or written warning documented and maintained in the employee's personnel record.

  Second offense: Depending upon the facts, a final written warning and suspension for 3-30 days without pay, documented and maintained in the employee's personnel record, or termination.

  Third Offense: Termination.

- Except in the case of termination, the employee shall be required to repeat the confidentiality training module on his/her own time. Disciplinary sanctions shall be reported to the applicable professional licensing board as appropriate.

Level 3. Personal Gain or Malice – This level of breach occurs when an employee accesses, reviews or discusses patient information for personal gain or with malicious intent. Examples include but are not limited to: an employee reviews a patient record to use information in a personal relationship; an employee compiles a mailing list for personal use or to be sold.

- Disciplinary Sanctions: Termination. Report to applicable professional licensing board.

B. Disciplinary Process

The following process must be followed when an employee breaches, or is suspected of breaching, patient confidentiality:

1. Initial reporting

   - Individual who observes or is aware of a breach reports it to his/her immediate supervisor.

   - Supervisor reports to the site Director or Administrator, Central Specialty Director or Administrator, or such local senior person(s) designated by the care unit (the "local Senior Manager") who notifies responsible matrixed manager as appropriate.

Harvard Vanguard Policy on the Disciplinary Process for Breach of Patient Confidentiality

Procedures *(continued)*

- Failure to report a breach of which one has knowledge will result in appropriate disciplinary action. Reporting of a breach in bad faith or for malicious reasons will result in appropriate disciplinary action.

2. Clear-cut Level 1 breaches

- For a breach involving any staff that is clearly only a Level 1 breach, the Local Senior Manager shall, in conjunction with the Human Resources Department and/or Legal Department as necessary, identify and implement an appropriate action plan as required under this policy and shall communicate such action to the Medical Director's Office in a timely manner.

3. Breaches other than clear-cut Level 1 breaches

- For all levels other than a clear-cut Level 1 breach, the Local Senior Manager shall notify the Medical Director's Office, attention Director of Professional Affairs or his/her designee of the alleged breach. The Local Senior Manager in consultation with the Medical Director's Office, shall establish an investigating team which will include the local senior management, and a representative from the Human Resources Department, and/or the Legal Department as either a participant or consultant.

- The investigating team shall conduct the necessary and appropriate investigation commensurate with the level of breach and the specific facts which may include, but is not limited to, interviewing the employee accused of the breach, interviewing other individuals, and reviewing documentation.

Harvard Vanguard Policy on the Disciplinary Process for Breach of Patient Confidentiality

Procedures *(continued)*

- Upon conclusion of the investigation, the investigating team shall prepare a written report, including its findings and conclusions with regard to the alleged breach and shall forward the report to the Medical Director and the Local Senior Manager for the employee. For all breaches determined to be Level 1 breaches involving physician and non-physician staff and for other levels of breach by non-physicians, the Local senior Manager, as defined above, will determine the appropriate disciplinary action. Except as otherwise provided herein, for members of the physicians group, the Medical Director will make the final decision as to the level of breach and appropriate disciplinary action. The final decision shall be communicated to the employee as appropriate.

4. Reporting and filing requirements

- For all levels of breach, after final resolution, the initial report and all written documentation relating to it shall be filed in a confidential file in the Medical Director's Office. The disciplinary action and appropriate documentation shall also be placed in the employee's personnel file.

C. Appeal Process

The following appeal processes apply when an employee is subject to a disciplinary action pursuant to this policy:

1. For Staff Handbook employees, the appeal shall begin at *Step 3* of the *Problem Resolution Procedure* as set forth in the Handbook.

2. For employees under a collective bargaining agreement, the applicable section of the collective bargaining agreement shall apply.

3. For physicians, the appeal processes set forth in the Physicians Handbook shall apply.

Harvard Vanguard Policy on the Disciplinary Process for Breach of Patient Confidentiality

Responsibility

The Medical Director is responsible for the content and administration of this policy. The policy shall be reviewed and evaluated in one year from its effective date with specific focus on the Disciplinary Process section, and then every two years thereafter.

HARVARD VANGUARD MEDICAL ASSOCIATES POLICY ON THE CONFIDENTIALITY OF CLINICAL INFORMATION AND POLICY ON THE DISCIPLINARY PROCESS FOR BREACH OF PATIENT CONFIDENTIALITY

ACKNOWLEDGEMENT

I have received a copy of the Harvard Vanguard Medical Associates *Policy on Confidentiality of Clinical Information* and the Harvard Vanguard *Policy on the Disciplinary Process for Breach of Patient Confidentiality* (collectively "the Policies"). I have read the Policies and understand their contents.

I agree to keep all Harvard Vanguard patient information as outlined in the Policies strictly confidential. I understand that breach of patient confidentiality as defined in the Policies will result in disciplinary action, up to and including termination of employment.

Employee Name (print)	**Employee Signature**
Social Security Number	**Date**

Harvard Vanguard Medical Associates

Revised 5/98

Confidentiality

Self Assessment

---

1. A patient's husband calls for the results of his wife's pregnancy test. Can you give him the results?

YES **NO**

2. A patient's wife calls to ask if her husband kept his appointment. Can you tell her?

YES **NO**

3. You wish to send a sympathy card to a coworker. Is it all right to look up his address in the medical records system?

YES **NO**

4. Do you, as a Harvard Vanguard employee and a parent, have the right to look up your own child's record?

YES **NO**

5. Can you give a spouse a copy of their husband or wife's medical records without written consent?

YES **NO**

6. Is it a breach of confidentiality if staff openly and publicly conduct a discussion of a patient's care?

YES **NO**

7. Can medical information be given when an employer calls regarding an employee's medical appointments or requesting information about an employee's absence?

YES **NO**

Confidentiality

Self Assessment

Page 2

8. Does AMRS maintain an audit trail of access to the AMRS system?

YES **NO**

9. If you see a neighbor in the health center is it all right to ask why they are there?

YES **NO**

10. If an employee who is a patient schedules an appointment, is it all right to ask what they are being seen for?

YES **NO**

11. Can a breach of confidentiality be grounds for termination of employment?

YES **NO**

12. If you overhear a conversation outside the clinical area regarding sensitive patient information, you should let the offenders know immediately that they are violating confidentiality policy.

YES **NO**

13. A clinician has the right to access any patient's medical record information, even those not under his care.

YES **NO**

Resource List

If you want to do more…

- The "Confidentiality Audits" booklet was created as a tool to monitor confidentiality and identify areas for improvement. Regular audits (related to confidentiality) help to focus attention on this important aspect of individual performance. A variety of materials are included to help staff maintain confidentiality for all patients. The booklet can be obtained from the facilitator guide to this course or from Harvard Vanguard Operations.
- Designate local experts in your site to help with confidentiality issues.
- Establish a confidentiality committee to guide and monitor policy.
- Participate in regular course offerings and conferences through Risk Management Foundation (RMF) or a professional organization, such as AMA, HSPH, MAHMO, or AHIMA.
- Stay on top of legislative initiatives.

Contacts

- Harvard Vanguard site Administrators for suspected breaches of confidentiality
- Medical records coordinators for release of information questions and problems, and to request a medical record audit
- Legal Department for legal assistance with subpoenas and sensitive case issues
- IT Customer Support Center for AMRS or EpicCare password and access help

These documents are proprietary to the Kaiser Permanente Medical Care Program.
They may only be use to assist organizations in the development of their own policies and may not be used as policies.

Examples of KPNC Policies:

1. **INTRODUCTION**
2. **CONFIDENTIALITY AND SECURITY RESPONSIBILITIES**
3. **SECURITY OF CORPORATE DATA**
4. **USE OF KPNC COMPUTING RESOURCES**
5. **DATA CLASSIFICATION**
6. **CONFIDENTIALITY OF PATIENT/MEMBERSHIP DATA**
7. **PATIENT DEMOGRAPHIC INFORMATION**
8. **CONFIDENTIALITY OF PATIENT/MEMBERSHIP FOR STAFF, EXECUTIVES, and CELEBRITIES**
9. **FAX CONFIDENTIALITY AND SECURITY**
10. **CAREGIVER-PATIENT E-MAIL COMMUNICATION**
11. **LOCAL AREA NETWORK (LAN) SECURITY**
12. **PHYSICAL SECURITY**
13. **RETENTION AND DISPOSAL OF DATA AND OUTPUT**
14. **GLOSSARY**

KPNC ICPS POLICIES, STANDARDS, AND PROCEDURES **REVISED: 04/07/98**

TITLE: INTRODUCTION

Information Confidentiality, Privacy, and Security (ICPS)

Data security is an important consideration for everyone who uses confidential or proprietary information. Kaiser Permanente Northern California (KPNC) has a legal and ethical obligation to preserve the confidentiality of its data, and the privacy of its patients, staff, and business partners.

Policy, Standard, and Procedure Development/The ICPSG

The ICPS Policies, Standards, and Procedures are developed by KPNC's Information Confidentiality, Privacy, and Security Group (ICPSG), which:

- owns KPNC's information confidentiality, privacy, and security processes (design, development, implementation strategy, and improvement)
- develops and communicates KPNC ICPS policies, standards, and procedures on all topics related to computer and data security, and information confidentiality and privacy
- works with Service Area (SA) leadership, Division Chiefs of Clinical Information Systems (DCCIS), and KP information technology organizations to:
  - develop and implement local ICPS policies, standards, and procedures which are compatible with operational and business requirements and compliant with KPNC ICPS policies, standards, and procedures
  - develop mechanisms for enforcing and monitoring compliance with ICPS policies, standards, and procedures
  - develop and implement security awareness training programs.

Scope

The ICPS Policies, Standards, and Procedures document KPNC intentions and staff responsibilities regarding information confidentiality, privacy, and security. Additionally, the ICPS Policies, Standards, and Procedures:

- augment related Regional policies by providing additional information or instructions to help interpret or clarify security-related issues
- serve as a foundation for local ICPS policies, standards, and procedures.

The ICPS Policies, Standards, and Procedures shall not supersede any other policies, standards, or procedures produced by KPNC. Local policies, standards, and procedures shall not supersede the ICPS Policies, Standards, and Procedures.

Coverage

The following persons are covered by the ICPS Policies, Standards, and Procedures:

- all employees of Kaiser Foundation Hospitals and Kaiser Foundation Health Plan, Inc., Northern California.
- all employees and physicians of The Permanente Medical Group, Inc.

- all employees of other Kaiser Permanente entities, or Program Offices, who are required to use Northern California data or data processing services during the course of their work

- all consultants, contractors, contract physicians, resident physicians, external service providers (including staff of provider institutions), volunteers, and vendors who are required to use KPNC data or data processing services.

Organization of the ICPS Policies, Standards, and Procedures

The Policies, Standards, and Procedures are divided into topics which represent major subject areas. Each document is identified by a topic abbreviation and a number. The title of the document identifies its specific subject matter.

The Table of Contents lists all of the documents by title and by number.

The Glossary defines terms which are used throughout the manual.

Publication of Documents

The ICPS policy documents are available on the public EMC2 conference "IPCS-Policies/Procs." Persons who need to be notified of the most recent versions of the documents should track the conference.

A Lotus Notes version of the documents will be developed in the near future.

These documents are for the use of KPNC only; distribution to other parties requires consent of the ICPSG.

User Comments

The ICPSG welcomes suggestions for revisions or additions to these documents. Please e-mail comments to any of the persons listed in the document "ICPSG Members" under the topic "* Introduction". The ICPSG will consider all recommendations.

KPNC ICPS POLICIES, STANDARDS, AND PROCEDURES **REVISED: 04/07/98**

TITLE: CONFIDENTIALITY AND SECURITY RESPONSIBILITIES **NUMBER: HR - 100**

POLICY

Every person who performs work for KPNC through employment, contract, residency, or as a student, vendor, or volunteer, has certain responsibilities for helping to ensure the confidentiality and security of corporate data.

RESPONSIBILITIES

A USER is any person who accesses any corporate data in any form. Each user is responsible for:
- maintaining the confidentiality of information as stated in Human Resources Policy 1.19
- complying with Regional policies, standards, and procedures including those in this document
- taking any reasonable and logical measure that is necessary to preserve information confidentiality and privacy even if it is not specifically published
- maintaining a secure work area as specified in the ICPS policy document on "Physical Security"
- safeguarding output (such as printed reports, screen prints, copies, diskettes)
- reporting an observed or suspected breach of information security (including misappropriation of cash) to management.

LOCAL DATA SECURITY OFFICER (LODSO) OR INFORMATION TECHNOLOGY PERSONNEL (title may vary) at medical facilities, service areas, and division departments are responsible for:
- ensuring appropriate management request access
- ensuring requested access is consistent with approved application guidelines and with facility/CSA guidelines
- granting, revoking, or requesting system access per local and Regional procedures.

IT SECURITY (ITSEC) is responsible for suppporting organization-wide security initiatives and for security administration.

SERVICE/FUNCTIONAL MANAGERS/SUPERVISORS oversee and are accountable for specific operational units within KPNC. These staff are responsible for:
- reviewing job responsibilities of a new or transferred employee, consultant/contractor, or other user and determining what access to functions/databases is needed within guidelines
- requesting access by the fewest users necessary to ensure completion of work
- contacting the LODSO/IT when a new user requires system access
- IMMEDIATELY notifying the LODSO/IT or IT Security when a user is terminated under sensitive circumstances
- annually reminding users of KPNC's confidentiality policies as required by Human Resources Policy 1.19
- informing users under their supervision of changes in policies, standards, or procedures
- complying with responsibilities detailed for each USER

The TRUSTEE is the party responsible for leading, managing, and administering activities related to an application from a user perspective. For information security, the Application Trustee is accountable for:
- determining how a business application and its data are used and developing and communicating application-specific policies, standards, and procedures that are consistent with KP policies, standards, and procedures
- identifying and monitoring for appropriateness the set of authorized users of the application and its data stores
- auditing use of and access to the application and data
- working with local or departmental management to take corrective action in the event of inappropriate or unauthorized use.

INFORMATION CONFIDENTIALITY, PRIVACY, AND SECURITY GROUP (ICPSG) represents major organizational groups within KPNC irrespective of the organizational entity. The ICPSG is responsible for

establishing, maintaining, and monitoring compliance with policies, standards, and procedures as well as discussing and resolving issues related to information security.

KPNC ICPS POLICIES, STANDARDS, AND PROCEDURES **REVISED: 04/07/98**

TITLE: SECURITY OF CORPORATE DATA **NUMBER: GE - 100**

POLICY

KPNC will protect the data and information it collects and maintains from unauthorized access, disclosure, modification, and destruction.

STANDARDS
---
1. KPNC will take all reasonable and appropriate measures to protect its corporate data assets against accidental or unauthorized modification, disclosure, or destruction, including the security of the equipment, software, and data.

2. Observance of data security policies, standards, and procedures is a condition of employment and failure to comply with the intent or specifics of these documents will result in disciplinary action up to and including termination.

3. Certain organizational units have responsibilities for gathering and distributing data to public agencies and/or the media. These include, but are not limited to, departments dealing with human resources, public affairs, accreditation and regulation, and facilities development. These departments are governed by specific policies that cover disclosure of material within their areas of responsibility.

4. Each manager is expected to establish, publish, and enforce departmental standards and procedures to:

   a. prevent unauthorized collection, disclosure, modification or destruction of data

   b. develop and maintain data security awareness among subordinates.

5. All data processing resources (e.g., software, servers, data) which are owned, used, or maintained by KPNC shall be properly secured in accordance with these standards.

REFERENCES/RELATED DOCUMENTS

ICPS Policies, Standards, and Procedures:

HR-100 "User Responsibilities"
GE-110 "Confidentiality of Patient/Membership Data"

Online Sources:

REG.Policies/Proced (EMC2 conference)

Other Manuals:

Human Resources Policy Manual

KPNC ICPS POLICIES, STANDARDS, AND PROCEDURES **REVISED: 04/07/98**

TITLE: USE OF KPNC COMPUTING RESOURCES **NUMBER: GE - 105**

POLICY

Kaiser Permanente, Northern California (KPNC) computing resources (systems and data) are provided for the singular purpose of facilitating patient care and business processes.

Any person who uses KPNC computing resources for non-business or unauthorized purposes may be subject to disciplinary measures up to and including termination and civil or criminal legal action.

Management at all levels are responsible for monitoring the actions of their staff and enforcing the intent of this policy.

STANDARDS
---

1. The following are examples of prohibited activities:

    a. using KPNC computing systems or data for personal business or gain

    b. unauthorized browsing of patient, personnel, financial, or other corporate information (e.g., for the purpose of satisfying personal curiosity or with the intent of improperly disclosing that information)

    c. interfering with the operation of any KPNC computing system, or using a KPNC computer to disrupt any external computing system

    d. altering or deleting data or software, except when performing authorized business functions

    e. installing unauthorized or illegally-copied software.

2. Actions of computing system users may be monitored by system administration or user management at any time.

3. Every user is accountable for all computing activities s/he performs.

4. Users shall take the following precautions to safeguard systems and data:

    a. user identification codes are not to be shared, except under special circumstances approved by the Information Confidentiality, Privacy, and Security Group.

    b. passwords shall not be divulged, orally or in writing

    c. workstations and terminals to be left unattended shall be logged off or locked up.

    d. all suspected or known breaches of confidentiality or computer security shall be reported to management immediately.

5. Management will instruct users in Information Confidentiality, Privacy, and Security (ICPS) policies, standards, and procedures; and the principles of information confidentiality and computer security.

6. Management shall make ICPS policies readily available to staff.

7. Users are expected to be able to refer to the ICPS policies as appropriate (e.g., when a question arises regarding output disposal).

8. Business data (including patient records) may only be disclosed under the direction of SA or TPMG management in accordance with corporate procedures and legal or regulatory requirements.

REFERENCES/RELATED DOCUMENTS

ICPS Policies, Standards, and Procedures:

All documents, as found in ICPS-Policies/Procs (EMC2 conference)

Other Manuals:

Human Resources Policy Manual

1. KPNC ICPS POLICIES, STANDARDS, AND PROCEDURES **REVISED: 04/07/98**

TITLE: DATA CLASSIFICATION **NUMBER: GE - 115**

POLICY

All corporate data, regardless of medium, will be classified according to its value and level of sensitivity.

RESPONSIBILITIES

Trustees are responsible for classifying data, and for ensuring that access audit reports are being monitored.

The Information Confidentiality, Privacy, and Security Group (ICPSG) is responsible for approving classifications of groupings of related data.

IT Security will consult with the Trustee and application developer to define control mechanisms for classified data.

STANDARDS
---

1. General
   ---
   a. Classification refers to a value assigned to data based upon the data's real monetary cost or cost to replace, and the degree to which disclosure or misuse could damage a patient, customer, business partner, or KPNC.

   b. The classification/level of sensitivity determines the access controls to be placed upon the data.

   c. Within general categories of data (e.g., patient medical record), some data may be considered more sensitive or critical than others. Some information in the patient medical record, mental health) therapeutic abortion) could be especially damaging to the patient if accidentally or intentionally disclosed. Therefore, this data shall have a higher level of classification.

2. Classes of Data
   ---
   a. PUBLIC

      Examples: publications to customers; press releases

      Classification Criteria: none

      Access Protocol: available to the general public

      Encryption: not required

      Auditing: none.

   b. INTERNAL

      Classification Criteria: disclosure may cause some harm to KPNC or its customers

      Examples: internal phone directories; organizational memos; announcements; procedures

      Access Protocol: generally available to all staff on a need-to-know basis

      Encryption: required if transmitted via Internet

      Auditing: none.

c. CONFIDENTIAL

Classification Criteria: disclosure may cause some harm to KPNC or its customers

Examples: patient laboratory, treatment, admissions, visit, appointment data (except for that which is REGISTERED CONFIDENTIAL); customer/vendor files

Access Protocol: limited to as few persons as possible, on a need-to-know basis

Encryption: required if transmitted via Internet

Auditing Criteria: accesses should be audited as determined by Application Trustee and ICPSG.

d. REGISTERED CONFIDENTIAL

Classification Criteria: disclosure may cause severe harm to KPNC or its customers

Examples: mental health/substance abuse treatment data; strategic corporate plans/financial information; payroll, benefits, and personnel data

Access Protocol: limited to as few persons as possible, on a need-to-know basis

Encryption: required if transmitted via Internet

Auditing: all accesses should be audited.

REFERENCES/RELATED DOCUMENTS

ICPS Policies, Standards, and Procedures:

AP-285 "Mental Health Data Access"

KPNC ICPS POLICIES, STANDARDS, AND PROCEDURES **REVISED: 04/07/98**

TITLE: CONFIDENTIALITY OF PATIENT/MEMBERSHIP DATA **NUMBER: GE - 110**

POLICY

KPNC recognizes its duty to provide adequate safeguards for the data it collects and uses. Standards and procedures will be implemented to assure all patients/members/membership applicants that this data:

. shall be held in confidence
. shall be available only to authorized parties.

STANDARDS
---
1. General
   ---
   a. "Patient/membership data" is any data which can be associated with one or more specific patients or Health Plan members/applicants. These concepts apply irrespective of the recording media.

   b. All patient/membership data recorded by or transferred to KPNC is the property of KPNC.

   c. All patient/membership data is confidential.

   d. Patients/members/applicants may obtain copies (paper or machine-readable) of their own patient/membership data from local Health Information Management organizations in accordance with division procedures.

   e. Clinical data may only be updated via addenda. It may not be altered or deleted.

   f. Inactive patient/membership data will be archived and retained in accordance with division procedures and legal requirements.

   g. The manner in which patient/membership data is created and maintained will comply with all laws and regulations.

   h. Inappropriate access to or use of patient/membership data is forbidden and may result in disciplinary action up to and including termination and possible criminal prosecution.

   i. Witnessed inappropriate access to or use of patient/membership data must be reported to management.

   j. Management at all levels is responsible for ensuring that data is accessed and used appropriately.

2. Access

   Employees, physicians, contractors, volunteers, and any other parties affiliated with KPNC will be given access to patient/membership data limited to the requirements of their jobs.

3. Confidentiality
   ---
   a. Patient/membership data shall be protected from unauthorized disclosure.

   b. Employees, physicians, contractors, volunteers, and any other parties affiliated with KPNC must hold in confidence any patient/membership data.

4. Security
   ---

a. Hardware, software, and procedural controls will be implemented to ensure that patient/membership data is protected from accidental or inappropriate access, disclosure, modification, or destruction.

b. Access to patient/membership data will be monitored.

REFERENCES/RELATED DOCUMENTS

ICPS Policies, Standards, and Procedures:

GE-110 "Data Classification"
GE-500 "Physical Security"
HR-100 "User Responsibilities"

Online Sources:

REG.Policies/Proced (EMC2 conference)

Other Manuals:

Human Resources Policy Manual

KPNC ICPS POLICIES, STANDARDS, AND PROCEDURES **REVISED: 04/07/98**

TITLE: PATIENT DEMOGRAPHIC INFORMATION (PATDEM) **NUMBER: AP - 200**

INTRODUCTION

The Patient Demographic Information (PATDEM) database is used throughout KPNC to view patient demographic information online.

These policies and standards are intended for PATDEM users as well as individuals responsible for administering access to PATDEM.

SCOPE

The policies and standards pertain to all users and uses of PATDEM data and related functions.

Other applications (e.g., PARRS, ADT/CABS, Reg Plus) should adhere to the principles of these policies and standards. When PATDEM data is downloaded or used outside the application, it should receive the same precautions as it does within the PATDEM production application.

RESPONSIBILITIES

General responsibilities regarding the use of PATDEM are enumerated in ICPS Policy HR-100, "Confidentiality and Security Responsibilities."

POLICY

The PATDEM database contains KPNC patients' addresses, phone numbers, and other personal information classified CONFIDENTIAL. Only staff who are directly involved in patient care or who have demonstrated a genuine business need may access this data.

STANDARDS
---
1. Assigning Access to PATDEM
   ---
   a. PATDEM access will be limited to staff who provide direct patient care, who need to contact patients, or who are doing analytical studies requiring residence, age, gender, or other demographic information.

   b. All requests for access for persons whose job functions are NOT as described above MUST be approved by the Trustee.

   c. Involuntary termination of an employee requires immediate deletion of that person's access to PATDEM.

   d. Access shall be granted to the fewest users necessary to ensure completion of work.

2. Assigning Access to the PATDEM Data Stores
   ---
   a. Data stores (including the Management Data Repository, or MDR) contain data which is used for management reporting. Users are granted access to PATDEM data stores according to their job requirements.

   b. Access to the data stores must be approved by user management based upon local and KPNC protocols.

3. Use of PATDEM
   ---
   a. Users shall ensure that any data they access in PATDEM is, to the to the best of their knowledge, accurate, complete, and up-to-date.

b. Purposely falsifying or deleting any PATDEM data is grounds for discipline.

c. The data fields in PATDEM shall be used only for the purposes for which they are intended.

4. Accountability
---

a. Each user is accountable for transactions performed under his/her user ID in PATDEM.

b. To ensure accountability, each user shall have an individual user ID and confidential password. Shared UICs are not permitted for PATDEM.

5. Confidentiality and Privacy
---

a. Policies, standards, and guidelines for security and confidentiality established by the Information Confidentiality, Privacy, and Security Group (ICPSG) must be complied with at all times.

b. PATDEM data will be used by authorized staff only in the conduct of KPNC business, in accordance with local and division policies. Any other use is forbidden.

c. KPNC expressly prohibits indiscriminate or unauthorized access to or disclosure of personal information, medical or otherwise, from any source regarding a patient or employee.

d. Users shall abide by provisions in Human Resources Policy 1.19 in maintaining confidentiality of information.

6. Local Policies, Standards, and Procedures

Facility- or CSA-level policies, standards, and procedures related to PATDEM are to comply with these policies, standards, and procedures.

7. Printed PATDEM Records

Any printed matter which displays patient demographic information which is not filed in the patients' Chart/Medical Record must be secured, destroyed in a manner which prevents reconstruction, or given to the patient.

8. PATDEM Data Shared with Other Applications

When PATDEM's data is shared with other applications for authorized organizational purposes, the acquiring applications and their databases shall follow security standards that are at a minimum comparable with these PATDEM-specific policies, standards, and procedures.

9. PATDEM Data Shared with Other Institutions

PATDEM data may only be released to other institutions (e.g., governmental agencies, other providers) in accordance with division policies and procedures.

10. Monitoring Access to PATDEM
---

a. The Trustee and ITSEC will develop procedures and tools for monitoring compliance with the policies and standards described in this document. The LODSO/DP and functional manager/supervisor will be notified of cases of noncompliance and will be asked to take appropriate action.

b. Logging:

1) Every update to PATDEM is logged.

2) All read accesses to PATDEM via the "Patient Information" online function are logged.

3) Patients who are concerned over who may have accessed his/her records should contact his/her caregiver. Caregivers who receive patient complaints/concerns, or staff who suspect security breaches should contact their local Health Information Manager (HIM).

c. Local Health Information Management staff may contact ITSEC to request access reports.

d. ITSEC will generate facility- and department-specific lists of users with access to the application and the MDR periodically. The LODSO/DP and local/departmental management will review for appropriateness of user IDs and menu items as related to job responsibilities no less than annually.

REFERENCES/RELATED DOCUMENTS

ICPS Policies, Standards, and Procedures:

HR-100 "Confidentiality and Security Responsibilities"
AP-100 "Acquiring, Controlling, and Possessing UICs"

Other Manuals:

Human Resources Policy Manual

KPNC ICPS POLICIES, STANDARDS, AND PROCEDURES **REVISED: 04/07/98**

TITLE: CONFIDENTIALITY OF PATIENT/MEMBERSHIP DATA FOR STAFF/EXECUTIVES/CELEBRITIES **NUMBER: GE - 120**

POLICY

Every patient's data and information is considered highly confidential. No special technical controls are placed upon data belonging to Kaiser Permanente Northern California (KPNC) staff or executives, or well-known persons (celebrities). However, KPNC staff must be aware of operational precautions which must be taken with regard to certain patients' data.

STANDARDS
---
2. Persons who have cause to access data associated with KPNC staff members or executives, or celebrities, will do so only in the course of providing medical services. Company policy, law, and regulation forbid any user of KPNC data processing systems from viewing any patient's records except as necessary in relation to the provision of medical services.

3. Managerial staff may **not** access online systems to review the records of subordinates for any reason **except** for the provision of necessary medical care.

4. Unauthorized access (such as casual or curious browsing) of patient records is grounds for disciplinary action up to and including termination and possible criminal prosecution.

5. Any staff member who knowingly divulges **any** patient's data to a non-authorized party is subject to disciplinary action up to and including termination and possible criminal prosecution.

6. Management will ensure that staff have been informed of the need to be especially cautious when providing services for celebrities. Reporters may misrepresent themselves as family members in order to obtain information about well-known patients. Inquiries regarding celebrity patients must be referred to local external affairs departments in accordance with local and division procedures.

Records of access to staff, executive, or celebrity patient data may be monitored regularly and/or at the discretion of management.

KPNCR ICPS POLICIES, STANDARDS, AND PROCEDURES **ISSUED: 10/10/96**

TITLE: FAX CONFIDENTIALITY AND SECURITY **NUMBER: GE - 860**

POLICY

All staff shall take precautions when using facsimile (fax) machines to transmit documents. Certain documents shall not be faxed.

STANDARDS
---
1. Fax machines shall not be located in areas accessible to the general public.

2. Staff shall not use company fax machines for transmitting personal documents.

3. Fax cover pages shall include the following information:

   a. the sender's name, business address, business phone number, and business fax number

   b. the recipient's name, business address, business phone number, and business fax number

   c. transmission time and date (if not stamped by fax or computer)

   d. classification of the document (for CONFIDENTIAL and REGISTERED CONFIDENTIAL documents).

4. Staff shall verify the fax number of the recipient before transmitting.

5. A recipient of a document containing REGISTERED CONFIDENTIAL information (e.g., for the recipient's eyes only, or containing patient-identifiable information pertaining to mental health or chemical dependency care) must be notified by phone before the document is transmitted. If at all possible, this type of document should not be faxed.

6. All pages plus the cover page of all CONFIDENTIAL documents to be faxed must be marked "Confidential" before they are transmitted.

REFERENCES/RELATED DOCUMENTS

ICPS Policies, Standards, and Procedures:

GE-115 "Data Classification"

KPNC ICPS POLICIES, STANDARDS, AND PROCEDURES **REVISED: 04/07/98**

TITLE: CAREGIVER-PATIENT E-MAIL COMMUNICATION **NUMBER: AP - 810**

POLICY

KPNC encourages caregivers to communicate with their patients via electronic mail (e-mail) and requires caregivers to comply with certain rules regarding e-mail.

DEFINITIONS

E-MAIL comprises any text messages which are transmitted electronically between computers.

RULES FOR PATIENT-CAREGIVER E-MAIL
---
1. Both caregiver and patient must agree to communicate via e-mail.

2. The patient must be informed of rules and guidelines for e-mail communication.

3. E-mail should not be used for urgent communications (e.g., regarding sudden or substantive changes in the patient's health). Patients must be informed that if their messages are not answered in that they consider to be a reasonable period of time, the addressee may not be at work. Another method of communication should then be used.

4. All communications must begin with the patient's full name and medical record number.

5. Patients must understand that messages may not necessarily be confidential. Messages can be misdirected to or intercepted by unintended parties.

6. Caregivers will take all reasonable precautions to ensure that e-mail responses to patients are not misdirected or otherwise become available to unintended parties.

7. Clinically relevant messages and responses will be documented in the medical record.

COMPLIANCE

Failure to comply with this policy will result in disciplinary action up to and including termination and possible criminal prosecution.

KPNC ICPS POLICIES AND STANDARDS **REVISED: 04/07/98**

TITLE: LOCAL AREA NETWORK (LAN) SECURITY **NUMBER: TE - 200**

RESPONSIBILITIES

General user/management responsibilities are enumerated in ICPS Policy HR-100, "Confidentiality and Security Responsibilities."

Information Technology Leaders (ITLs)/Department Managers:
---
1. approve and enforce SA or department-level LAN security policies and procedures

2. appoint and manage LAN administration teams

3. ensure compliance with KPNC LAN security standards.

LAN System Administrators:
---
1. properly configure LANs and workstations to ensure compliance with the security standardsdocumented herein

2. understand the licensing agreements for software installed on the LANs, and will ensure that illegal software is never used

3. develop and recommend local LAN security policies, standards, and procedures.

LAN Security Administrators:
---
1. develop and maintain procedures to add and delete users on the user database.

2. develop and maintain procedures for applying access controls to new and/or modified applications and data.

3. train users in LAN security procedures.

4. review audit reports and notify LAN system administration and user management of any suspicious activities.

5. regularly review the security controls of the LAN and ensure that they are functioning properly.

LAN Users:
---
1. understand the need for LAN system and data security

2. comply with KPNC and local LAN security policies and standards

3. report security problems or breaches to LAN administration, local data processing, or IT Security.

POLICY

KPNC will take precautions to safeguard the hardware, software, data, and mainframe entry points used by Local Area Networks (LANs).

STANDARDS
---
1. General

SA Information Technology Leaders (ITLs) or department managers are responsible for ensuring that appropriate LAN security control mechanisms are implemented for all LANs.

2. Physical Security
---

a. LAN servers must be located in physically secure areas. Entry to server areas will be limited to the LAN system administrator and/or other persons designated by the ITL or department manager.

b. Persons not assigned to the LAN administration team (e.g., other KPNC staff, vendors, repair persons, etc.) may not enter the secured server area unless accompanied by a member of the LAN administration team or facility security.

3. LAN Management/Configuration
---

a. Information Technology Leaders (ITLs) will ensure that LAN system administration activities are appropriately segregated from LAN security administration.

b. LANs may be used to access mainframe systems only through approved gateways.

c. Server and workstation configuration shall only be performed by an authorized member of the LAN system administration team.

d. Servers and workstations must be configured to prevent users from:

1) booting the system from diskettes

2) installing unauthorized software

3) modifying system configuration files

4) modifying access control lists for system files or files belonging to other users.

e. Use of a LAN to gain remote dial access to mainframe systems is forbidden, unless the LAN is equipped to verify the identity of the incoming caller.

f. KPNC-approved virus detection/eradication software will be installed on all LANs and workstations.

4. User Identification/Authentication
---

a. Each user must sign on to the LAN with a unique user ID. User IDs may not be shared.

b. Guest accounts must be disabled whenever possible. If guest accounts must exist, their use must be controlled by the LAN system administrator or LAN security administrator.

c. Passwords must expire no more than every 35 days.

d. Passwords must be at least 6 characters long.

e. The LAN security application must disallow re-use of the 5 most recently-used passwords.

f. The LAN security application must disallow use of common or easily-guessed passwords (e.g., user ID, user name, etc.).

g. A user must be able to change his/her own password, but no more than once per day.

h. A user ID will be suspended after 3 invalid attempts to enter a correct password.

i. Users are forbidden from automating password entry (i.e., programming a PF key to type in the password).

5. Data Access and Security
---

a. LAN security administrators will apply appropriate access control lists (ACLs) to ensure that locally-stored data may be accessed only by those persons who need the data to perform their job functions.

b. Only data which is of a business nature may be maintained on workstations or servers.

c. Users will be trained to apply access controls to their personal business files.

6. Auditing/Monitoring
---

a. LAN security administrators reserve the right to conduct periodic spot audits of workstations and to remove any applications or data which has been placed there inappropriately.

b. The ITL or department manager will determine which LAN activities or data access must be monitored. The LAN system administrator will configure the system to log these activities/accesses and to produce reports.

c. LAN system and/or security administrators will monitor LAN user activity (including system and data access) in accordance with KPNC and local policy. Inappropriate activities will be reported to user management.

REFERENCES/RELATED DOCUMENTS

ICPS Policies, Standards, and Procedures:

HR-100 "Confidentiality and Security Responsibilities"

KPNC ICPS POLICIES, STANDARDS, AND PROCEDURES **REVISED: 03/31/97**

TITLE: PHYSICAL SECURITY **NUMBER: GE - 500**

POLICY

Management will establish rules and procedures to ensure that all staff maintain a secure work area, i.e., one in which which physical security helps to protect the confidentiality and privacy of information.

STANDARDS
---
1. Where feasible, workstations/terminals will be positioned or shielded so that screens are not visible to the general public or unauthorized staff.

2. Users will use the "soft timeout on demand" feature to clear the screen if the workstation/terminal must be left briefly unattended.

3. Users shall sign off/power off workstations/terminals when not in use or when leaving the work area for breaks or at the end of the day.

4. Any electronic media being discarded or replaced (including hard drives in workstations) shall be written over, degaussed, or irrecoverably destroyed to ensure proper erasure of confidential or proprietary data.

5. Users shall secure media (such as hard copy, diskettes, etc.) which contain confidential information in a locked desk, cabinet, or room.

6. Management shall provide users with facilities (shredders, secured bins, etc.) for proper disposal of confidential printouts. Users shall dispose of printouts at these facilities.

7. Users shall print documents only when necessary.

8. Copying of confidential documents shall be minimized.

9. Management and users will take any other reasonable and logical measure necessary to maintain a secure work area, even if this measure is not specifically enumerated above.

REFERENCES/RELATED DOCUMENTS

ICPS Policies, Standards, and Procedures:

HR-100 "User Responsibilities"
GE-550 "Retention and Disposal of Data and Output"

KPNC ICPS POLICIES, STANDARDS, AND PROCEDURES **REVISED: 04/07/98**

TITLE: RETENTION AND DISPOSAL OF DATA AND OUTPUT **NUMBER: GE - 550**

POLICY

Data and output will be retained and/or disposed of according to the requirements of external regulatory agencies, KPNC policies, and KPNC organizational units.

STANDARDS
---
1. Policies and instructions regarding the retention, storage, and destruction of certain types of records are covered by Procedure 96A, "Retention and Disposal of Records." This standard does not supersede RP-96A, but provides additional information relating to other types of data.

2. Certain organizational units (e.g., Division of Research) have special needs, which may exceed regulatory requirements, for historical data and output. Their requirements must be considered before retention periods are determined. Contact representatives of appropriate organizational units if any data or output being considered for disposal has potential value as research material.

3. Data and output to be retained must be secured from inappropriate access.

4. In the event that there are no regulatory agency requirements for data/output retention, the retention periods will be determined by local organizational units, upon consultation with ITS.

5. Printed material which contains:

. personally identifiable patient information (e.g., patient name, medical record number, address, phone number, social security number;
. personal or employment-related information for staff members; or
. company-confidential information (any information which, if released prematurely or at all, could cause harm to the company

shall be disposed of in a manner that ensures confidentiality.

6. Secure methods will be used to dispose of data and output. For example:

   a. confidential printed material shall be shredded and recycled by a firm specializing in the disposal of confidential records

   b. all other paper should be recycled when possible

   c. on-line data must be deleted by using appropriate utilities

   d. computer tapes must be written over or "degaussed" to prevent recovery of data

   e. mainframe disk drives being sold or replaced must be written over using initialization utilities

   f. diskettes to be re-used must be written over or erased using a special utility to prevent recovery of data

   g. diskettes to be discarded must be cut into pieces

   h. microfilm or microfiche must be cut into pieces or chemically destroyed.

REFERENCES/RELATED DOCUMENTS

ICPS Policies, Standards, and Procedures:

GE-500 "Physical Security"

Related Regional Policies and Procedures:

86A "Retention and Disposal of Records"

GLOSSARY

ADMIT, DISCHARGE, AND TRANSFER (ADT) is a business/clinical application that collects, maintains, and reports daily activity for inpatients, outpatient surgeries, and other outpatient services for all Northern California Kaiser Permanente facilities.

BUSINESS APPLICATION is a group of automated transactions used to accomplish a specific business function.

CASE ABSTRACTING SYSTEM (CABS) is a business/clinical application that receives data from ADT and further enables data to be analyzed and coded.

CONFIDENTIALITY is the practice of protecting information from disclosure to unauthorized individuals, entities, or processes.

CUSTOMER INFORMATION CONTROL SYSTEM (CICS) is an IBM product through which automated business applications are presented to the user.

DATA STORE is a repository of business data from which data can be read repetitively and non-destructively. Data includes binary objects such as documents, images, voice records, and motion video as well as coded data elements (text, numbers, dates, etc.).

DATABASE 2 (DB2) is an IBM product which is used to store and manage data. Date stored in DB2 database tables is arranges into virtual groups or "views." Authorized users can access data in these views to create reports.

INFORMATION CONFIDENTIALITY, PRIVACY, AND SECURITY GROUP (ICPSG) represents major organizational groups within KPNCR irrespective of the organizational entity. The ICPSG is responsible for establishing, maintaining, and monitoring compliance with policies, standards, and procedures as well as discussing and resolving issues related to information security. The ICPSG is accountable to the IT Enterprise Board.

INFORMATION SECURITY is the practice of protecting information from accidental or malicious access, modification, destruction, or disclosure. Security embodies both protections for confidentiality and data integrity.

INFORMATION SECURITY CONTROLS are any measures taken to protect information. These could include administrative controls such as establishing policies, standards, and procedures as well as monitoring logs of activity. These could also include physical security, such as devices and positioning of terminals. Security controls are the administrative and technical techniques and methods used to ensure that only authorized users can access the computer system and its resources and that the overall environment ensures the integrity, availability, and confidentiality of system resources.

INFORMATION TECHNOLOGY SECURITY (ITSEC) is the business process responsible for ensuring that users receive access to mainframe business applications and data.

The INTERNET is the international electronic infrastructure which permits diverse, non-connected computer systems ("hosts") to communicate, share computing resources, and share data with one another.

KAISER PERMANENTE PERSONNEL comprise all staff persons or physicians employed or contracted by Kaiser Foundation Hospitals, Kaiser Foundation Health Plan, or The Permanente Medical Group.

LOCAL DATA SECURITY OFFICER/INFORMATION TECHNOLOGY (LODSO/IT) is a person in a division department or at a medical facility whose job assignment is to: assist users in gaining access to business applications and data, performing first-level trouble shooting for security problems (e.g., resetting passwords), and assisting management in verifying the appropriateness of user access.

MANAGEMENT DATA REPOSITORY (MDR) contains historical data for a number of business applications. Persons in management and analytical job functions use MDR data to generate reports to support decision-making processes and regulatory reporting requirements.

MEDICAL CENTER SYSTEMS MENU (MCS MENU) provides each user with a list of medical center functions s/he may access. The menu appears automatically when the user signs on.

NEED TO KNOW refers to limiting access to data only to personnel performing specific business requirements.

PASSWORD is a unique, confidential string of characters, with a minimum of four and maximum of eight characters. The purpose of a password is to verify or authenticate the identify of the user. The security system prompts the user to change the initial password assigned when the user ID is established and periodically thereafter.

PRIVACY is the right of an individual or organization to determine whether, when, and to whom personal or organizational information is released.

TRUSTEE is the person or group who is accountable for: determining how a business application and its data are used, identifying and monitoring the set of authorized users, auditing use of and access to the application and data, and taking corrective action in the event of inappropriate or unauthorized use.

USER ID is the identifier which allows a user to sign on to computer systems. Each user has a user ID, which identifies him/her to the computer system, and a password, which verifies the user's identity.

MAYO CLINIC POLICY ON CONFIDENTIALITY

Purpose

This policy provides general confidentiality guidelines for Mayo Medical Center.

Policy

It is critically important to maintain patient confidentiality (see Medical Records Access Policy), as well as to maintain confidentiality about Medical Center employees and business information. This policy pertains to all information (oral, paper-based, and electronic) related to the operation of the Medical Center including, but not limited to:

- Financial information
- Patient names and other identifying information
- Patient personal and medical information
- Patient billing information
- Employee names, including salaries and employment information
- Proprietary products and product development
- Marketing and general business strategies
- Any discoveries, inventions, ideas, methods, or programs that have not been
- Publicly disclosed

In addition to the above, any information that has been marked "confidential" by the Medical Center will be deemed to be covered under this policy.

Unauthorized access, use, or release of confidential and sensitive information to non-authorized individuals is strictly prohibited and may result in immediate disciplinary action up to and including termination.

Maintaining confidentiality is the responsibility of all Mayo staff members. The responsibility includes assuring compliance with Mayo's policies for confidentiality by non-Mayo employees performing work at, or for Mayo. Non-Mayo employees, working with Mayo, must be informed of their obligations regarding Mayo confidentiality policies and agree to consequences appropriate to any breaches by them of Mayo confidentiality policy. Contracts should include references to the policy and consequences of breach. Nondisclosure and confidentiality agreement documents should be used to assure Mayo security.

Human Resources, in order to better protect employee interests, will implement guidelines for the release of sensitive information. Sensitive information is defined as W-2 Statements, Statements of Earnings (SOEs), hand-drawn checks, home addresses and phone numbers, work locations and phone numbers, and salary information.

To protect employees, Statements of Earnings, checks, W-2 copies, payroll history copies, and other personal information requested from Human Resources will require a signature and picture ID when being picked up from the above offices.

Procedure

Employees who have a reasonable basis to believe that a breach of confidentiality has occurred should report the incident as soon as possible to any of the following:

- Immediate Supervisor
- Administrator
- Human Resources
- Data Security Officer

Employees who have a reasonable basis to believe that a breach of confidentiality has occurred but do not report it are subject to corrective action. An investigation will be conducted by administration responsible for monitoring the performance of the individual suspected of breaching confidentiality. All information gathered from the investigation will be reviewed with the appropriate member(s) of management, the Data Security Officer, the Human Resources Service Partner, and Legal Counsel, if warranted. These individuals will document the investigation and determine what corrective action is to be taken, which may include, but is not limited to, suspension or termination of employment. Under no circumstances will retaliation or intimidation of a complainant be tolerated.

COMPUTER AND INTERNET USE

Purpose

This policy provides guidelines for the use of Mayo computers, the Mayo Network, and the Internet via the Mayo Network.

Policy

Use of the Mayo Network (including Dial-In services and Internet access), computers, and data center must be primarily for Mayo business-related activity or professional development. Limited personal use is acceptable but discretion is necessary to ensure that individuals do not degrade Mayo's public image through their activities, adversely affect the availability of network resources, or disrespect the rights of other individuals at Mayo. Be aware that items posted to Internet bulletin boards, mailing lists, etc., are identified by your Mayo Foundation electronic address. Do not post anything that could be misconstrued as an endorsement by the Mayo Foundation, or could reflect negatively on Mayo.

When using the Internet via the Mayo Network, users should adhere to the Mayo Foundation Standards of Personal Conduct. Material that would be considered inappropriate, offensive, or disrespectful to others should not be accessed or stored. The electronic environment is part of the workplace and carries with it the same expectation of mutual respect and confidentiality that applies to all other activities at Mayo.

Mayo's computer resources (including access to the Internet and electronic mail) must be used appropriately. Inappropriate use includes but is not limited to the following activities:

- Personal business or gain
- Solicitation of Mayo employees
- To provide information about, or lists of, Mayo employees and/or patients
- To individuals outside the Mayo organization
- To send any form of chain letter to other individuals
- To install or access any non-work-related software

Any use of Mayo computing resources and/or the Internet which interferes with the work of any employee at Mayo is prohibited. Any computer activity which constitutes a violation of the above guidelines or Mayo's Data Security Policies and Standards is strictly prohibited. Infractions will be addressed through Mayo's corrective action policy and may result in immediate suspension or termination of employment.

Procedure

Employees who have a reasonable basis to believe that inappropriate access or use of the Mayo Network/Internet has occurred should report the incident as soon as possible to any of the following:

- Immediate Supervisor
- Administrator
- Human Resources
- Data Security Officer

Employees who have a reasonable basis to believe that a violation has occurred but do not report it are subject to corrective action. An investigation will be conducted by administration responsible for monitoring the performance of the individual suspected of violating Mayo's standards. All information gathered from the investigation will be reviewed with the appropriate member(s) of management, the Data Security Officer, the Human Resources Service Partner, and Legal Counsel, if warranted. These individuals will document the investigation and determine what corrective action is to be taken, which may include, but is not limited to, suspension or termination of employment. Under no circumstances will retaliation or intimidation of a complainant be tolerated.

CORRECTIVE ACTION

Purpose

This policy sets forth a set of guidelines for the Corrective Action process to be followed when an employee has performance, attendance or behavior problems that interfere with work, patient care or operations of the Medical Center.

Policy

Corrective Action should be used to correct inappropriate behavior. Supervisors are responsible for accurate and timely documentation of inappropriate behaviors or performance issues. Corrective Action should be used consistently. Supervisors should identify and inform employees of:

- What is expected behavior and the performance standards of their job
- When they are not meeting these expectations
- What must be done to correct the inappropriate behavior and an improvement plan with a time line for its accomplishment
- Consequences if improvement does not occur

The corrective action process is meant to assist employees in recognizing the seriousness of their behavior and encouraging their commitment to changing these

behaviors. In many situations, informal counseling may be utilized by the supervisor to resolve issues prior to the formal corrective action process.

An informal counseling is used by management as a reminder to employees of Mayo policies and practices. Supervisors can utilize informal counseling to explain the performance expectations of the job to the employee who is not meeting the performance standards or job requirements. Notes of an informal counseling should be retained by the supervisor and may be referenced at a later time. Supervisors may choose to have the employee acknowledge the informal counseling session in writing by initialing the note.

Supervisors must complete a Corrective Action Conference form after each formal step of the process. Employees will be asked to sign this form indicating that they have had an opportunity to review it. If an employee elects not to sign, this should be noted on the form. Employees should be given a copy. The Corrective Action Conference form is sent to Human Resources, where it will be placed in the employee's file. If the documentation regarding discipline is not related to Equal Employment Opportunity legislation, including Sexual Harassment, it will be removed two years after the date of the incident, unless a related offense is repeated during this time.

In some cases, an immediate suspension pending an investigation is appropriate. There may be situations where an employee may be terminated without progressing through the steps outlined in this policy. Some steps can be repeated or omitted if the facts of the situation warrant it. Human Resources may be contacted as a resource for any issues that arise.

Procedure

Step 1 - Supervisor's Conference (may coordinate with Human Resources). This step serves as a reminder to the employee as to the behavior that is expected of them. The goal of the meeting is to insure that there is both understanding and commitment by the employee to correct the inappropriate behavior.

Step 2 - Written Warning (encouraged to coordinate with Human Resources). During this meeting, the supervisor should stress the seriousness of this action and what is expected behavior. The employee should be informed that should similar behavior reoccur, she/he will face additional disciplinary action up to and including termination of his/her employment with Mayo Medical Center.

Step 3 - Suspension Without Pay (required to coordinate with Human Resources). As with all previous steps, the problem should be identified along with an indication of what is the expected behavior. (Be sure that this is clear to the employee.) Any previous incidents of similar nature resulting in discipline should be reviewed along with the conclusions reached at those meetings. The employee must realize that a suspension without pay normally is a "last chance" and that future incidents of a similar or related nature will likely result in their termination from employment with Mayo Medical Center.

Step 4 - Termination (required to coordinate with Human Resources). Termination of employment by its very nature is the most severe form of discipline that can be imposed. The facts surrounding the rule infraction or unacceptable behavior must be investigated before a termination proceeding is finalized.

Process to Appeal Corrective Action

Employees who wish to appeal disciplinary action, may use the Appeals Procedure. For more information contact your Human Resource Service Partner.

Guidelines for Corrective Action

The following are meant to give assistance to supervisors in assessing the seriousness of an offense, provide consistency, and establish the appropriate discipline. These are not work rules. They are guidelines only. To insure the fair interpretation of the following guidelines, supervisors should review each situation for the following:

- Is the "rule" necessary for the orderly, effective and safe operation of Mayo Medical Center?
- Was the employee informed of the "rule" or work expectation; did he/she understand the explanation?
- Has the "rule" been applied equally?.

Each case is unique; therefore, equally does not mean rigid enforcement of "rules". Consider the specifics of each incident (i.e., theft of a 5-cent item would not necessarily be a Group III offense although "theft" is listed under Group III).

<u>Group I</u>

The following behaviors are usually subjected to all four steps of the Corrective Action process beginning with the supervisor's conference. Repeated offenses may be followed by a documented written warning, suspension and ultimately termination:

1. Reporting to work in improper attire or failure to maintain a clean, neat appearance
2. Loitering, neglecting work or loafing during working hours
3. Interference with work of other employees
4. Horseplay or disorderly conduct
5. Causing a disturbance, commotion or disorder
6. Disregard for safety rules or Mayo's safety practices
7. Careless operation and/or use of Mayo's property which results in its damage
8. Creating or contributing to unsanitary conditions
9. Unauthorized posting, removal or defacing of Mayo notices, signs or writing in any form on any medical center's bulletin boards
10. Distribution of literature and/or solicitation of employees, patients and the public on Mayo time, unless prior permission is received from Administration
11. Stopping work before specified stopping time
12. Being out of the department or assigned working areas during working hours without permission of a supervisor, except for the use of the rest rooms
13. Rude or discourteous behavior
14. Excessive tardiness
15. Excessive absences from work
16. Not meeting work and or job performance standards
17. Smoking on Mayo property and or chewing tobacco (refer to Mayo policy)
18. Unauthorized use and or misuse of the telephone
19. Unauthorized overtime

Group II

These offenses may begin with a written warning. Repeated offenses or more serious incidents may result in suspension or termination:

1. Accepting gratuities or tips from patients, their relatives, visitors or vendors
2. Sleeping or appearing to be asleep while on duty
3. Threatening, intimidating or coercing patients, fellow employees, or visitors on Mayo's premises at anytime for any reason
4. Harassment of employees, visitors, or patients based on equal employment opportunity protected categories.
5. Use of obscene or abusive language or gestures
6. Deliberate falsification of time card or other data related to work assignments

Group III

Incidents in Group III are very severe infractions of Mayo policies and may result in a suspension or termination.

1. Refusal to carry out instructions of supervisory personnel pertaining to work
2. Deliberate slowdown in regards to work
3. Deliberate refusal to complete work shift without approval of immediate supervisor
4. Immoral or indecent conduct on Mayo property
5. Possession of marijuana, alcoholic beverage, and/or illegal drugs on Mayo property
6. Reporting for work with the odor of alcohol on one's breath, or appearing to be under the influence of alcoholic beverages, marijuana, or any drug that impairs judgment or work performance
7. Willfully falsifying application for employment or other data requested by Mayo
8. Defacing or intentional destruction in any manner of Mayo's property, the property of fellow employees, patients or visitors
9. Theft of Mayo, other employee's, patient's or visitor's property
10. Fighting, agitating a fight, or attempting bodily harm or injury to anyone on Mayo property
11. Bringing a firearm or dangerous weapon onto Mayo property
12. Breach of ethics concerning confidentiality of employee or patient information

DATA SECURITY

Policy

Data is one of the most valuable assets of Mayo Foundation. It is our policy to protect this asset from accidental or intentional unauthorized modification, disclosure or destruction. Our data security program must be a well-organized and cost-effective plan which formulates the safeguards to protect patient and Foundation interests.

SECURITY ADMINISTRATION

Policy

A group will exist to develop, implement and maintain a data security program. This group will define the program, implement its standards, promote awareness of the program to all employees, and monitor the program's successes and failures to validate its effectiveness. The program shall provide cost-effective methods of protecting Mayo Foundation's interests.

Organization

Data security officer

The data security officer is responsible for recommending, developing, implementing and monitoring a consistent data security program. This will enable those responsible for system and data integrity to better perform those functions. The Information Security Subcommittee will monitor this responsibility. The data security officer will:

- Coordinate the development and maintenance of data security policy and standards
- Coordinate data security activities with Mayo Security, Internal Audit Services, Information Services and Treasury Services
- Monitor security activities to ensure implementation and operational integrity of data security standards
- Assist the data stewards in assessing their data for classification and advise them of available controls
- Develop, implement and maintain a data security awareness program
- Provide consulting services for data security throughout Mayo

Steward

The steward is the person appointed or responsible for a particular set of data, for example, a division chair or principal research investigator. Stewards are responsible for implementing data security policy and standards and will ensure custodianship. The steward will:

- Assume responsibility for data
- Recommend appropriate business controls and practices
- Communicate control and protection requirements to custodians and users
- Authorize data access and assign responsibility for custody of the data
- Monitor compliance and periodically review control decisions
- Review security violations and report to management

Custodian

The custodian is the person responsible for supplying data processing services and taking care of the system. An example is a system manager. The custodian implements the data security policy and standards, and will:

- Administer steward-specified business and data protection controls

- Administer access control
- Provide backup and recovery of data
- Detect and respond to violations and weaknesses

User

Users are any people who use Mayo data processing services and facilities. They must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure of it. Users are responsible for protecting institutional information to which they have access and for reporting security violations. Users must comply with the data security policy and standards, and they are accountable for their actions.

Data assessment

Standard

Stewards will assess their data and the corresponding threats, and classify their data as *public* information, *Mayo internal*, *Mayo restricted* or *Mayo confidential* and ensure appropriate controls.

Guidelines

- *Public* information requires no security controls.
- *Mayo internal* information should be kept within the institution, but requires no special handling in-house. An example is non-medical patient demographic data.
- *Mayo restricted* information should be handled on a need-to-know basis within the institution and not released externally. Examples include purchasing information, accounts payable and most research data.
- *Mayo confidential* information is very sensitive and should be closely controlled from creation to destruction. Examples include patient medical information, salary, personnel, legal and proprietary information.

Data Classifications

	Mayo Internal	Mayo Restricted	Mayo Confidential
Label	None	None	"Confidential"
Access/Storage	Store out of sight to non-Mayo personnel	Discretionary access controls Store out of sight	Discretionary access controls Lock up Encrypt off-campus data transmissions
Destruction	No special handling required	No special handling required	Shred Overwrite magnetic media
Mail	1st Class Mail Internet Mail	1st Class Mail Internal Mail	1st Class Mail Internal Mail using confidential envelope

Security controls are not required for public information.

Training

Standard

The Department of Human Resources, together with the data security officer, will provide data security training.

Guidelines

- The Department of Human Resources will describe data security to all new employees.
- Awareness programs will provide instruction on good security practices.
- Mayo will support specific technical and management training for Information Services personnel and users as needed.

Monitoring

Standard

Compliance with the data security standards will be monitored.

Guidelines

- Monitoring compliance is the responsibility of the system or area management, the data security officer and Internal Audit.
- All users, custodians and stewards should report instances of noncompliance.

Violations

Standard

Any exception to the data security policies and standards is a violation, and will be reviewed for appropriate disciplinary action which could include termination of employment or criminal prosecution.

Guidelines

- The data security officer, the Department of Human Resources and an appropriate level of department management will review standards violations and recommend corrective and disciplinary actions.
- Users should report security violations to a custodian, steward, supervisor, the data security officer, the Security Section or Internal Audit Services, as appropriate.

Exceptions

Standard

All exceptions to these standards are to be requested in writing by the steward of the data and approved by the Information Security Subcommittee.

PHYSICAL ACCESS CONTROL

Policy

Physical access to Mayo Foundation data processing areas, equipment and media must be controlled. Access must be controlled for the transportation of data processing media and other computing resources. The level of control is contingent on the level of risk and exposure to loss. The Security Section has the responsibility for implementing physical access controls.

Access to computing facilities and equipment

Standards

The level of physical access control for any area containing *Mayo confidential* or *Mayo restricted* data and facilities must be consistent with the level of risk and exposure.

Highly sensitive sub-areas, such as data centers, must have separate control systems to limit access.

Personal computers, software, documentation and diskettes shall be secured commensurate with the threat and exposure to loss. Available precautions include equipment enclosures, lockable power switches, equipment identification and fasteners to secure the equipment. The Security Section recommends controls based on risk.

Guidelines

- The senior manager of the area will determine the physical access controls based on Mayo security policies, standards and guidelines.
- All those granted access to an area or to data are responsible for their actions. Additionally, if you give another person access to an area, you are responsible for that person's activities.

Media and hardcopy protection and transportation

Standard

Media or hardcopy containing *Mayo restricted* or *Mayo confidential* data must have access controls during transportation and disposal.

Guidelines

- Printed versions (hardcopy) of *Mayo confidential* or *Mayo restricted* data should not be copied indiscriminately or left unattended and open to compromise.
- Media containing *Mayo confidential* data or documents should be placed in confidential envelopes and hand-carried by Mayo employees, transported on the General Service courier network or through an approved outside carrier. These outside carriers may include, but are not limited to, the U.S. Postal Service, Federal Express and the United Parcel Service.
- *Mayo restricted* or *Mayo confidential* media in transit on campus may be transported by Mayo employees in any containers deemed appropriate. Reasonable care should be used, and media should be secured when left unattended.

- Magnetic media containing *Mayo internal*, *Mayo restricted* or *Mayo confidential* data which is released from Mayo should first be processed to destroy any data residing on that media.
- Degaussing and overwriting are acceptable methods of destroying data.
- Responsible personnel must authorize the shipping and receiving of magnetic media, and appropriate records must be maintained.
- *Mayo confidential* information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.

LOGICAL ACCESS CONTROL

Policy

Access to all of Mayo Foundation's computing, data communications and sensitive data resources will be controlled based on the user's needs. Access is controlled through user identification and authentication. Users are responsible and accountable for work done under their personal identifiers. Access control violations must be monitored, reported and resolved.

Data Access Control

Standard

Access to *Mayo restricted* and *Mayo confidential* programs, databases and files must be controlled.

Guidelines

- All computer terminal access should be controlled through a password or through physical security measures.
- Each user should have a unique identification code.
- Each user's identity should be authenticated through an acceptable verification process. For example, access may be granted to a device, a unique token such as a card with a magnetic strip, or an individual password.
- Passwords are the individual's responsibility, and users should not share passwords.
- Users should be able to select and change their own passwords, and should do so at least every ninety days. Permanent passwords are discouraged.
- Passwords should be at least six characters long and not easily guessed or found in a dictionary. Use of numeric digits and non-alphanumeric characters in passwords is encouraged for protection of *Mayo confidential* and *Mayo restricted* information.
- Users should not write down passwords, store them on hard copy or keep them on a personal computer for remote log-on purposes.

Standards

Custodians must periodically review user access privileges and remove identification codes and passwords from their systems when users no longer require access.

Custodians must implement discretionary access controls to limit access to *Mayo restricted* and *Mayo confidential* information when available and technically feasible. These features are found in access control software such as RACF and some operating systems such as VMS.

Custodians must implement inactivity time-outs, where technically feasible, for terminals and workstations which access *Mayo restricted* and *Mayo confidential* information. Custodians must implement inactivity time-outs for all terminals and workstations at non-Mayo locations which have remote access to Mayo systems and information. The data steward should specify the time-out interval based on business needs and the level of risk and exposure.

Custodians must audit all unauthorized accesses and attempts to access *Mayo restricted* and *Mayo confidential* information. Custodians also must audit all off-campus accesses and attempts to access Mayo systems. Audit records shall be kept at least six months, and custodians shall periodically review the audit records for evidence of violations or system misuse.

Communications access controls

Stewards of *Mayo restricted* and *Mayo confidential* data must be aware of access-control vulnerabilities for that data while it is in transmission within the Mayo network. Stewards of *Mayo restricted* and *Mayo confidential* data who are concerned with access control vulnerabilities for their data should ask for proper engineering solutions such as leased lines or encryption. Stewards of *Mayo restricted* and *Mayo confidential* data should be aware of the costs to implement secure engineering solutions. However, steps must be taken to ensure proper solutions for security of the data, not necessarily those of least cost.

<u>Standard</u>

All requests for access to data and/or systems from non-Mayo locations or affiliates require the approval of the Information Security Subcommittee or its delegate.

<u>Guidelines</u>

- Remote access via modem should be through an approved security device such as a dial-back system or hardware token technology.
- If a security device is not used for remote access, a Mayo employee must enable and disable the modem and directly supervise its use. Modems should not be left unattended in answer mode.

DATA INTEGRITY CONTROLS

<u>Policy</u>

Controls must exist to ensure data remains consistent with its source. These controls must encompass both manual and electronic processing. Errors, duplications, omissions and intentional alterations should be discovered and investigated. Many data integrity controls will be determined by the steward of the data and will reside within the application or system.

Separation of duties and functions

Standard

Where feasible, separation of duties must be maintained.

Guideline

- Avoid overlapping responsibilities of application programmer, system programmer, data center operator, data base administrator, network operation and user functions.

Medical Records

Standard

The Medical Records Access Policy will not be compromised by the recording of information in alternate locations or systems.

Guidelines

- Information required for the medical care of patients must be in the medical record, and information stored in alternate locations or systems may not substitute for its placement in the medical record.
- Patient medical data must have the same protection as the medical record.

APPLICATION SOFTWARE

Standard

Only tested and controlled software should be installed on networked systems. Use of unevaluated and untested software outside an application development environment is prohibited.

Computer Crime

Standards

Computer crimes violate state and federal law as well as the Data Security Policy and Standards. They include but are not limited to: unauthorized disclosure, modification or destruction of data, programs, or hardware; denial of computer services; theft of computer services; illegal copying of software; invasion of privacy; theft of hardware, software, peripherals, data, or printouts; misuse of communication networks; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under state or federal law, held civilly liable for their actions, or both. Mayo must comply with license agreements for copyrighted software and documentation. Licensed software must not be copied unless the license agreement specifically provides for it. Copyrighted software must not be loaded or used on systems for which it is not licensed. This includes employee-owned home computers used for Mayo business.

End-user ethics

Standard

Any action that harms the resources of the institution or employs computers to adversely affect other individuals is prohibited.

Guidelines

- Users should not use Mayo computing resources for personal purposes.
- Users should scan all personal computer programs and data for viruses before loading them onto Mayo systems.

Standards

Users must not attempt to gain physical or logical access to data or systems for which they are not authorized. Users must not attempt to reverse-engineer commercial software. Users must not load unauthorized programs or data onto Mayo systems.

Electronic-mail

Standards

Mayo Foundation owns the electronic mail service, and considers electronic-mail private, direct communication between sender and recipient(s) or recipient(s)' designee(s); however, employees cannot expect absolute confidentiality. The contents will not be monitored, observed, viewed, displayed or reproduced in any form by anyone other than the sender and recipient(s) or recipient(s)' designee(s) unless specifically authorized by an officer of Mayo Foundation, a law enforcement representative or the data security officer.

Electronic mail is considered official correspondence of Mayo Foundation, and users must avoid the inclusion of inappropriate or derogatory language in their messages. Electronic mail is maintained in computer systems and on backup media for varying lengths of time and may be recovered subsequent to deletion. The messages may be disclosed in the same manner as paper records. Reasons for recovery of electronic mail messages may include legal discovery, external investigations by law enforcement personnel and internal security investigations.

Work-related mail is forwarded to the most appropriate employee in the case of employment termination or when an employee is absent for an extended period of time. A recipient may designate another employee to receive and read work-related mail for business reasons. Personal messages are forwarded to the intended recipient. If that is not possible, they are destroyed. Messages are not examined further than is necessary to determine the category into which they fall.

Internet

Standard

Use of the Internet via the Mayo network must be primarily for Mayo business or professional development. Limited personal use is acceptable but discretion is necessary

to ensure that individuals do not degrade Mayo's public image through their activities or adversely affect the availability of network resources. Use of the Internet via the Mayo network for personal business is not permitted.

PREVENTIVE MEASURES, BACKUP, AND RECOVERY

Policy

Fire prevention, backup of computer facilities and recovery procedures for the network, computer equipment, programs, data and utility services must be in place. These plans must provide recovery capabilities that are consistent with the business needs of the Mayo Foundation. Each procedure for data backup and recovery must be tested on a regular basis.

Disaster recovery planning

Standard

All Mayo data centers and computerized systems critical to Mayo Foundation must have written and operationally tested disaster recovery plans.

Guidelines

- Data processing management will maintain teams to execute recovery procedures for a data center or network disaster, recovery of host data bases and recovery of the network.
- The disaster plan should include procedures to facilitate an immediate, planned response to emergency situations.
- All areas of data processing are required to maintain recovery documentation consisting of a system recovery overview, systems chart and job-level recovery documentation.
- Recovery procedures should address computers, peripheral equipment, environmental systems, supplies and anything else essential to the data processing operation.
- Stewards, custodians and users should all be involved in disaster recovery planning.
- All recovery tasks are to be assigned to specific personnel. Each person should have an alternate. Recovery plans must allow alternate personnel to access the necessary instructions and procedures to accomplish recovery tasks.
- Testing of recovery plans should be an ongoing activity. All activity during a test must be recorded and reviewed for the purpose of improving the plans. Tests should include alternate site processing.

Backup

Standard

All data must have sufficient backup and be recoverable.

Guidelines

- Multiple levels of backup and storage should be used for key data and files.
- Backup should provide for the loss of multiple cycles.
- Users of personal computers are responsible for the backup and recovery of their system files and programs.
- Files and programs should be properly labeled and indexed to facilitate recovery.

- Alternate fire zone storage facilities should be used for media containing vital data that, if lost or destroyed, would be difficult to recreate.
- Alternate fire zone storage facilities should be used for files containing patient care programs, program changes, or data that could be used to reconstruct essential systems in the event of a disaster.
- Backup and recovery procedures should be tested.

Prevention

Standard

A frequent testing program of prevention methods as they apply to fire, utility services and other environmental hazards must exist.

Guideline

- Combustibles should not be stored in data centers, network hub rooms, network points of presence, or other areas critical to the computing base.

PARTNERS

POLICY ON CONFIDENTIALITY FOR PATIENTS

Keeping your medical records confidential

What you need to know about the Partners Confidentiality Policy

Partners HealthCare System and Partners Community HealthCare are committed to providing you with high quality health care and to forming a relationship with you that is built on **trust.** That means respecting your **privacy** and **confidentiality** of you medical information. We protect your privacy and confidentiality rights by creating and putting into practice policies and procedures that allow access to your personal medical information **only** for legitimate reasons.

Your medical record

As we provide your health care, we are required to maintain a complete copy of your medical history, current condition, treatment plan and all treatment given, including the results of all tests, procedures and therapies. Whether this information is stored in writing, on a computer, or other means, we will keep this information in a safe and secure way that protects your privacy and confidentiality. Of course, the physicians and other health care professionals who are involved in your care need to access this information in order to provide appropriate treatment for you.

Your medical information is private and confidential

You, or anyone to whom you give written permission, or your legal representatives, have the right to read or get a copy of your medical information. Your medical record is the physical property of the individual hospital or physician practice.

How do we assure your privacy?

Partners has put in place detailed policies regarding access to medical records by our staff and employees and has carefully outlined the circumstances under which your medical information may be released to parties outside the hospital or physician practice. These policies conform with state and federal law and are designed to safeguard your privacy.

Our staff and employees are trained in the appropriate use of medical information and know that it is available to them only to continue to provide care to you or for other limited but legitimate reasons. A violation of confidentiality or the failure of an employee to protect your information from accidental or unauthorized access will not be tolerated.
This may include the employee being fired from his or her job.

We ask for your permission

We do not allow others outside Partners to access your medical information unless we have the appropriate authorization to do so. We will request your authorization to release information at your first visit or admission. In addition, some laws prevent certain types of patient information from being released without specific patient permission. Examples include, but are not limited to:

- Confidential details of:
  - Psychotherapy (from records of my treatment by a psychiatrist, licensed psychologist or psychiatric clinical nurse specialist)
  - Other professional services of a licensed psychologist
  - Social Work Counseling/Therapy
  - Domestic Violence Victims' Counseling
  - Sexual Assault Counseling
- HIV test results (Patient authorization required for **EACH** release request.)
- Records pertaining to Sexually-Transmitted Diseases
- Alcohol and Drug Abuse Records that are protected by Federal Confidentiality Rules (42 CFR Part 2)

Please note, however, that the law requires some information to be disclosed in certain circumstances. This includes mandatory reports of abuse of children or elderly or disabled persons. Also, subpoenas or court orders may compel the disclosure of confidential or privileged health information in the context of a lawsuit or administrative proceeding.

Medical records are sometimes used for reasons other than patient care. For example, records are periodically reviewed to evaluate the quality of care, or to be sure that the Partners organizations follow the rules of regulatory agencies for the efficient and effective utilization of care such as Medicare, Department of Public Health, or Department of Mental Health. Your insurance company may request information that we are required to submit in order to provide and bill for your care. Anyone reviewing records must follow the same confidentiality laws and rules required of all health care providers.

Patient records are valuable tools used by researchers in finding the best possible treatments for diseases and medical conditions. All researchers must follow the same rules and laws that other health care workers are required to follow to insure the privacy of patient information. Information that may identify you will not be released to anyone outside Partners without your written approval. In all research conducted within Partners, concern for your privacy and well-being is our first priority.

If you have questions . . .

If you have questions about the privacy of your medical records, please speak with your physician, a member of his or her office staff, or the Medical Record Office, as appropriate. They will be happy to help you.

GUIDELINES ON CONFIDENTIALITY FOR EMPLOYEES

The following guidelines are a resource for the staff of Partners organizations and/or practices. These Guidelines are intended as a minimum set of expectations for confidentiality management. It is the expectation that these Guidelines will be incorporated into the policies and procedures of each organization/practice.

Partners HealthCare System and Partners Community HealthCare are dedicated to providing the best possible care to all patients at any of its facilities. Partners will enforce policies that preserve the privacy and confidentiality of patient information to the full extent provided by the law, and that facilitate timely communication to referring physicians/providers and continuing care physicians/facilities. Patient information will be stored and maintained in a safe and secure manner, and access to patient information will be limited to those specifically authorized. Access to patient information by those outside of Partners is prohibited without the written authorization of the patient or unless otherwise permitted by law or regulation.

Partners organizations, practices, and physicians are required to fully document a patient's medical history, current condition, treatment plan and all treatment rendered including the results of all tests, procedures and therapies. This information is required to be maintained by the organization in a safe and secure way to protect privacy and confidentiality. The information must be available to those involved in the patient's care, but is restricted and is only accessed on a Need-to-Know basis. All other access is prohibited to the extent permitted by law without the patient's written authorization.

When access to patient information is permitted, such access may be made by viewing the original paper record, by obtaining a copy of the record, by electronically receiving a transmission of the specified information, or by accessing the approved information online on a Need-to-Know basis.

RELEASE OF MEDICAL INFORMATION

Each organization/practice that is part of Partners will use a written authorization from the patient for the Release of Medical Information. This form will include a statement that recognizes that the organization/practice is part of an integrated health care delivery system comprised of Partners HealthCare System and Partners Community HealthCare, and that information will be shared among the Partners entities on a Need-to-Know basis. The Release of Medical Information authorizes the physician or physician group practice to release health information requested by any insurance company or third party programs related to the claims filed for specific visits/admissions or benefit assessment. This statement should also include authorization for the release of medical information to other hospitals, physician(s), primary care physician(s), referring physician(s), or agencies in order to facilitate current care, to arrange transfers

or the provision of continuing care following discharge or treatment, or in the case of medical emergency, or for those health workers involved in teaching, Institutional Review Board approved research, and/or internal utilization management and quality review. All other access is prohibited without specific written authorization by the patient.

Some laws prevent certain types of patient information from being released without specific patient permission. Examples include, but are not limited to:

- Confidential details of:
  - Psychotherapy (from records of my treatment by a psychiatrist, licensed psychologist or psychiatric clinical nurse specialist)
  - Other professional services of a licensed psychologist
  - Social Work Counseling/Therapy
  - Domestic Violence Victims' Counseling
  - Sexual Assault Counseling
- HIV test results (Patient authorization required for **EACH** release request.)
- Records pertaining to Sexually-Transmitted Diseases
- Alcohol and Drug Abuse Records that are protected by Federal Confidentiality Rules (42 CFR Part 2)

Certain medical data are needed in order to treat a patient and are not considered psychotherapist-privileged data and do not require additional patient consent in order for the data to be transmitted to other caregivers who have a Need-to-Know. These data are:

- Patient's name
- Diagnosis
- Dates of Service
- Types of Service
- Medications
- Relevant behavioral material, e.g. elements of danger that other caregivers need-to-know.

See Appendices A and B for Release of Medical Information and Release of Protected Medical Information.

PRINCIPLES FOR MEDICAL INFORMATION ACCESS/RELEASE

STAFF

- The right to access and to contribute to a patient's medical information is granted to staff if they are, have been, or will be involved in that patient's care. In this context, "staff" includes all clinicians and/or appropriate support staff that participate actively in a patient's care, e.g. physicians, psychologists, social workers, nurses, physician assistants, medical assistants, physical therapists, occupational therapists, medical students, case managers.

- Staff may be unexpectedly involved in the emergency care of a patient. Thus, provisions must be made to allow such staff to access a patient's medical information. At the same time, such emergency access must be closely monitored, to be certain that it has been appropriate.

- Clinicians who are not part of a PCHI-owned or affiliated practice and clinicians in any Partners entity should be able to access information about patients for whom they have responsibility wherever these patients receive care within PCHI/Partners institutions. Primary care clinicians should have access to the medical information of patients for whom they are the primary caregiver or for whom they are covering for the caregiver. Subspecialists should have access to the medical information of patients for whom they serve as primary care physician, and to the medical information of patients they have seen in the past, or are scheduled to see in the future, as consultants or as specialty care providers.

- Staff ancillary departments, e.g., laboratories, radiology, volunteer services, should have access to patient's medical information that is required by their responsibilities. Laboratory technicians, for example, that would typically need the results of laboratory tests. Volunteers would not typically access clinician information although access to non-clinical information, e.g., demographics, bed location, might be appropriate.

- Access to information about certain types of patients requires special security measures and restrictions because of the sensitive nature of the clinical problem. Clinically sensitive problems include conditions and treatments for which state or federal law imposes special restriction.

  Examples of such protected information include, but are not limited to:
  - Confidential details of:
    - Psychotherapy (from records of my treatment by a psychiatrist, licensed psychologist or psychiatric clinical nurse specialist)
    - Other professional services of a licensed psychologist
    - Social Work Counseling/Therapy
    - Domestic Violence Victims' Counseling
    - Sexual Assault Counseling
  - HIV test results (Patient authorization required for **EACH** release request.)
  - Records pertaining to Sexually-Transmitted Diseases
    Alcohol and Drug Abuse Records that are protected by Federal Confidentiality Rules (42 CFR Part 2)

  Other individuals who would require special security measures include people who may generate curiosity, such as victims of crime, celebrities or public figures.

- Authorization allowing release of a patient's health information must be obtained from all patients cared for outside a Partners institution or a PCHI practice. The authorization would limit access, on a Need-to-Know basis, to health workers

involved in the patient's care, teaching, Institutional Review Board approved research, and/or internal utilization management and quality review.

- Any access to patient's health information may be audited for appropriateness of access.

PATIENTS

- Patients may have access to their records, within a reasonable period of time, as provided by state and federal law.

- A patient who disagrees with the accuracy of the information as presented in his/her medical record may make amendments to the medical record. Such amendments will be in the form of addenda to the record since changes and/or deletions in the original record are not allowed.

RESEARCH

- Medical information may be made available for research only when the research protocol has been approved by a Partners-affiliated institutional Review Board (IRB). All researchers must follow the same rules and laws that other health care workers are required to follow to insure the privacy of patient information. Identifiable patient information will not be released to anyone outside Partners for research purposes without the patient's informed consent, except as required by law.

HUMAN RESOURCE MANAGEMENT OF CONFIDENTIALITY

Each Partners organization or practice has Human Resource policies that address confidentiality. These include, but are not limited to:

- A personnel policy that addresses confidentiality that includes a statement outlining corrective action that will be taken in the event of a breach of policy,

- A system for incorporating the Partners Confidentiality Policy into new employee orientation, e.g., discussion, distribution of policy,

- A signed statement by the employee stating they have read and understand the importance of confidentiality which will be placed in each employee's personnel file,

- A system for incorporating periodic education or an annual review of the Partners Confidentiality Policy, e.g., annual performance appraisal or annual required training,

- A statement regarding confidentiality that is incorporated into job descriptions of those employees who routinely deal with confidential issues.

Appendices C,D and E include a Confidentiality Agreement for employees, students and volunteers to sign, Confidentiality Dos and Don'ts for Employees (two pages), and a Confidentiality Contract (two pages) for vendors.

PROFESSIONAL CONDUCT

Persons with access to information about patients, employees, or business matters may only obtain information that is necessary to do one's job. ***Regardless of the format in which information is obtained,*** i.e., verbal, written, electronic or other technologic formats yet to be developed, it must be treated with the same level of confidentiality.

Viewing any information other than what is required to do one's job is a violation of the Partners Confidentiality standard, ***even if one keeps the information to oneself and does not disclose it to any other person and will lead to corrective action up to and including termination of employment and/or suspension and loss of privileges.***

Persons who receive/view information about patients, employees, or business matters in order to do their jobs may not share the information with any others, unless the others need to know that information by virtue of their jobs. If a person needs to discuss confidential information with someone else as part of performing his/her job, he/she must be sure that the conversation is private and cannot be overheard. See Appendix C for the Employee Do's and Don'ts.

INFORMATION ACCESS

Partners organizations, practices and physicians are required to fully document a patient's medical history, current condition, treatment plan and all treatment rendered, including the results of all tests, procedures and therapies. This information is required to be maintained by the organization in a safe and secure way to protect privacy and confidentiality. The information must be available to those involved in the patient's care, but is restricted and is only accessed on a Need-to-Know basis. All other access is prohibited to the extent permitted by law without the patient's written authorization.

If certain information documented in the medical record is highly sensitive, access to this information may be further restricted. Access to this restricted information may be overridden in the case of medical emergency, but is subject to audit.

Need-to-Know is defined as that which is necessary for one to adequately perform one's specific job responsibilities. ***Access to a function on the computer does not imply that it is proper to search this information at will simply to satisfy curiosity.*** Hard copy records are accessed by request to the department responsible for safeguarding the document and should be signed out appropriately.

Persons not employed by Partners may have legitimate reasons to access patient information and/or information systems. Such access will be granted only when proper authorizations are in place. Such access will be time-limited. Non-employees include, but are not limited to, students, employees of private medical staff, contractors, consultants, volunteers, insurers, vendors, and payor-based case managers.

PASSWORD SECURITY STANDARDS

Data available through each organization's information system are safeguarded by limiting access through personal passwords. ***Access is determined by one's position, role, and/or responsibility. If a person's position, role and/or responsibility change, system access will be reevaluated as to its applicability***. If a password holder believes that someone else has access to their password, the password holder must take the proper steps to ensure that the password is changed. Further, the password holder should report the occurrence to the Security Administrator. Each Partners organization or practice should minimally have the following security standards in place:

- A designated written authorization process for granting of passwords and access. Such a process includes how the Password Administrator is identified. This Password Administrator is a specifically identified individual who grants others access to computer systems and functions within those systems.

- A system for annually (at a minimum) reviewing and amending those who have access to computer systems.

- A system that identifies the holder of the password through which each data inquiry, access and/or update is made, thus making it possible to determine information any given password holder has sought.

- A system to grant appropriate access to temporary personnel or outside staff, e.g., third party reviewers, that allows for an automatic deactivation at specified time frames.

- A system to deactivate a user's password immediately upon termination or if a user's position, role and/or responsibility change.

- A system for instructing a new user:
  - Not to share his/her password or to inappropriately access information.
  - That each user is responsible for his/her password.
  - That each user is responsible for logging off the computer.

Additionally, the following safety precautions should be in place:

- Passwords are assigned with a minimum 5 or 6 alpha/numeric code.
- Passwords should not be re-used, even after their expiration.

- Passwords should be time-limited.
- Access should be granted, as appropriate, by varying levels of security.

ELECTRONIC COMMUNICATION

Staff must use electronic communication systems and devices including, but not limited to: electronic mail, fax machines, the internet, voice mail, cellular phones, in a way that protects the confidential information of others.

ELECTRONIC MAIL

Staff must use discretion in transmitting patient-identifying information by electronic mail. It is recognized that electronic mail is a vital form of communication and is used to facilitate the care process. ***When transmitting information via electronic mail or the Internet, the security of the transmission cannot necessarily be guaranteed.*** Patient-identifying information should be communicated within Partners institutions only as needed. The patient's identity should be omitted in Internet communications. Staff should be aware that electronic mail communications are both hard to delete from the email system and may be subject to discovery in a lawsuit. The informality of electronic mail may lead staff to be more casual than they would otherwise be. However, electronic mail could be subpoenaed and introduced in a legal proceeding. Staff should take care in the tone and content of their communications on electronic mail.

REPRODUCING PATIENT INFORMATION (E.G. FAXING, PHOTOCOPYING)...

- Fax machines are the least controllable technology when one transmits patient information. It is critically important when faxing information that the sender has the correct fax number and that they know the receiving fax machine is in a secure location and/or that the intended receiver is available to immediately receive the fax.

- Fax cover sheets should contain the following wording:

  "The documents accompanying this fax transmission contain confidential patient information belonging to the sender that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this patient information is prohibited from disclosing the information to any other party. If you have received this transmission in error, please notify the sender immediately and destroy the information that was faxed in error, and keep any information you may have viewed confidential."

- When receiving faxed patient information:
  - Immediately remove the fax transmission from the fax machine and deliver it to the recipient.

- Manage patient information received via fax as confidential in accordance with policy.
- Destroy patient information faxed in error and immediately inform the sender.

- The following types of medical information are protected by federal and/or state statute and may NOT be faxed or photocopied without specific written patient authorization.
  - Confidential details of:
    - Psychotherapy (from records of my treatment by a psychiatrist, licensed psychologist or psychiatric clinical nurse specialist)
    - Other professional services of a licensed psychologist
    - Social Work Counseling/Therapy
    - Domestic Violence Victims' Counseling
    - Sexual Assault Counseling
  - HIV Test Results (Patient authorization required for **EACH** release request.)
  - Records Pertaining to Sexuality-Transmitted Diseases
  - Alcohol and Drug Abuse Records Protected by Federal Confidentiality Rules (42 CFR Part 2)

- Questions about faxing patient information, or routine patient information requests should be sent to the Health Information Department.

NETWORK SECURITY

- Data from systems managed by any division of Partners HealthCare System, Inc. will be exported/transferred internally and/or externally only with authorization.

- Data exports include, but are not limited to:
  - downloads
  - outgoing interfaces
  - abstracts.

- Exports will be executed via any medium, electronic or other. The content of data exports adheres to the "Need-to-Know" and the "least necessary privilege" concepts.

- Patient identity will be masked unless explicitly authorized and required.

- All connections to Partners networks will be authorized by each respective organization's information systems department. These include, but are not limited to:
  - connections to departmental workstations and local area networks (LANs)
  - connections with non-Partners computers, e.g. electronic dial-in via desktop modem
  - connections with remote Partners facilities

- connections to the Internet.

- Access to networks will be limited through the use of personal passwords.

- External connections must be approved by the authorized information security function of the respective organization and use an authorized firewall approach. Firewalls of protective barriers prevent the establishment of direct communication sessions from external networks to hosts on the internal network of the organization.

- Links to regional, national and international electronic networks will be established and maintained only if the links do not threaten the privacy, confidentiality and security of patient information and/or information systems after authorization has been approved.

- Information obtained in a data export may not be re-released without the proper authorization(s).

INTERNAL AUDITS

The Partners Internal Audit Services, in conjunction with the Health Information Department, is responsible for the process by which access of health information is audited. Results of audits that are conducted will be available for inspection by the Partners Confidentiality Steering Committee.

REQUESTS FROM OUTSIDE SOURCES AND/OR QUESTIONABLE REQUESTS

All questions from the news media or other outside sources regarding patient information should be directed to the respective spokesperson for each Partners organization, unless the questions fall within the scope of one's own job description.

An employee who receives a request for information from a source he/she considers inappropriate should immediately report the request to his/her supervisor, who will take appropriate action.

MANAGER RESPONSIBILITY

Department chairpersons, department directors, managers and supervisors ***should periodically review this policy with staff, monitor access to and distribution of information and act immediately on any suspected breach of confidentiality.***

Appendix A

PARTNERS

PARTNERS HEALTHCARE SYSTEM/PARTNERS COMMUNITY HEALTHCARE

RELEASE OF MEDICAL INFORMATION

I understand that **[name or organization, practice, physician]** is part of an integrated health care delivery system comprised of Partners HealthCare System and Partners Community HealthCare. I understand that **[name of organization]** its physicians and physician group practices are required to fully document my medical history, current condition, treatment plan and all treatment rendered, including the results of all tests, procedures and therapies. This information is required to be maintained by the organization in a safe and secure way to insure privacy and confidentiality. I understand that the information documented must be available to those involved in my care. Access to my medical record information within the organization is restricted and only available on a Need-to-Know basis.

I understand that my health care information, whether stored on paper, computer, film, or other medium is available to Partners HealthCare System and Partners Community HealthCare physicians and facilities now and in the future on a Need-to-Know basis to health workers involved in my care, teaching, Institutional Review Board approved research, and/or internal utilization management and quality review.

I hereby authorize **[name of organization]** and its physicians or physician group practices to release my health information requested by any health insurance company/organization related to the claims filed for this visit/admission, or benefit assessment. I also authorize the release of medical information to other hospitals, facilities, physician(s), including my primary care physician(s) or referring physician(s), or agencies in order to facilitate my current care, to arrange transfers or the provision of other continuing care following my discharge or treatment from **[name of organization, practice, physician]**, or in the case of medical emergency. All other access is prohibited without my specific written authorization.

Because of federal laws and/or statutes, certain types of confidential information are not covered by this authorization and, if they exist, will not be disclosed or discussed to anyone outside **[name of organization, practice, physician]** without my specific approval; these include confidential details of psychotherapy and social work counseling, substance abuse rehabilitation treatment, HIV testing and results, and treatment of sexually-transmitted diseases.

My signature below constitutes my acknowledgment that I have read and understand the information provided in this form, that any questions I asked have been satisfactorily answered, and that I agree to this release of medical information as described herein.

Patient's Signature:_____

Date:_____

When patient is under legal age or incompetent to give consent, signature of legal guardian or health care agent:

Signature:_____
Date:_____
Relationship to Patient:_____

Appendix B

PARTNERS

PARTNERS HEALTHCARE SYSTEM, INC.
PARTNERS COMMUNITY HEALTHCARE, INC.

RELEASE OF PROTECTED OR PRIVILEGED INFORMATION

I, _____ **D.O.B.** _____ do hereby authorize Partners HealthCare System and/or Partners Community HealthCare to release health information including copies of my medical record for the time period of: _____ to the following:

1. _____
2. _____
3. _____

For the purpose(s) of: _____

I request the release of the specifically protected or privileged categories of information that I have *INITIALED* below:

Confidential Details of:
_____ Psychotherapy (from records of my treatment by a psychiatrist, licensed psychologist or psychiatric clinical nurse specialist)
_____ Other professional services of a licensed psychologist
_____ Social Work Counseling/Therapy
_____ Psychotherapy
_____ Social Work Counseling
_____ Domestic Violence Victims' Counseling
_____ Sexual Assault Counseling

Additional categories of protected or privileged information:
_____ HIV test results **(PATIENT AUTHORIZATION REQUIRED FOR EACH RELEASE REQUEST.)**
_____ Records Pertaining to Sexually-Transmitted Diseases
_____ Alcohol and Drug Abuse Records Protected by Federal Confidentiality Rules 42 CFR Part 2
(FEDERAL RULES PROHIBIT ANY FURTHER DISCLOSURE OF THIS INFORMATION UNLESS FURTHER DISCLOSURE IS EXPRESSLY PERMITTED OR WRITTEN CONSENT OF THE PERSON TO WHOM IT PERTAINS OR AS OTHERWISE PERMITTED BY 42 CRF PART 2.)
_____ Other(s): Please List _____

I understand that I may withdraw my consent at any time except to the extent that action has been taken in reliance on this statement. I understand that even if I do not withdraw consent that this statement shall expire in **(please check one)**:
___ **3 months** ___ **6 months** ___ **1 year from this date.** I have carefully read and understand the above, and do herein expressly and voluntarily consent to disclosure of the above information about, or medical records of, my condition to those persons or agencies listed above.

Partners HealthCare System and Partners Community HealthCare requires physicians and physician group practices to fully document my medical history, current condition, treatment plan and all treatment rendered, including the results of all tests, procedures and therapies. This information is required to be maintained by the organization in a safe and secure way to insure privacy and confidentiality. I understand that the information documented must be available to those involved in my care.

I understand that other health care information, whether stored on paper, computer, film, or other medium is available to Partners HealthCare System and Partners Community HealthCare physicians and facilities now and in the future on a Need-to-Know basis to health workers involved in my care, teaching, Institutional Review Board approved research, and/or internal utilization management and quality review.

_____ _____ _____ _____
Patient Signature Date Witness Date

_____
Relationship, if not patient

Appendix C

PARTNERS

PARTNERS HEALTHCARE SYSTEM, INC.
PARTNERS COMMUNITY HEALTHCARE, INC.

CONFIDENTIALITY AGREEMENT

Partners HealthCare System, its affiliates, and Partners Community HealthCare have a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their health information. Additionally, Partners HealthCare System, its affiliates, and Partners Community HealthCare must assure the confidentiality of its human resources, payroll, fiscal, research, computer systems, and management information. In the course of my employment/assignment at a Partners organization/practice, I may come into the possession of confidential information. In addition, my personal access code [“USER ID(s)” and PASSWORD(s)] used to access computer systems is also an integral aspect of this confidential information.

By signing this document I understand the following:

1. I agree not to disclose or discuss any patient, human resources, payroll, fiscal, research and/or management information with others, including friends or family, who do not have a need-to-know.
2. I agree not to access any information, or utilize equipment, other than what is required to do my job, even if I don’t tell anyone else.
3. I agree not to discuss patient, human resources, payroll, fiscal, research or administrative information where others can overhear the conversation, e.g. in hallways, on elevators, in the cafeterias, on the shuttle buses, on public transportation, at restaurants, at social events. It is not acceptable to discuss clinical information in public areas even if a patient’s name is not used. This can raise doubts with patients and visitors about our respect for their privacy.
4. I agree not to make inquiries for other personnel who do not have proper authority.
5. I agree not to willingly inform another person of my computer password or knowingly use another person’s computer password instead of my own for any reason.
6. I agree not to make any unauthorized transmissions, inquiries, modifications, or purgings of data in the system. Such unauthorized transmissions include, but are not limited to, removing and/or transferring data from Partner’s computer systems to unauthorized locations, e.g. home.
7. I agree to log off prior to leaving any computer or terminal unattended.

I have read the above special agreement and agree to make only authorized entries for inquiry and changes into the system and to keep all information described above confidential. I understand that violation of this agreement may result in corrective action, up to and including termination of employment and/or suspension and loss of privileges. I understand that in order for any “USER ID” and/or PASSWORD to be issued to me, this form must be completed. I further understand that computer access activity is subject to audit.

Please indicate the institution(s) with which you are affiliated:

- ☐ *Brigham and Women’s Hospital*
- ☐ *Dana-Farber Cancer Institute*
- ☐ *Massachusetts General Hospital*
- ☐ *McLean Hospital*
- ☐ *North Shore Medical Center*
- ☐ *Partners HealthCare System*
  - ☐ *Partners Community HealthCare*
- ☐ *Spaulding Rehabilitation Hospital*
- ☐ *Other:*_____

_____ _____
Signature of Employee / Physician / Student / Volunteer Date

_____
Print Name

To Be Filed in Employee’s Personnel Record

PARTNERS

CONFIDENTIALITY: DOs AND DON'Ts FOR EMPLOYEES

REGARDING VERBAL COMMUNICATION...

- Patient information should not be discussed where others can overhear the conversation, e.g. in hallways, on elevators, in the cafeterias, on the shuttle buses, on public transportation, at restaurants, at social events. It is not OK to discuss clinical information in public areas even if a patient's name is not used. This can raise doubts with patients and visitors about our respect for their privacy.

- Dictation of patient information should occur in locations where others cannot overhear.

REGARDING WRITTEN INFORMATION...

- Confidential papers, reports, and computer print-outs should be kept in a secure place.

- Confidential papers should be picked up as soon as possible from copiers, mail boxes, conference room tables, and other publicly accessible locations.

- Confidential papers should be appropriately disposed of, e.g. torn or shredded, when they are no longer needed.

REGARDING EMPLOYEE CONDUCT...

- Employees with access to information about patients, employees, or business matters may only obtain information that is necessary for job performance. *Regardless of the format in which information is obtained, i.e. verbal, written, electronic or other technologic formats yet to be developed, it must be treated with the same level of confidentiality*

.

- Accessing any information other than what is required to do your job is a violation of the Partners Confidentiality Policy, *even if you don't tell anyone else.*

- Accessing data must not occur simply to satisfy a curiosity. It is unacceptable to look up data, e.g. a friend's birthday, address or phone number. Information is only viewed when required for one's job.

Remember...it is your responsibility to keep patient and hospital information - whether it is spoken, written, in a computer system, or just in your head - totally confidential.

(Over, Please ☞)

Appendix D (continued)

CONFIDENTIALITY: DOs AND PARTNERS DON'Ts FOR EMPLOYEES

REGARDING REPRODUCING PATIENT INFORMATION (E.G. FAXING, PHOTOCOPYING)...

- Fax machines are the least controllable technology when one transmits patient information. It is critically important when faxing information that the sender has the correct fax number, that they know the receiving fax machine is in a secure location, and that **the patient has signed a Release of Information that allows us to release their health information to another location.**

- Fax cover sheets should contain the following wording:

  "The documents accompanying this fax transmission contain confidential patient information belonging to the sender that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this patient information is prohibited from disclosing the information to any other party. If you have received this transmission in error, please notify that sender immediately and destroy the information that was faxed in error.

- When receiving faxed patient information:
  1. Immediately remove the fax transmission from the fax machine and deliver it to the recipient.
  2. Manage patient information received via fax as confidential in accordance with policy.
  3. Destroy patient information faxed in error and immediately inform the sender.

- The following types of medical information are protected by federal and/or state statute and may NOT be faxed or photocopied outside the individual organization, and/or practice without specific written patient authorization.
  - Confidential details of:
    - Psychotherapy (from records of my treatment by a psychiatrist, licensed psychologist or psychiatric clinical nurse specialist)
    - Other professional services of a licensed psychologist
    - Social Work Counseling/Therapy
    - Domestic Violence Victims' Counseling
    - Sexual Assault Counseling
  - HIV test results (Patient authorization required for **EACH** release request)
  - Records pertaining to Sexually Transmitted Diseases
  - Alcohol and Drug Abuse Records that are protected by Federal Confidentiality Rules (42 CFR Part 2)

- Questions about faxing patient information, or routine patient information requests should be sent to the Health Information Department.

REGARDING COMPUTER INFORMATION...

- Sharing a password instead of having your own password is prohibited.
- Passwords must not be written down where others can find and/or use them.
- Employees must not log on and let someone else use a computer under their password.
- Employees should protect their data and computer against unauthorized use by:
  - Using virus protection software.
  - Locking up backup diskettes or keeping them securely offsite.
  - Locking offices whenever possible
- Employees must log off the computer system when leaving a workstation.

Appendix E

PARTNERS HEALTHCARE SYSTEM, INC.
PARTNERS COMMUNITY HEALTHCARE, INC.

CONFIDENTIALITY CONTRACT REGARDING ACCESS TO PATIENT INFORMATION

INTRODUCTION

This Confidentiality Contract has been established to ensure that access by non-Partners employees to patient information is protected and is in compliance with Partners Policies, state and federal laws, and accrediting agencies This contract is to ensure that individuals requesting access to information have been authorized and need access in order to perform their duties for patient care, continuity of care and/or administrative review.

CONTRACT PROVISIONS

In that I have requested that Partners HealthCare System and/or Partners Community HealthCare permit my designated staff members to have access to patient information, for the purpose of (please check all that apply):

- ☐ Patient care/continuing care
- ☐ Benefits review/utilization/quality review
- ☐ Billing
- ☐ Other (Specify) _____

1. I agree to maintain the confidentiality of patient information in accordance with the Partners Confidentiality Policies. I agree to keep a copy of such policies available to my staff at all times.

2. I agree to review the Partners patient information policies with my staff and instruct them as follows:

   - They are to access information only as necessary to carry out the responsibilities of their employment.

   - They are to maintain confidentiality of patient information in accordance with the Partners Confidentiality Policies.

   - Violation of patient confidentiality may be subject to corrective action up to and including termination of employment and/or suspension and loss of privileges.

3. I agree to obtain from each of my staff members who uses or has access to patient information a written statement that he or she has been informed about and understands the

obligation to protect patient confidentiality and will do so. I will maintain that statement in the employee's personnel file and update it annually.

Appendix E (continued)

4. I agree that Partners may, at its sole discretion, revoke access to patient information at any time. I understand that access may be revoked in the event of a breach of patient confidentiality by me or any of my employees. I agree to immediately suspend or terminate further access to information by any employee if so requested.

5. I agree to adopt and observe policies and procedures which meet the Partners standard with regard to maintaining patient information in a secure manner and properly disposing of any information which is no longer needed and which has been converted to another media, e.g. paper, tape.

6. I agree that the Partners may audit access to and use of its patient information by me or my staff at any time or on an ongoing basis and may ask for and receive copies of the employee statements described in paragraph 3, above.

7. Special condition(s) that apply to this contract, if any, are described here:

   _____
   _____
   _____
   _____
   _____
   _____

8. This contract is effective as of the date signed and shall continue in effect until revoked by either payor replaced by a revised contract.

My signature below indicates that I have read, understand, and agree to the above provisions.

ON BEHALF OF: _____ **ON BEHALF OF:** _____

(Name of Company/Organization) (Partners Organization or Practice)

SIGNED BY: _____ **SIGNED BY:** _____

TITLE: _____ **TITLE:** _____

DATE: _____ **DATE:** _____

GLOSSARY OF TERMS

CASE LAW
A body of law on a subject that derives from the resolution of court cases. Because it is the uncompiled outcomes of specific suits involving unique individuals and circumstances, case law is subject to varying interpretations and applications.

CONFIDENTIALITY
The right to rely on the trust or discretion of another; the right of an individual to control access to and disclosure of private information entrusted to another. Confidentiality arises in a relationship when an individual gives private information to another on the condition of or with the understanding that the other will not further disclose it, or will disclose it only to the extent that the individual directs.

CONSENT
An individual's reasoned and voluntary agreement to something of a defined scope and purpose. Informed consent for medical treatment involves making an independent decision based on reasonable information of the risks and benefits of a particular procedure or treatment. Consent usually is express, either given in writing or by affirmative oral statement. It also may be implied by certain actions or inaction of the individual that lead others to a reasonable presumption about the individual's intent.

DISIDENTIFIED INFORMATION
Medical information which is anonymous, or from which identifying characteristics are completely removed. Disidentification requires the elimination not only of primary or obvious identifiers, such as the patient's name, address, date of birth, and treating physician, but also of secondary identifiers through which a user could deduce the patient's identity.

ELECTRONIC MEDICAL RECORDS
A system of recording or retaining medical information in electronic form. As commonly understood, electronic medical records mean more than word-processed documents stored on an individual physician's computer, but rather an integrated and interactive system for storing records that can be accessed from remote locations.

INFORMATION PRIVACY
The specific right of an individual to control the collection, use and disclosure of personal information.

LEAST NECESSARY PRIVILEGE
Access to information and computer systems must be limited to those who legitimately need the data. To the greatest extent possible each individual's access to data should be limited to only what is necessary to accomplish the individual's work.

MEDICAL INFORMATION
Personal or private information that is reported at or derived from a clinician-patient encounter. In addition to medical history and treatment, medical information includes demographic, psychosocial, and behavioral information reported to or ascertained by a health care provider in the course of a patient visit.

PRIVACY
The right to be left alone; the right of an individual to withhold himself and his property from public scrutiny. Privacy derives from the concepts of personal freedom and autonomy, and involves the ability of an individual to control the release or dissemination of information that relates to him/herself.

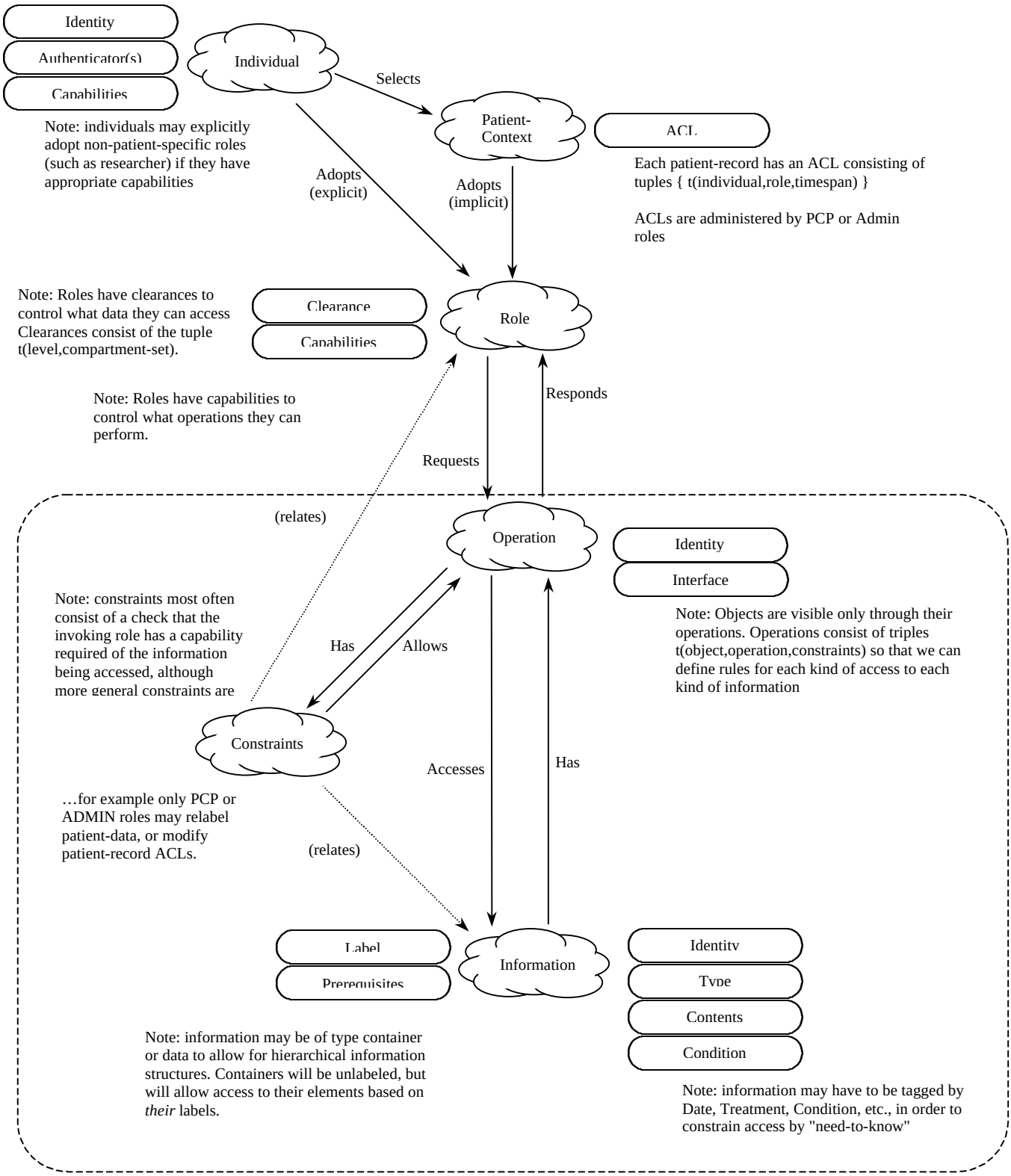
REGULATIONS
Formal rules adopted by a government agency or department to implement uniform application of a statute. Although regulations are not themselves laws, they also are binding upon all persons to whom the statute applies.

SECURITY
Security encompasses all of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness and oversight of all of these areas. The purpose of security is to protect both the system and the information it contains from unauthorized access from without and from misuse from within. Through various security measures, a health information system can shield confidential information from unauthorized access, disclosure and misuse, thus protecting the privacy of the individuals who are the subjects of the stored data.

SENSITIVE INFORMATION
Medical information for which the individual seeks heightened confidentiality protections. The determination of what is sensitive is unique to each individual, although certain categories of medical information are commonly recognized as potentially sensitive, such as mental health records, sexual history and orientation, sexually transmitted disease treatment, substance abuse treatment, etc. Information reported by an individual about family members or other persons should be considered sensitive for most purposes.

STATUTE
A law that is the result of a formal action taken by a legislature. A statute governs all persons to whom it applies within the legislatures jurisdiction (i.e. federal or state). A statute may be a single act of the legislature or any number of related acts addressing one legal topic.

PCASSO Security Policy Model



1. Security Policy

The complete PCASSO Security Policy Model is provided in Appendix A. The essential PCASSO Security Policy is reiterated in the following table, which includes a compliance matrix referencing the mechanisms (described in Section 6) which implement the policy.

Policy ID	Description	Implementation
R0000	The system shall provide a closed environment (i.e., a reference monitor) that ensures information confidentiality, integrity, accountability and availablility.	$6.1 CE_010 – CE_100
R0005	The system shall audit all actions to the granularity of a single individual.	$6.9 TBD Appendix B
R0010	System information and functions will be accessible only to authenticated individuals functioning in authorized patient-roles	$6.1 CE_080 $6.2 UIA_010 - 060 $6.3 IBAC_010 - 050 $6.4 LBAC_010 - 060 $6.5 RBAC_010 - 070
R0020	An individual may be *authorized* to adopt only one role for any given patient	$6.3 IBAC_010
R0030	Multiple individuals may be *authorized* to adopt the same (patient-)role	(not prohibited)
R0040	A given individual may be *acting* in only *one* (patient-)role at any given time	$6.2 UIA_060
R0050	Multiple individuals may be *acting* in the same (patient-)role at any given time	(not prohibited)
R0060	Because of R0020-0050, changing *context* from one patient to another will either (1) require the individual to *adopt* a defined role for that patient, <u>or</u> (2) transparently *assume* the individual's previously authorized role for that patient	$6.5 RBAC_010-030
R0070	Roles will be granted access to information based on both (1) role attributes (identity, clearance, capabilities and need-to-know) <u>and</u> (2) information attributes (identity, sensitivity, and prerequisite capabilities)	$6.5 RBAC_030 $6.5 RBAC_060
R0080	The patient should be able to access all portions of his/her record *except* for	$6.4 LBAC_010-040

	portions marked as “deny to patient”	
R0090	Only a patient’s primary care provider(s) may alter the security attributes of their patient record information (e.g., sensitivity)	$6.5 RBAC_060
R0091	The sensitivity of patient record data may not be lowered below “standard”	$6.4 LBAC_050 $6.4 LBAC_060
R0100	(removed)	
R0110	A patient’s primary care provider(s) can grant/revoke the ability of individuals to assume roles with respect to that patient	$6.5 RBAC_050
R0120	A patient’s primary care provider(s) can authorize and grant rights to secondary care providers	$6.5 RBAC_050
R0130	It shall be possible to deny guardian(s) (e.g., parent(s)) access to portions of their ward(s) (e.g., children(s)) patient-record	$3.4 $6.4 LBAC_020, 030
R0140	It shall be possible to notify patient’s of all changes or accesses to their patient-record on a patient-selectable period	$6.9 TBD
R0150	In emergency situations, legitimate care-providers with appropriate need must be able to acquire read-access to any specific patient record	$6.5 RBAC_040
R0160	It should be possible for a patient’s primary care provider to promote an individual from secondary- to primary-care-provider for a specified period of time. When the time has elapsed, the individual must revert back to a secondary-care-provider authorization.	$6.5 RBAC_050 (TBD restoration of original role not currently implemented?)
R0170	Access to the system or a system-role will be automatically revoked after a specified period (of inactivity)	$6.3 IBAC_010 $6.3 IBAC_050

Table 2-1. PCASSO Security Policy Implementation Matrix

```
% SCCS: @(#)spm.p   1.10 97/01/14 (c) 1996 SAIC
/*****************************************************************\
            NLM PCASSO Security Policy Model (SPM)

  Description:
    This document is a semi-formal exposition of the NLM PCASSO
    security policy model. This model constitutes a framework of
    abstractions that remain to be instantiated to express the
    exact security policy of the system.

    The approach in this SPM is to model the basic abstractions
    pertinent to the security policy using Entity-Relationship
    or Object-Attribute-Operation formalisms.

    The SPM involves the following kinds of entities:

        System
            ...which represents the information-system itself
        Individuals
            ...who represent the people using the system
        Roles
            ...which represent the capabilities of people
            that are working in a particular relationship
            to the system or to a particular patient
        Patient-Information
            ...which represents (primarily) the patient-information
            managed by the system.
        Contexts
            ...which represent the patient or the system and
            provide a means of modeling requirements for
            simplifying the transitions between one patient-role
            and another.

    The SPM is expressed in terms of the operations on these
    entities and the security rules associated with them. The
    operations are expressed in the following predicate notation:

        ENTITY_op(EntityID,Request,Result)

    where:
        ENTITY      is one of the previously identified entity-types
        EntityID    is the Identifier for the Entity to whom an
                    operation request is being directed
        Request     is the requested operation together with any
                    inputs to the operation (represented in
                    functional predicate(Argument,...) notation)
        Response    is the visible response to, or output from
```

the requested operation. This may also be
in functional prediate(Argument,...) notation.

To specify the side effects of these operations, predicates of the form:

entity(EntityID,Attribute,Value)

are used. The following entities are used to represent information that must be maintained and managed by the system to enforce the security policy:

individual(Individual,Attribute,Value)
...which represents information about individuals
role(Role,Attribute,Value)
...which represents information about instances of roles
information(Identity,Attribute,Value)
...which represents (primarily) patient-information
emergency(Individual,role,Role)
...which indicates that an Individual is accessing a Role with emergency exemption (subject to audit review)

Rules/Requirements:

The following rules constitute an informal statement of the NLM Security Policy:

R0000:
The system shall provide a closed environment (i.e., a reference monitor) that ensures information confidentiality, integrity, accountability and availablility.
R0005:
The system shall audit all actions to the granularity of a single individual.
R0010:
System information and functions will be accessible only to authenticated individuals functioning in authorized (patient-)roles.
R0020:
An individual may be AUTHORIZED to adopt only one role for a given patient
R0030:
Multiple individuals may be AUTHORIZED for a single role
R0040:
A given individual may be ACTING in only ONE (patient-)role at any given time
R0050:

Multiple individuals may be ACTING in the SAME (patient-)role
at any given time

R0060:
Because of R0020-0050, changing context from one patient to
another will:
(1) require the individual to ADOPT a defined role
for that patient,
or
(2) transparently ASSUME the individual's previously
authorized role for that patient.

R0070:
Roles will be granted access to information based on:
(1) Role attributes
(clearance, rights and need-to-know)
and
(2) Information attributes
(sensitivity, and prerequisites).

R0080:
The patient should be able to access all portions of his/her
record EXCEPT for portions marked as "deny to patient".

R0090:
Only a patient's primary care provider(s) may alter the security
attributes of their patient record information (sensitivity).

R0091:
The sensitivity of patient record data may not be lowered below
"standard" (i.e., patient-specific).

R0100: **** REMOVED 961213 ****
(downgrading by consensus of SCPs)

R0110:
A patient's primary care provider(s) can grant/revoke the
ability of individuals to assume roles with respect to that
patient.

R0120:
primary care physician can authorize and grant rights to
secondary care physicians.

R0130:
It may be necessary for physicians to deny parent's access to
some portions of their children's record(s)

R0140:
The patient must be notified of all changes to his/her patient
record, or to any of his/her patient-roles.

R0150:
In emergency situations, care-providers with appropriate need
should have unrestricted (read) access to a patient-record.

R0160:
It should be possible for a patient's PCP to promote an individual
from SCP to PCP for a specified period of time.

```
      When the time has elapsed, the individual should revert BACK to SCP.
   R0170:
      Access to the system or a system-role will be automatically
      revoked after a specified period of inactivity.

\*********************************************************************/

/*************************************************\
  System:
    The model includes a system abstraction to
    allow modeling of login/logout operations
  Attributes:
  Operations:
    login
    logout
  Predicates:
    individual(Individual,identity,Individual).
\*************************************************/

    /*************************************************************************\
      system:login
        identify and authenticate an individual to the system
    \*************************************************************************/

login :-
    % ######## Trusted Path Interaction ... #######
        write('(Trusted Path) Name? '),
        read(Individual),
        write('(Trusted Path) Authenticator? '),
        read(Authenticator),
    % ########### ... End Trusted Path ##############
    individual_op(Individual,authenticate(Authenticator),true).

    /*************************************************************************\
      system:logout
        terminate association with the system by deleting current user
        and authentication into any currently active roles
    \*************************************************************************/

logout :-
    individual(Individual,identity,Individual),
    individual_op(Individual,relinquish,_).

/*************************************************\
  Individual:
    Individuals model the people using the system.
  Attributes:
```

```
    :identity
        individual identity, records who is
        current "logged-in"
    :role
        individual's current (and ONLY) role
    :authenticator
        individual's authenticator (password)
  Operations:
    create(Individual,Authenticator)
    delete(Individual)
    authenticate(Authenticator)
        authenticates an individuals
    relinquish
  Predicates:
    individual(Individual,Attribute,Value)
        contains individual attributes
    individual_op(Individual,Request,Result)
\*************************************************/

:- dynamic(individual/3).

    /*************************************************************************\
      Creator:create(Individual,Authenticator)
        identify/authenticate an Individual
      REQUIREMENTS
        + the Individual may not exist
        + the Creator must have the create_individual right
      EFFECTS
        + creates Individual, sets Individual:authenticator = Authenticator
    \*************************************************************************/

individual_op(Creator,create(Individual,Authenticator),true) :-
    not individual(Individual,_,_),
    individual(Creator,role,Crole),
    role(Crole,rights,Rights),
    member(create_individual,Rights),
    assert(individual(Individual,authenticator,Authenticator)).

    /*************************************************************************\
      Creator:delete(Individual)
        delete an individual
      REQUIREMENTS
        + the Individual must exist
        + the Creator must have the delete_individual right
      EFFECTS
        + creates Individual, sets Individual:authenticator = Authenticator
    \*************************************************************************/
```

```
individual_op(Creator,delete(Individual),true) :-
   individual(Individual,_,_),
   individual(Creator,role,Crole),
   role(Crole,rights,Rights),
   member(delete_individual,Rights),
   retractall(individual(Individual,_,_)).

   /*************************************************************************\
     Individual:authenticate(Authenticator)
       identify/authenticate an Individual
     REQUIREMENTS
       + there must be a defined individual with the claimed identity and
         authenticator
     EFFECTS
       + records Individual:identity to mark individual as "logged in"
       + deletes association of Individual with any role
   \*************************************************************************/

individual_op(Individual,authenticate(Authenticator),true) :-
   individual(Individual,authenticator,Authenticator),
   retractall(individual(Individual,identity,_)),
   retractall(individual(Individual,role,_)),
   assert(individual(Individual,identity,Individual)).     % record current individual

   /*************************************************************************\
     Individual:relinquish
       relinquish identity as Individual. This requires that relinquish
       all roles into which the Individual may have been authenticated
       and then delete the Individual as a current user of the system.
     REQUIREMENTS
       + individual must be logged in
     EFFECTS
       + relinquishes Individual from all authenticated roles
       + retracts Individual:identity to delete Individual's "logged in"
         status
   \*************************************************************************/

individual_op(Individual,relinquish,true) :-
   individual(Individual,identity,Individual),
   setof(Role,Is^role(Role,individuals,Is),Roles),
   roles_op(Roles,relinquish(Individual),_),
   retractall(individual(Individual,role,_)),
   retractall(individual(Individual,identity,_)).

/*****************************************************************\
  Sensitivity/Clearance Levels
```

```
   + Levels are used to define an individual's clearance as
     well as the sensitivity level of information
   + The levels are organized into an hierachical lattice
     defined by a dominates(L1,L2) relationship

   + Hierarchy:

       Role    Clearance Level

       PCP, SCP
             patient_deniable
       patient
             guardian_deniable
       guardian
             public_deniable
       OCP
             standard
       public
             low

\*******************************************************************/

level(patient_deniable).    % deniable to patient
level(guardian_deniable).   % deniable to guardian/parent
level(public_deniable).     % deniable to public
level(standard).            % patient-specific
level(low).                 % non-patient-specific

% level hierarchy

adjacent_levels(system_high,patient_deniable).
adjacent_levels(patient_deniable,guardian_deniable).
adjacent_levels(guardian_deniable,public_deniable).
adjacent_levels(public_deniable,standard).
adjacent_levels(standard,low).
adjacent_levels(low,system_low).

% dominates relationship

dominates(L1,L2) :-
   adjacent_levels(L1,L2).
dominates(L1,L2) :-
   adjacent_levels(L1,L),
   dominates(L,L2).

/*************************************************\
  Prerequisites:
```

```
   The following are prerequisites that may be
   associated with information to control access
   based on "need-to-know". Information having
   such tags may be accessed only by a role
   whose rights contain these prerequisites.
\**************************************************/

prerequisite(problem(_,_)).   % access data by problem(Description,Date)

/**************************************************\
  Rights:
   The following are rights that roles must
   possess to be allowed certain kinds of
   operations.
\**************************************************/

right(create_individual).
right(delete_individual).

right(create_role).
right(delete_role).
right(add_role_access).
right(delete_role_access).
right(set_role_clearance).
right(grant_role_right).
right(revoke_role_right).

right(create_patient_role).
right(delete_patient_role).
right(add_patient_role_access).
right(delete_patient_role_access).
right(set_patient_role_clearance).
right(grant_patient_role_right).
right(revoke_patient_role_right).

right(raise_information_sensitivity).
right(lower_information_sensitivity).
right(add_prerequisite).
right(delete_prerequisite).

/**************************************************\
  Role:
   Individuals adopt roles in order to perform
   operations on information. Access to the
   information is controlled by Role attributes
   and information attributes.
  Attributes:
```

```
    :individuals
        set of individuals currently
        AUTHENTICATED to OPERATE in role
    :acl
        set of t(individual,authenticator,timespan) for
        individuals ALLOWED to ADOPT role
    :clearance
        maximum sensitivity role may read/write
    :rights
        set of access role rights/privileges
  Operations:
    create
    delete
    add(Individual,Authenticator)
        add an individual to a role's ACL
    delete(Individual)
        delete an individual from a role's ACL
    clearance -> Clearance
    clearance(Clearance)
        set role clearance
    grant(Right)
        grant a Right to the role
    revoke(Right)
        revoke a Right from the role
    adopt(Individual,Authenticator,Emergency)
  Predicates:
    role(Role,Attribute,Value)
        contains role attributes
    role_op(Role,Request,Response)
    role_op(t(Patient,Role),Request,Response)
\**************************************************/

:- dynamic(role/3).
:- dynamic(emergency/3).        % emergency(Individual,role,t(Patient,Role))

    /*****************************\
        role definitions
    \*****************************/

    % system administrator

role_def(admin,clearance,publis_deniable).
role_def(admin,rights,
[
       add_patient_role_access,
    delete_patient_role_access,
    create_individual,
```

```
    delete_individual
]).

    % patient

role_def(patient,clearance,guardian_deniable).
role_def(patient,rights,
[
    problem(_,_)
]).

    % guardian (for minors)

role_def(guardian,clearance,public_deniable).
role_def(guardian,rights,
[
    problem(_,_)
]).

    % primary-care-provider

role_def(pcp,clearance,patient_deniable).
role_def(pcp,rights,
[
       add_patient_role_access,
    delete_patient_role_access,
    raise_information_sensitivity,
    lower_information_sensitivity,
    problem(_,_)
]).

    % secondary-care-provider

role_def(scp,clearance,patient_deniable).
role_def(scp,rights,
[
    problem(_,_)
]).

    % researcher

role_def(researcher,clearance,low).
role_def(researcher,rights,[]).

    /*************************************************************************\
      t(Patient,Role):create
        create an instance of a Patient-Role
```

```
    REQUIREMENTS
      + requested patient-role may not exist
      + requesting role must have create_patient_role right
    EFFECTS
      + instantiates requested role definition such that
          !Role:acl       = []
          !Role:clearance = role-definition:clearance
          !Role:rights    = role-definition:rights
  \*************************************************************************/

role_op(t(Patient,Role),create,true) :-
  not role(t(Patient,Role),_,_),
  individual(Individual,role,Irole),
  role(Irole,rights,Rights),
  member(create_patient_role,Rights),
  role_def(Role,clearance,Clearance),
  role_def(Role,rights,Rights),
  assert(role(t(Patient,Role),acl,[])),
  assert(role(t(Patient,Role),clearance,Clearance)),
  assert(role(t(Patient,Role),rights,Rights)).

  /*************************************************************************\
    t(Patient,Role):delete
      delete an instance of a Patient-Role
    REQUIREMENTS
      + Patient-Role must exist
      + requesting role must have delete_patient_role right
    EFFECTS
      + deletes all Role attributes and Role instance itself
  \*************************************************************************/

role_op(t(Patient,Role),delete,true) :-
  role(t(Patient,Role),_,_),
  individual(Individual,role,Irole),
  role(Irole,rights,Rights),
  member(delete_patient_role,Rights),
  retractall(role(t(Patient,Role),_,_)).

  /*************************************************************************\
    t(Patient,Role):add(Individual,Authenticator,Timespan)
      add an entry t(Individual,Authenticator,Timespan) to a
      Patient-Role's ACL where Timespan = t(From,Until)
    REQUIREMENTS
      + requesting role must have add_patient_role_access right
      + Patient-Role:acl must not already contain Individual
    EFFECTS
      + !Patient-Role:acl contains t(Individual,Authenticator,Timespan)
```

```
    NOTES
      To enforce the semantics of R0160, we specify that this operation
      should behave as if the new ACL entry is "pushed" onto the ACL
      so that it can later be automatically "popped" off when the
      t(Patient,Role):adopt(Individual,Authenticator,Emergency)
      operation is attempted after the timespan expires.
  \*********************************************************************/

role_op(t(Patient,Role),add(Individual,Authenticator,Timespan),true) :-
  individual(Individual,role,Irole),
  role(Irole,rights,Rights),
  member(add_patient_role_access,Rights),
  role(t(Patient,Role),acl,ACL),
  not member(t(Individual,Authenticator,Timespan),ACL),
  retract(role(t(Patient,Role),acl,ACL)),
  assert(role(t(Patient,Role),acl,[t(Individual,Authenticator,Timespan)|ACL])).

  /*********************************************************************\
    t(Patient,Role):delete(Individual)
      delete an entry t(Individual,_,Timespan) from a Patient-Role's ACL
    REQUIREMENTS
      + requesting role must have delete_patient_role_access right
      + Patient-Role must have an entry for t(Patient,Authenticator,Timespan)
    EFFECTS
      + Updated Patient-Role:acl does-not-contain:
          t(Individual,Authenticator,Timespan)
  \*********************************************************************/

role_op(t(Patient,Role),delete(Individual),true) :-
  individual(Individual,role,Irole),
  role(Irole,rights,Rights),
  member(delete_patient_role_access,Rights),
  retract(role(t(Patient,Role),acl,ACL1)),
  remove(ACL1,t(Individual,_,_),ACL2),
  assert(role(t(Patient,Role),acl,ACL2)).

  /*********************************************************************\
    t(Patient,Role):clearance(Clearance)
      set t(Patient,Role):clearance = Clearance
    REQUIREMENTS
      + requesting role must have set_patient_role_clearance right
    EFFECTS
      + !Patient-Role:clearance = Clearance
  \*********************************************************************/

role_op(t(Patient,Role),clearance(Clearance),true) :-
  individual(Individual,role,Irole),
```

```
    role(Irole,rights,Rights),
    member(set_patient_role_clearance,Rights),
    retract(role(t(Patient,Role),clearance,_)),
    assert(role(t(Patient,Role),clearance,Clearance)).

    /*************************************************************************\
      t(Patient,Role):grant(Right)
        add a Right to a Patient-Role
      REQUIREMENTS
        + requesting role must have grant_patient_role_right right
      EFFECTS
        + if Patient-Role:rights contains Right then
            no-effect
          else
            !Patient-Role:rights contains Right
    \*************************************************************************/

role_op(t(Patient,Role),grant(Right),true) :-
    individual(Individual,role,Irole),
    role(Irole,rights,Rights),
    member(grant_patient_role_right,Rights),
    role(t(Patient,Role),rights,Rights),
    (member(Right,Rights) ->
        true
    ;
        retract(role(t(Patient,Role),rights,Rights)),
        assert(role(t(Patient,Role),rights,[Right|Rights]))
    ).

    /*************************************************************************\
      t(Patient,Role):revoke(Right)
        delete a Right from a Patient-Role
      REQUIREMENTS
        + requesting role must have revoke_patient_role_right right
      EFFECTS
        + if Patient-Role:rights contains Right then
            !Patient-Role:rights does-not-contain Right
          else
            no-effect
    \*************************************************************************/

role_op(t(Patient,Role),revoke(Right),true) :-
    individual(Individual,role,Irole),
    role(Irole,rights,Rights),
    member(revoke_patient_role_right,Rights),
    role(t(Patient,Role),rights,OldRights),
    (member(Right,OldRights) ->
```

```
      retract(role(t(Patient,Role),rights,OldRights)),
      remove(OldRights,[Right],NewRights),
      assert(role(t(Patient,Role),rights,NewRights))
   ;
      true
   ).

   /*********************************************************************\
     Role:adopt(Individual,Authenticator,Emergency)
       allow an Individual to adopt a Role given a valid Role Authenticator.
       if the role is being adopted in an Emergency note that access
       controls should be suspended subject to audit-review.
     REQUIREMENTS
       + Individual must not currently be in Role
       + Role:acl must contain t(Individual,Authenticator,Timespan)
       + ACL entry t(Individual,Authenticator,Timespan) must be current
     EFFECTS
       (role:acl entry t(Individual,Authenticator,Timespan) is current)
       + !Individual:role = Role
       + !Role:individuals contains Individual
       + asserts emergency(Individual,role,Role)

       (role:acl entry is not current)
       + !Role:acl does not contain t(Individual,Authenticator,Timespan)

     NOTES
       To implement R0160, this operation is specified to delete an
       ACL entry t(Individual,Authenticator,Timespan) if the Timespan
       has expired.
   \*********************************************************************/

role_op(Role,adopt(Individual,Authenticator,Emergency),true) :-
   not individual(Individual,role,Role),
   role(Role,acl,ACL),
   member(t(Individual,Authenticator,Timespan),ACL),
   Timespan = t(From,Until),
   ymd(YMD),
   (From =< YMD, YMD =< Until ->
      % ACL entry for role is currently valid
      retract1(individual(Individual,role,CurrentRole)),
      assert(individual(Individual,role,Role)),
      role(Role,individuals,Individuals),
      (member(Individual,Individuals) ->
         true
      ;
         retract(role(Role,individuals,Individuals)),
         assert(role(Role,individuals,[Individual|Individuals]))
```

```
        ),
        (Emergency = emergency ->
            assert1(emergency(Individual,role,Role))    % R0150
        ;
            retract1(emergency(Individual,role,Role))
        )
    ;
        % ACL entry for role has expired, delete it
        Until =< YMD,
        retract(role(t(Patient,Role),acl,ACL)),
        remove(ACL,t(Individual,Authenticator,Timespan),ACL1),
        assert(role(t(Patient,Role),acl,ACL1))
    ).

    /*************************************************************************\
      Role:relinquish(Individual)
        allow an Individual to relinquish a Role
      REQUIREMENTS
        + Individual must be in Role
      EFFECTS
        + !Individual:role is undefined
        + !Role:individuals does-not-contain Individual
        + retracts emergency(Individual,role,Role)
    \*************************************************************************/

role_op(Role,relinquish(Individual),true) :-
    retract(individual(Individual,role,Role)),
    retract1(emergency(Individual,role,Role)),
    role(Role,individuals,Individuals),
    remove(Individual,Individuals,NewIndividuals),
    assert(role(Role,individuals,NewIndividuals)).

/*************************************************\
  Roles:
    The Roles abstraction allows us to "apply"
    an operation to a set of roles, e.g., in
    order to relinquish all an Individual's roles.
  Attributes:
  Operations:
    relinquish(Individual)
  Predicates:
    roles_op(Role,Request,Response)
\*************************************************/

roles_op([],_,true).
roles_op([Role|Roles],Operation,true) :-
    role_op(Role,Operation,true),
```

```
   roles_op(Roles,Operation,true).

/*************************************************************************\
  Patient-Context:
    An individual may work in the context of only a single patient:role
    at a time. Since an individual may have only one role for a patient
    at a time, we may transparently change context to another
    patient:role as long as there has been a previous authorized
    adoption of that role.
  Predicates:
    individual(Individual,role,Role)
\*************************************************************************/

    /*************************************************************************\
      Contexts:
        Contexts are provided to simplify the adoption of roles.

        Note: There are two cases here:
            1)  the Individual is already authenticated into a single
                role with respect to the Patient. In this case, we
                allow the designation of the Patient to imply the
                selection of a Role.
            2)  the Individual is NOT already authenticated in ANY
                role with respect to the Patient. In this case, we
                require that the individual be authenticated into the role.

        Another issue is emergency access. We model this as a special
        "mode" associated with the patient-role in which all access is
        granted to any care-provider subject to audit-review.

    \*************************************************************************/

context(Patient,Emergency) :-
    individual(Individual,identity,Individual),
    setof(t(P,R),authenticated(Individual,P,R),[t(Patient,Role)]),
    (individual(Individual,role,CurrentRole) ->
        role_op(CurrentRole,relinquish(Individual),_)
    ;
        true
    ),
    (Emergency = emergency ->
        assert1(emergency(Individual,role,Role))        % R0150
    ;
        retract1(emergency(Individual,role,Role))
    ),
    assert(individual(Individual,role,Role)).
context(Patient,Emergency) :-
```

```
   individual(Individual,identity,Individual),
   % ######## Trusted Path Interaction ... #######
      write('(Trusted Path) Role? '),
      read(Role),
      write('(Trusted Path) Authenticator? '),
      read(Authenticator),
   % ########### ... End Trusted Path ##############
   role_op(t(Patient,Role),adopt(Individual,Authenticator,Emergency),true).

   /*********************************************************\
     authenticated(Individual,Patient,Role)
      is a helper predicate to collect all Patient-Roles
      into which an Individual may have been authenticated.
      It is necessary to express the constraint that
      an individual may be authenticated into only a
      single Patient-Role at a time...
   \*********************************************************/

authenticated(Individual,Patient,Role) :-
   role(t(Patient,Role),individuals,Individuals),
   member(Individual,Individuals).

/**************************************************\
  Constraints:
   Constraints are the access control rules
   defining whether a Role may execution an
   Operation on a particular Patient:Information
   object.

   They are separated out to provide flexibility
   in associating constraints with the tuple:

     t(Role,Operation,t(Patient,Information))

   In this way, we can reuse constraints
   if necessary
\**************************************************/

   /****************************************************\
     R0150 - In emergencies,
             Bypass access control constraints
   \****************************************************/

constraint(Role,_,Patient,_) :-
   individual(Individual,individual,Individual),
   emergency(Individual,role,t(Patient,Role)).
```

```
   /*********************************************************************\
     Role read t(Patient,Info) if
       Role:clearance dominates Information:sensitivity
   \*********************************************************************/

constraint(Role,read,Patient,Info) :-
   role(t(Patient,Role),rights,Rights),
   role(t(Patient,Role),clearance,Clearance),
   information(t(Patient,Info),sensitivity,Sensitivity),
   information(t(Patient,Info),prerequisites,Prerequisites),
   is_subset(Rights,Prerequisites),
   dominates(Clearance,Sensitivity).

   /*********************************************************************\
     Role write t(Patient,Info) if
       Information:sensitivity dominates Role:clearance
   \*********************************************************************/

constraint(Role,write,Patient,Info) :-
   role(t(Patient,Role),rights,Rights),
   role(t(Patient,Role),clearance,Clearance),
   information(t(Patient,Info),sensitivity,Sensitivity),
   information(t(Patient,Info),prerequisites,Prerequisites),
   is_subset(Rights,Prerequisites),
   dominates(Sensitivity,Clearance).

   /*********************************************************************\
     Role raise_information_sensitivity(NewSensitivity) t(Patient,Info) if
       NewSensitivity is higher than CurrentSensitivity, and
       level patient_deniable dominates NewSensitivity, and
       current role has raise_information_sensitivity right
   \*********************************************************************/

constraint(Role,raise_information_sensitivity(NewSensitivity),Patient,Info) :-
   information(t(Patient,Info),sensitivity,CurrentSensitivity),
   dominates(NewSensitivity,CurrentSensitivity),
   dominates(patient_deniable,NewSensitivity),
   role(t(Patient,Role),rights,Rights),
   member(raise_information_sensitivity,Rights).

   /*********************************************************************\
     Role lower_information_sensitivity(NewSensitivity) t(Patient,Info) if
       CurrentSensitivity dominates NewSensitivity
       current role has lower_information_sensitivity right
   \*********************************************************************/

constraint(Role,lower_information_sensitivity(NewSensitivity),Patient,Info) :-
```

```
   information(t(Patient,Info),sensitivity,CurrentSensitivity),
   dominates(CurrentSensitivity,NewSensitivity),                % R0091
   dominates(NewSensitivity,standard),
   role(t(Patient,Role),rights,Rights),
   member(lower_information_sensitivity,Rights).

   /*********************************************************************\
     Role add_prerequisite t(Patient,Info) if
       Role has add_prerequisite right
   \*********************************************************************/

constraint(Role,add_prerequisite,Patient,_) :-
   role(t(Patient,Role),rights,Rights),
   member(add_prerequisite,Rights).

   /*********************************************************************\
     Role delete_prerequisite t(Patient,Info) if
       Role has delete_prerequisite right
   \*********************************************************************/

constraint(Role,delete_prerequisite,Patient,_) :-
   role(t(Patient,Role),rights,Rights),
   member(delete_prerequisite,Rights).

/*********************************************************************\
  t(Patient,Information)
    Information is modeled as a tuple t(Patient,Information) in
    order to express the concept of patient-information.
  Attributes:
    :type = |container|data|
        information may be of two types: data or
        container (in order to allow hierachical data models)
    :sensitivity = |non_patient|patient|deniable|
        sensitivity level of information
    :new_sensitivity = t(NewSensitivity,Concensus)
        when changing information sensitivity by concensus,
        this attribute models previous level change requests
        as t(NewSensitivity,Concensus) where Consensus is
        the Individuals having previously made the same
        level change request.
    :prerequisites
        rights which the accessing role must have to access
        information
    :contents
        the actual information contents. for containers, the
        identities of the information in the container.
  Operations:
```

```
    create(Type,Sensitivity,Prerequisites)
    read -> Contents
    write(Contents)
    append(Contents)
    insert(Contents)
    delete(Contents)
    type -> Type
    type(Type)
    sensitivity -> Sensitivity
    sensitivity(Sensitivity)
    prerequisites -> Prerequisites
    prerequisites(Prerequisites)
  Predicates:
    information(Information,Attribute,Value)
        contain information attributes
    information_op(Information,Request,Result)
        operations
\*********************************************************************/

:- dynamic(information/3).

    /*****************************************************\
      Types of information
        information and containers allows modeling of
        arbitrary information structures
    \*****************************************************/

information_type(container).
information_type(data).

    /*****************************************************\
      Operations/Constraints for SPECIFIC Information
        ...this is TBD until we know the information schema
    \*****************************************************/

          /*********************************\
            Default Operations/Constraints
          \*********************************/

    /*************************************************************************\
      t(Patient,Info):create(Type,Sensitivity,Prequisites)
        create patient-information within the system
      REQUIREMENTS
        + the individual must be in a patient-role
        + the create_information:constraint must be satisfied
        + the Patient-Information may not already exist
      EFFECTS
```

```
      + !Information:type            = Type
      + !Information:sensitivity      = Sensitivity
      + !Information:prerequisites    = Prerequisites
      + !Information:contents         = undefined

    NOTE!!!   since PCASSO is a read-only system, patient-record information
              can only be created by IMPORTing it from external systems.

  \*************************************************************************/

information_op(t(Patient,Info),create(Type,Sensitivity,Prerequisites),true) :-
   individual(Individual,role,t(Patient,Role)),

   constraint(Role,create_information,Patient,Info),          % !!!?

   not information(t(Patient,Info),_,_),
   assert(information(t(Patient,Info),type,Type)),
   assert(information(t(Patient,Info),sensitivity,Sensitivity)),
   assert(information(t(Patient,Info),prerequisites,Prerequisites)),
   assert(information(t(Patient,Info),contents,undefined)).

   /*************************************************************************\
     t(Patient,Info):read -> Contents
       get the contents of the specified information
       to avoid covert channels, read operations that fail the
       read:constraint must return "undefined" as the contents.
     REQUIREMENTS
       + the individual must be in a patient-role
       + for containers, only the information in the container
          which satisfies the read:constraint will be seen
       + for regular information, the read:constraint must be satisfied.
     EFFECTS
       + none
   \*************************************************************************/

information_op(t(Patient,Info),read,VisibleContents) :-     % containers
   information(t(Patient,Info),type,container),
   individual(Individual,role,t(Patient,Role)),
   information(t(Patient,Info),contents,Contents),
   visible(Contents,Patient,Role,VisibleContents).
information_op(t(Patient,Info),read,Contents) :-
   individual(Individual,role,t(Patient,Role)),           % data
   constraint(Role,read,Patient,Info),
   information(t(Patient,Info),contents,Contents).
information_op(t(Patient,Info),read,undefined).

visible([],_,_,[]).
```

```
visible([Item|Contents],Patient,Role,[Item|VisibleContents]) :-
   constraint(Role,read,Patient,Item),
   visible(Contents,Patient,Role,VisibleContents).

   /*************************************************************************\
     t(Patient,Info):write(Contents)
       set the contents of the specified information
     REQUIREMENTS
       + the individual must be in a patient-role
       + the write:constraint must be statisfied
     EFFECTS
       + !t(Patient,Information):contents = NewContents

     NOTE!!!   because PCASSO is a read-only system, patient-record
               information may not be modified on-line.

   \*************************************************************************/

information_op(t(Patient,Info),write(NewContents),true) :-
   individual(Individual,role,t(Patient,Role)),
   constraint(Role,write,Patient,Info),
   retract(information(t(Patient,Info),contents,_)),
   assert(information(t(Patient,Info),contents,NewContents)).

   /*************************************************************************\
     t(Patient,Info):append(Data)
       append Data to the contents of the specified information
     REQUIREMENTS
       + the individual must be in a patient-role
     EFFECTS
       + !t(Patient,Information):contents = [OldContents,Data]

     NOTE!!!   because PCASSO is a read-only system, patient-record
               information may not be modified on-line.

   \*************************************************************************/

information_op(t(Patient,Info),append(Data),true) :-
   individual(Individual,role,t(Patient,Role)),
   retract(information(t(Patient,Info),contents,Contents)),
   append(Contents,[Data],NewContents),
   assert(information(t(Patient,Info),contents,NewContents)).

   /*************************************************************************\
     t(Patient,Info):type -> Type
       get the type of the specified information
     REQUIREMENTS
```

```
      + the individual must be in a patient-role
      + the read:constraint must be statisfied
    EFFECTS
      + none
  \*********************************************************************/

information_op(t(Patient,Info),type,Type) :-
   individual(Individual),
   role(t(Patient,Role),individual,Individual),
   constraint(Role,read,Patient,Info),
   information(t(Patient,Info),type,Type).

   /*********************************************************************\
    t(Patient,Info):type(Type)
      set the type of the specified information
    REQUIREMENTS
      + the individual must be in a patient-role
      + the write:constraint must be statisfied
    EFFECTS
      + !t(Patient,Information):type = Type
   \*********************************************************************/

information_op(t(Patient,Info),type(Type),true) :-
   individual(Individual),
   role(t(Patient,Role),individual,Individual),
   constraint(Role,write,Patient,Info),
   retract(information(t(Patient,Info),type,_)),
   assert(information(t(Patient,Info),type,Type)).

   /*********************************************************************\
    t(Patient,Info):sensitivity -> Sensitivity
      get the sensitivity of the specified information
    Note: unlabeled information is implicitly "deniable".
    Note: the sensitivity of some types of information may also be
          implicit (e.g., HIV-positive indicators.)
             => information(t(Patient,hiv),sensitivity,deniable).
    REQUIREMENTS
      + the individual must be in a patient-role
      + the read:constraint must be statisfied
    EFFECTS
      + if the read:constraint is not satisfied,
          the returned :sensitivity is "deniable"
   \*********************************************************************/

information_op(t(Patient,Info),sensitivity,Sensitivity) :-
   individual(Individual),
   role(t(Patient,Role),individual,Individual),
```

```
    constraint(Role,read,Patient,Info),
    information(t(Patient,Info),sensitivity,Sensitivity).
information_op(_,sensitivity,deniable).

    /*************************************************************************\
      t(Patient,Info):sensitivity(NewSensitivity)
        set the type of the specified information
      REQUIREMENTS
        + the individual must be in a patient-role
        + the NewSensitivity must not be the same as the CurrentSensitivity
        + if the NewSensitivity dominates the CurrentSensitivity
            the raise_information_sensitivity:constraint must hold
          else
            the lower_information_sensitivity:constraint must hold
      EFFECTS
        + !t(Patient,Information):sensitivity = Sensitivity
    \*************************************************************************/

information_op(t(Patient,Info),sensitivity(NewSensitivity),true) :-
    individual(Individual),
    role(t(Patient,Role),individual,Individual),
    information(t(Patient,Info),sensitivity,Sensitivity),
    NewSensitivity \= Sensitivity,
    (dominates(NewSensitivity,Sensitivity) ->
        constraint(Role,raise_information_sensitivity(NewSensitivity),Patient,Info)
    ;
        constraint(Role,lower_information_sensitivity(NewSensitivity),Patient,Info)
    ),
    retract(information(t(Patient,Info),sensitivity,Sensitivity)),
    assert(information(t(Patient,Info),sensitivity,NewSensitivity)).

    /*************************************************************************\
      t(Patient,Info):prerequisites -> Prerequisites
        get the prerequisites of the specified information
      REQUIREMENTS
        + the individual must be in a patient-role
        + the read:constraint must hold
      EFFECTS
        + none
    \*************************************************************************/

information_op(t(Patient,Info),prerequisites,Prerequisites) :-
    individual(Individual),
    role(t(Patient,Role),individual,Individual),
    constraint(Role,read,Patient,Info),
    information(t(Patient,Info),prerequisites,Prerequisites).
```

```
   /*********************************************************************\
     t(Patient,Info):prerequisites(Prerequisites)
       set the prerequisites of the specified information
     REQUIREMENTS
       + the individual must be in a patient-role
       + the NewPrerequisites must not be the same as the CurrentPrerequisites
       + if the CurrentPrerequisites is a subset of the CurrentPrerequisites
           the add_prerequisite:constraint must hold
         else
           the delete_prerequisite:constraint must hold
     EFFECTS
       + !Patient-Information:prerequisites = Prerequisites
   \*********************************************************************/

information_op(t(Patient,Info),prerequisites(NewPrerequisites),true) :-
   individual(Individual),
   role(t(Patient,Role),individual,Individual),
   information(t(Patient,Info),prerequisites,Prerequisites),
   NewPrerequisites \= Prerequisites,

   % treat adding prerequisites like raising sensitivity

   (is_subset(Prerequisites,NewPrerequisites) ->
      constraint(Role,add_prerequisite,Patient,Info)
   ;
      constraint(Role,delete_prerequisite,Patient,Info)
   ),
   retract(information(t(Patient,Info),prerequisites,Prerequisites)),
   assert(information(t(Patient,Info),prerequisites,NewPrerequisites)).

/*********************************************************************\
         **** End PCASSO Security Policy Model ****
\*********************************************************************/
```

```
/*************************************************\
  Supporting Predicates
\*************************************************/

% remove(X,Y,Z) => Z is the list where X is removed from Y

remove(_,[],[]).
remove(X,[X|Y],Y).
remove(X,[H|Y],[H|Z]) :-
   remove(X,Y,Z).

%----------------------------------------
% is_subset(+SUBSET,+SET) if SUBSET is a subset of SET
%
%   NOTE: works even with permutations of SUBSET and S
%       but CANNOT GENERATE SUBSETs!
%
%----------------------------------------

is_subset([],_).
is_subset([X|Y],Set) :-
   member(X,Set),
   is_subset(Y,Set).

% assert fact only if it is not aready asserted

assert1(Fact) :-
   (Fact ->
      true
   ;
      assert(Fact)
   ).

% non-failing retract

retract1(Fact) :-
   (Fact ->
      retract(Fact)
   ;
      true
   ).

% write a list

w([]) :-
   nl.
```

```
w([X|Xs]) :-
   write(X),
   w(Xs).

/*****************************************************************\
 Issues:

   1.  The current model does not accurately portray the notion
       that patient-records are collections of entries. One can
       create and entry and append it to the record. However,
       an existing entry may not be modified other than to mark it
       as [RETRACTED].

   2.  information(t(Patient,Data),sensitivity,Sensitivity)
       may have to GENERATE the label if unlabeled or mislabled!!!

   3.  how should we control the level associated with new information
       added to a patient record. Should we use a "current level"
       concept, automatically label data implicitly by its identity,
       or rely on explicit labeling operations.

   4.  do we need role hierarchies? (NO).

   5.  what to do about researchers? they need access to almost everything
       but it should be retrieved in such a way that it is no longer
       sensitive (ie can't be tied to a particular patient.) This could
       be done with a "unsanitized" prerequisite that could be put on
       all sensitive fields to indicate that retrieval of this information
       might involve dynamically sanitizing it to reduce the sensitivity
       to "non_patient". This might also require that certain fields
       simply be blanked out (address, location, time period, etc.).

   6.  Since there is no concept of "current working level" the SPM has
       no way of specifying the level to be associated with new
       information. There should be a notion of "default information
       level" for each KIND of information so that whoever creates
       information of that kind, it will have the default level
       associated with it (similar to how such information will be
       imported into the system.)

 Notes:

   1.  (961203) PCASSO (in its initial form) will be a read-only system.
       This means that patient-information objects will be created only
       when they are IMPORTed into PCASSO. Information objects will not
       be created by patient-roles. Existing patient-information may be
       augmented by appending to it. Existing partient-information may be
```

corrected by marking it as "[retracted]" and appending the revised information.

2. It might be necessary to restrict access to those portions of a patient's record based on his/her current "problem" or "treatment" or "claim". This could be modeled using information:prerequisites and role:rights by tagging information with a "prerequisite" of the form: problem(Description,Date). This same tag could be added to the appropriate patient's roles.

   In this model, primary care physician needs a "wildcard" right (e.g., problem(*)) to access ALL such information. Secondary care physicians/nurses/... may only need rights for the treatment at hand.

3. Treat insurance providers as "outside" the system. Patient records would be forwarded to them by the physician on a "need-to-know" basis.

4. model treatment/problem as a special "right/prerequisite"
   => prerequisite = problem(description,date)

**********/

Project Phoenix
Policy on Management of Patient Records

1. GOAL

Project Phoenix is committed to maintaining the security of patient records and the confidentiality of patient information in the Georgetown University Medical Center (GUMC)/Total Renal Care, Inc. (TRC) renal care program. It will provide all necessary patient information when needed to authorized personnel. Authorized personnel include unit staff and physicians who provide direct or consulting care to patients. Patients have the right to review their own information at any time. Information will be provided to other personnel as required and formally approved for specific, identified purposes (e.g. billing, quality assurance audits, and regulatory review). On the basis of their professional judgment and sense of ethics, attending physicians may discuss a patient's condition with family members or guardians in the course of providing care. Access to and/or knowledge of patient information is otherwise prohibited.

2. RESPONSIBILITIES REGARDING CONFIDENTIALITY

Managing the confidentiality of patient records is a broad institutional process, not just a function of maintaining the security of patient records in the information system. Project Phoenix recognizes the following types of obligation for maintaining patient confidentiality:

Individual Obligations: In the course of doing their daily work, Project Phoenix staff and investigators will acquire medical, familial, financial and other types of private information about patients in the Georgetown renal care program. They should divulge such information only to authorized persons and for authorized purposes as required. They should never discuss such information outside the context of patient care, quality assurance, authorized research activities, or as required by law or administrative edict. They should attend all inservice training on data security and patient confidentiality. They should read and comprehend Project Phoenix policies, procedures and practices for data security and patient confidentiality. They are individually responsible for seeking answers to questions and/or issues they do not understand in these processes including bringing ambiguous, incomplete or erroneous policies, procedures and practices to the attention of Project Phoenix administrators. Success in discharging these duties merit positive notice in annual evaluations. Failure to discharge one's individual obligations in maintaining patient confidentiality may lead to disciplinary action including possible dismissal.

Administrative Obligations: Project Phoenix principal investigators, investigators and administrators bear responsibility for creating and promoting a climate for maintaining the confidentiality of patient information. Conditions favorable to such a climate include acting as role models in practicing good patient confidentiality practices, developing effective staff inservice training programs on patient confidentiality, aggressively investigating and disciplining potential breaches of patient confidentiality, rewarding exemplary practices in maintaining patient confidentiality, developing and revising as needed policies, procedures and practices for patient confidentiality and communicating a sense of good confidentiality practices to renal care patients. Success in creating and promoting a satisfactory climate for patient confidentiality in Project Phoenix merits positive notice in annual evaluation. Failure to promote a satisfactory climate for patient confidentiality may lead to disciplinary action including reassignment or removal from the project team.

Institutional Obligations: Georgetown University Medical Center and Total Renal Care, Inc. bear responsibility for supporting investigators, administrators and staff in Project Phoenix in their efforts to maintain patient confidentiality. Such support includes agreeing to cooperate in developing jointly acceptable policies, procedures, and practices for maintaining patient confidentiality, assuring project management promotes a climate of patient confidentiality, affirming project management's authority to investigate and discipline potential breaches of patient confidentiality, and including performance in maintaining patient confidentiality as a component of all staff's annual evaluation. Institutional officials should continuously reaffirm the importance of good patient confidentiality practices to the life of the Georgetown renal care community.

3. ADMINISTRATION

1. Managing the security of patient records and confidentiality of patient information is the responsibility of all dialysis unit staff, consulting physicians and Project Phoenix investigators. All staff members are required to have read this policy and to follow it. Failure to adhere to the policy will result in disciplinary action, including immediate dismissal for grave misconduct. Staff members will review the Project Phoenix policy on management of patient records annually and will sign a statement that they have read and understood the policy.

2. Responsibility for planning, implementing and evaluating a system for safeguarding the security of patient records and confidentiality of patient information in the dialysis unit will be assigned to specific administrators as follows:

Project Administrators:
Principal Investigator/Seong Ki Mun, Ph.D.: oversee activities of Project Phoenix investigators
Project Coordinator/Betty Levine, M.S..: coordinate daily operations of Project Phoenix
Clinical Director/James Winchester, MD: consult on clinical issues related to security and confidentiality, coordinate enforcement of policies

Security Administrators:
Team Leader, Security/Jeff Collmann, Ph.D.: plan, implement, and evaluate security measures and policies
Consultant, Security/Lance J. Hoffman, Ph.D.: consult on technical and administrative issues related to security and confidentiality
Consultant, Security/Arwa Al-Aama, M.S.: plan, implement, and evaluate security measures and policies; enhance on-line training tools
Project Engineer/Nassib Khanafer, M.S.: ensure proper operations and adherence to technical security procedures on a day-to-day basis

For questions or comments, please contact Jeff Collmann at (202) 784-3433 or Marion Meissner at (202) 687-1910.

3. The security administrators will routinely perform the following tasks:
a. conduct analyses of the threats to data security and patient confidentiality, and recommend and evaluate measures to improve the security and confidentiality of patient records in the dialysis unit;
b. develop, implement and evaluate policies and procedures for granting authorization for access to and use of patient records;

c. develop, implement and evaluate policies and procedures for conducting regular audits of security measures;
d. monitor electronic audit logs regularly
e. investigate incidents of security breaches

4. Administrators responsible for information management in Project Phoenix will work to coordinate information security practices between the project, Georgetown University Medical Center and Total Renal Care, Inc.

5. Evaluation of the technological needs of the security program in Project Phoenix will occur continuously and throughout the life of the project .

6. Reports on the status, performance, and needs of the technological infrastructure supporting information security in Project Phoenix will be prepared and submitted on a quarterly basis. The reports will include a list of needed improvements ranked according to priority and a budget.

4. METHODS

The records of all patients will be compiled in paper-based and/or computerized patient charts. In order to make patient information freely available to providers and prevent access of unauthorized users, patient charts will be stored in and not be allowed to circulate outside restricted areas, namely the renal care clinic or associated storage facilities. Only authorized personnel and patients will have access to the renal care clinics and associated storage facilities. Measures are taken to protect and assure the security of all data entry, transmission and storage units, including paper charts, dialysis machines and computers.

4.1 Access to Patient Information

4.1.1 Access to the Dialysis Unit

Because patient records are freely available to all persons circulating in the dialysis unit, only authorized personnel may enter the dialysis unit. Authorized personnel are the dialysis patients, all dialysis unit staff, and attending and consulting physicians. Family members or guardians of dialysis patients may enter to assist in preparing patients for beginning or ending dialysis but are otherwise not permitted to remain in the dialysis unit. The unit Head Nurse may grant temporary access to the dialysis unit to other persons as needed. A member of the regular unit staff must accompany all persons with temporary access during their entire stay. The Head Nurse will require all persons with temporary access to sign in and sign out of a visitors logbook. Methods to safeguard the dialysis unit from unauthorized entry during closed hours will be adopted as determined by comprehensive risk analyses.

4.1.2 Access to the Patient Chart

Authorized personnel may consult, add or correct information in the patient chart as required. Patients may review their information and, in consultation with the attending physician, add or correct information, as required. No one is authorized to delete information from the patient chart under any circumstances. Detailed access privileges for the paper-based and computerized patient chart are as follows:

4.1.2.1 Paper-based chart

The following table illustrates the access rights of each staff member to the different parts of the paper-based patient chart.

Chart Component	Access Rights		
	Consult	Add/Correct Information	Discuss w/ Patient, etc.
Dialysis Profile	All Staff		Physician
Flow Sheets	All Staff	Nurse (charge nurse co-signs) Technician (charge nurse co-signs)	Physician
Consent Forms	All Staff	None	Physician Nurse
Lab Results	All Staff	None	Physician Dietitian
Physicians' Orders	All Staff	Physician Licensed Nurse	Physician
History + Physical (Progress Notes)	All Staff	Physician Nurse (charge nurse co-signs) Technician (nurse signs)	Physician
Radiology Results	All Staff	None	Physician
EKG	All Staff	None	Physician
Assessments			
Annual Nursing Assessment	All Staff	Nurse Dietitian Social Worker	Physician Nurse Dietitian Social Worker
Initial Social Work Assessment	All Staff	Social Worker	Physician Social Worker
Patient Care Plan	All Staff	Nurse Dietitian Social Worker	Physician
Consults	All Staff	None	Physician
Discharge	All Staff		Physician

Table 1. Staff access rights to paper-based patient chart

4.1.2.2 Computerized chart

Access to the computerized telemedicine system and its databases will be limited to physicians and staff participating in Project Phoenix and controlled using passwords. Access rights to different parts of the computerized patient information will be determined on the basis of the following categories:

Chart Component	Access Rights		
	Consult	Add/Correct Information	Discuss w/ Patient, etc.
Patient Demographics	All Staff	Physician Telemedicine Nurse	Physician
Dialysis Parameters	All Staff	None	Physician
Still Fistula Images	All Staff	Physician Telemedicine Nurse	Physician
EKG	All Staff	Physician Telemedicine Nurse	Physician
Heart Sounds	All Staff	Physician	Physician

		Telemedicine Nurse	
Fistula Sounds	All Staff	Physician Telemedicine Nurse	Physician
Lung Sounds	All Staff	Physician Telemedicine Nurse	Physician

Table 2. Staff Access Rights to Computerized Patient Information

These access rights will be linked to each user's login ID and enforced by the computer software. All staff members accessing computerized patient records must have their own login ID and password. A login ID will be assigned by the administrator responsible for information management when a new staff member joins the telemedicine project. The administrator will revoke and remove login IDs and passwords of former staff members as soon as the former staff member ceases employment at the renal care unit. Each staff member will create his or her own password and change it regularly according to the guidelines outlined in Appendix 1. Staff members may under no circumstances share their computer password with any other persons.

4.1.3 Access to computerized data during electronic transmission

All patient data will be encrypted during electronic transmission between the local and remote telemedicine computers in order to minimize the risk of unauthorized interception and use.

4.2 Records Storage

4.2.1 Active patient records

4.2.1.1 Paper records

As long as a patient is actively receiving care in the GUMC/TRC renal care program, his or her chart will be stored in the clinic where dialysis takes place. During dialysis sessions, the chart will be placed on top of the dialysis machine or adjacent table to be easily accessible to clinical staff. When the patient is not undergoing dialysis, the chart will be stored on shelves in the dialysis unit.

4.2.1.2 Computerized records

Patients who consent to participate in the telemedicine project will have some information pertinent to their care stored in computerized database(s). As long as a patient consents to participate and actively receives care in the Georgetown telemedicine renal care program, his or her computerized chart will be stored in a central electronic database in the Union Plaza dialysis unit. Data may be electronically transmitted to and stored in computers at other locations, namely, the private office of James Winchester, MD, at 3800 Reservoir Road, Suite 6003, Washington DC, 20007, the home of Dr. Winchester in McLean, Virginia, or a central magnetic tape archive in the ISIS Center, 2115 Wisconsin Avenue, Suite #603, Washington DC, 20007. During dialysis sessions, the telemedicine computer at Union Plaza will be placed in the treatment area. During scheduled and emergency telemedicine consultations, the telemedicine dialysis nurse will connect, operate and evaluate the functioning of the telemedicine computer according to the terms of the “Operations Protocol”. When the Union Plaza renal care center is closed, the telemedicine computer will be locked in Dr. Winchester’s office.

4.2.2 Archived patient records

4.2.2.1 Paper record

The charts of inactive patients will be stored in a secure location away from the site of dialysis. An archive index will be created and maintained to permit easy identification and retrieval of patient charts when necessary. In order to retrieve an archived record, authorized personnel only must issue a formal written request for retrieval from the authorized keeper of the archive. The keeper of the archive may grant a retrieval request only after verifying the identity of the requester and confirming that the requester is authorized to use the chart. Requests will be logged and initialed by the requester and the keeper of the archive. Records will be transported between the archive and other locations in a secure manner.

4.2.2.2 Computerized record

The computerized charts of inactive patients and older records of active patients will be stored in a long term magnetic tape archive in the ISIS Center, 2115 Wisconsin Avenue, Suite #603, Washington, DC 20007. An archive index will be created and maintained to permit easy identification and retrieval of patient charts when necessary. Access to the long term archive using either the Internet or local workstations will be restricted to authorized personnel and will be controlled using computerized access controls and authentication procedures. Other security measures, including but not limited to encryption, will be evaluated and implemented as needed.

4.2.3 Research data containing patient information

Research data generated by Project Phoenix, which may include some patient information, will be stored in a locked cabinet at the corresponding dialysis unit. Only the telemedicine nurse and the researchers involved with Project Phoenix will have access to this data and they will use it solely for the purposes of the project.

4.3 Training

4.3.1 Initial staff and physician training

New dialysis unit staff will receive detailed training about the policies, procedures and methods of safeguarding the security and confidentiality of patient records as part of their initial orientation (see attached training materials in Appendix 2). Physicians will also receive detailed training on the policies, procedures and methods of safeguarding the security and confidentiality of patient records upon receiving initial privileges to admit patients to the dialysis unit. All physicians and staff will receive special training in the operation and methods for assuring security of computerized patient records as part of inaugurating the telemedicine network.

4.3.2 Updates to Policies

Dialysis unit staff and physicians will receive updates to the policies, procedures, and methods of safeguarding the security and confidentiality of paper-based and computerized patient records as changes occur.

4.3.3 Annual review

A thorough review of the policies, procedures and methods of safeguarding the security and confidentiality of paper-based and computerized patient records will occur at least one time per year as part of each staff member's annual performance evaluation. Staff will be required to reaffirm their commitment to the principles of patient confidentiality as part of completing their annual evaluation.

4.3.4 Manual in Data Security and Confidentiality:

All staff and physicians will receive a manual outlining all policies, procedures and methods of safeguarding the security and confidentiality of patient records in Project Phoenix during initial training. Copies of the manual will be stored in all participating renal care clinics, the regional and national headquarters of TRC, Inc., the office of the Georgetown medical director, and the ISIS Center. This manual will be updated as necessary with no fewer than one complete review per year.

4.4 Patient Education in Information Management Policies, Procedures and Methods

4.4.1 Informed Consent

Patients will be briefed on the policies, procedures, and methods of safeguarding the security and confidentiality of their dialysis information as part of their initial orientation to the dialysis center. Patients are entitled to receive as much information about the management of their records as necessary to answer their questions, including the right to question their physician and/or the information management administrators.

4.4.2 Patient's guide to data security

A patient's guide to data security, outlining all policies, procedures and methods of safeguarding the security and confidentiality of patient records in Project Phoenix, will be prepared. All patients will receive copies as part of their initial orientation to the dialysis center. Copies of the guide will be stored in all participating renal care clinics, the regional and national headquarters of TRC, Inc., the office of the Georgetown medical director, and the ISIS Center. This guide will be updated as necessary with no fewer than one complete review per year.

4.4.3 Patient review of data

Patients will be informed of their right to review and, in consultation with the attending physician, add or correct information in their chart, as required.

Project Phoenix
Policy Compliance Statement

I understand that confidential patient information may be divulged only

- to authorized persons,
- for authorized purposes, and
- in authorized contexts.

I understand that it is my responsibility to seek answers to any questions I have about patient confidentiality and data security in the context of Project Phoenix.

I have read and understood the Project Phoenix Policy on Management of Patient Records and agree to adhere to this policy to the best of my abilities.

_____
Employee Name (Printed)

_____ _____
Employee Signature Date

Toolkit Section 4.4

Assigning Roles and Responsibilities

Toolkit Section 4.4.1

Introduction

The "security team" includes everybody in the organization, including staff, partners, vendors, and patients. Leaving "security" to the information technologists does everyone a disservice. Without every staff member implementing sound security practices in their own work, the contributions of the IT professionals will fail. Without IT professionals understanding the organizational and clinical setting, they risk developing inappropriate tools protecting the wrong assets. Relying only on "technological fixes", moreover, potentially creates a false sense of security that cannot possibly exist. An effective information security program depends on diligent and coordinated efforts under centralized responsibility. An organization's information security program should guide and formulate its overall security approach. CPRI has produced a document entitled "Guidelines for Managing Information Security Programs" which outlines how organizations can implement effective structures for maintaining confidentiality and security. It outlines the roles and responsibilities for an information security manager and describes an organizational structure for effectively leading the effort. Some highlights of the information security function include:

1. Information security must be perceived to be organization-wide.
2. Information security must be led by a central authority (the "information security manager") with ownership shared by all other information and system users.
3. The information security manager must be aware of continual changes in health care and security and must understand the impact of security on patient care and business operations.
4. Information security teams should include advisors from all organizational functions including information technology, clinical functions, risk management, finance/patient accounting, human resources, patient relations, quality assurance and legal counsel.

Guidelines
For
Managing Information Security Programs
At
Organizations Using Computer-based Patient Records

Prepared by
CPRI Work Group on
Confidentiality, Privacy, & Security

January 1996

Computer-based Patient Record Institute
Advancing health care through information technology

Guidelines
For
Managing Information Security Programs
At
Organizations Using Computer-based Patient Records

Prepared by
CPRI Work Group on
Confidentiality, Privacy, & Security

January 1996

Computer-based Patient Record Institute
Advancing health care through information technology

Computer-based Patient Record Institute
Advancing health care through information technology

Guidelines for Managing Information Security Programs
At Organizations Using Computer-based Patient Records

© Copyright 1996, by the Computer-based Patient Record Institute. All rights reserved.

No part of this publication may be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

Printed in the United States of America

This book was prepared camera-ready.

Guidelines for Managing Information Security Programs at Organizations Using Computer-based Patient Record Systems

Overview

The Computer-based Patient Record Institute Work Group on Confidentiality, Privacy, and Security was established to encourage creation of policies and the implementation of mechanisms which protect patient and caregiver privacy as well as preserve the confidentiality, protect the integrity, and ensure the availability of information in computer-based patient record systems.

During the early phases of its efforts, the Work Group determined that although computer-based patient records (CPRs) offer the potential for achieving greater protection of health information than can be provided with paper-based records, it is necessary that formal information security programs be established by each organization entrusted with health information in order to achieve an appropriate and consistent level of protection.

Therefore, in addition to its other activities, the Work Group is developing a series of information security guidelines to assist organizations implementing computer-based patient record systems to establish formal information security programs.

The other documents in this series that have been published are:

- *Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Record Systems*
- *Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Record Systems*

Additional guidelines are being developed to address:

- *Information security terms.*
- Implementing electronic signatures.
- Methods for identifying and authenticating users of computer-based patient records.
- Developing confidentiality statements and agreements.
- System and application security features.
- Security audit functions and processes.

Acknowledgments

This document was prepared by members of the Work Group on Confidentiality, Privacy, and Security, Kathleen Frawley and Dale W. Miller, Co-Chairpersons. The material for the document and the initial versions were prepared by the Project Team on Information Security Management led by Kenneth Kung.

The Project Team Leader and Work Group Co-Chairpersons are indebted to the many volunteers who participated in the work group meetings, provided input, and prepared and reviewed the drafts of this document.

Table of Contents

Overview iii

Acknowledgments iv

Introduction 1

Objectives 1

Scope 1

Managing the Information Security Program 2

- Purpose and Function 2
- Organizational Infrastructure 2
- Reporting Relationships 4
- Working Relationships 4
- Authority and Responsibility 5
- Accountability 5

Information Security Management Functions 6

- Planning 6
- Organizing 7
- Directing and Implementing 7
- Reporting 7
- Communicating 7
- Supporting Incident Response and Investigation 8

Staffing Considerations 8

- Skills and Abilities 8
- Determining the Number of Persons Required 9

References 10

Guidelines for Managing Information Security Programs at Organizations Using Computer-based Patient Record Systems

Introduction

Ensuring that health information is protected from unauthorized disclosure and safeguarded to prevent unauthorized modification or destruction is an essential prerequisite for implementing computer-based patient record systems. Because of the diversity of the organizational issues and the technical complexity of the systems and networks, protecting health information can be achieved most effectively with an organization-wide program.

A comprehensive information security program consists of written policies, standards, training, technical and procedural controls, risk assessment, auditing and monitoring, and assigned responsibility for management of the information security program. Although often considered a component of the program, assigned responsibility for managing the program is unique in that the other components will not be totally effective without successful program management.

This document has been prepared by the Work Group on Confidentiality, Privacy, and Security to provide recommendations for managing the information security programs at organizations implementing computer-based patient record systems.

Objectives

The objectives of the work group in developing these guidelines are to:

- Foster the recognition of the need to establish an organizational infrastructure to implement and maintain the information security program.
- Encourage and facilitate effective management of the information security program by defining the functions and responsibilities of information security management.
- Assist organizations to select, appoint, and educate information security managers.
- Provide a reference document for information security managers.
- Facilitate information security management in all organizations.

Scope

This document is intended to be applicable to organizations that utilize computer-based patient record systems to collect, create, receive, store, report, and process health information. All health care provider organizations - hospitals, physician offices, home health agencies, pharmacies, nursing homes, and others - will benefit from applying the principles described in these guidelines.

Managing the Information Security Program

Managing the information security program in an organization using computer-based patient record systems presents significant challenges. Information is typically collected, stored, and processed in all departments and locations of the organization, including within hospital facilities, clinics, physicians' offices, research facilities, pharmacies, etc.

Diverse types of media, systems, and networks are used for the storage and transmission of confidential patient and caregiver information. The confidentiality, integrity, and availability of such information must be protected with consistent, effective measures. Staff members and others who may have access must be informed of the importance of protecting the information and about their specific responsibilities for information protection. Appropriate techniques and mechanisms to protect the information must be provided and communicated to all users of information.

The information security manager must be alert to continual changes in the dynamic healthcare environment. Healthcare organizational structures are changing. Community and regional health systems and networks are being formed. Legal and accreditation requirements for protecting patient privacy are changing. Security technology is evolving rapidly. The installation of computer-based patient record systems and networks dictates evaluating risks, determining system and network security requirements, and implementing appropriate controls.

The information security manager must be prepared to implement measures for information protection in an environment where these measures are sometimes incorrectly perceived as an impediment to providing care and completing business functions.

Purpose and Function

The information security manager serves as the central focal point for the overall coordination of security policy and procedures for the organization. This responsibility is shared with management, caregivers, and all other information and system users. The information security manager identifies potential exposures and risks to the confidentiality, integrity, and availability of information and makes recommendations to management to mitigate the risks.

It is the responsibility of the information security manager to identify the impact on the information security program of changes in the patient-cue, business, and computer systems environments in the healthcare industry and specifically within the organization. Based on an awareness of the industry and organizational needs, the information security manager should direct and/or modify the information security program. The scope of this responsibility encompasses the organization's information in its entirety.

Organizational Infrastructure

Depending upon the size and complexity of the organization, the information security function may range from a part-time assignment for one person to a unit with a full-time information security manager and multiple information security staff members. The information security unit is typically assigned to the chief information officer but may be assigned to any senior manager in the organization if that manager will provide the most effective reporting arrangement.

The information security function should be perceived to be an organization-wide function and not an entity that is limited to a specific department or person. Therefore, except for system security functions, which can be successfully managed by the information systems organization with advice from the information security manager, many of the security administration functions will be distributed throughout the organization.

When planning the staffing requirements for systems and application security administration in organizations with fully implemented computer-based patient record systems, it is important to consider that the need for separate system security administrators is likely to be considerably less than in organizations with traditional information systems and paper-based records. With computer-based patient record systems the security functions are more likely to be integrated with other automated functions. The discrete functions of approving and granting access to information that are currently performed by security administrators are likely to be accomplished automatically by caregivers and managers as an integrated component of routine management and scheduling functions included in computer-based patient record systems.

An information security advisory group should be formed to provide advice and support to the information security manager. Typical functions of this group include reviewing proposed policies, standards, procedures, and education programs.

Members of an information security advisory group should include but not be limited to:

- chief information officer
- health information manager
- representatives of physicians, nurses, and other caregivers
- risk manager
- finance and patient accounting manager
- human resources manager
- patient relations manager
- quality assurance
- legal counsel

Reporting Relationships

The information security manager reports to the chief information officer or similar senior manager for management and administration purposes, but the scope of the position is organization-wide and involves information on all types of media and in all representations, patient clinical and administrative information, financial information, caregiver information, employee records, organization strategic and administrative information, and computer software. The information security manager maintains an allegiance to the goals and objectives of the organizations information security program rather than to a specific manager or department.

Working Relationships

The information security manager must maintain a working relationship with representatives from all functional areas of the organization including but not limited to:

- Chief information officer - direct reporting relationship as well as support for implementation of information security controls in systems and networks.
- Chief executive officer - provide status reports, advice, apprise of serious incidents, and recommend policy.
- Senior and middle management, caregivers and other staff - foster awareness, determine responsibility for protection of information assets, and provide advice and on-going education.
- Internal and external auditors - report on status of information security measures as requested and respond to audit findings on information security issues.
- Consultants and vendors - convey information security requirements.

Authority and Responsibility

The information security manager is responsible for:

- Implementing and maintaining a process for defining the organization's goals and objectives for information security.
- Determining the methodology and procedures for accomplishing the goals of the information security functions.
- Proposing information security policies to senior management and establishing standards and programs to implement the policies.
- Determining which security incidents and findings will be communicated to senior management.
- Determining the adequacy of risk assessment and the appropriateness of risk acceptance.
- Determining information ownership responsibilities or when ownership decisions must be escalated.
- Making personnel and administrative decisions in the supervision of the information security and computer access control administration staff, including hiring, termination, and training.
- Controlling the use and expenditure of budgeted funds.
- preparing a quarterly status report for the chief executive officer on the following programs:
    - Compliance with security provisions of accrediting and regulating organizations.
    - Awareness training.
    - Information security incidents.
    - Audit issues raised by internal or external auditors.
    - Management concerns and recommendations related to information security.
    - Risk assessments.
    - Access control administration function.

Accountability

The information security manager is accountable for successful implementation of the information security program. Therefore the information security manager must:

- Maintain a broad range of technical knowledge about systems, networks, and telecommunications.

- Maintain a detailed technical knowledge about information security technology.
- Effectively manage staffing and budget.
- Ensure competent, motivated and knowledgeable staff, able to function effectively in a dynamic environment.
- Provide prompt information security support to all users of the organization's systems and networks.
- Maintain effective communications with all departments of the organization and with appropriate vendor and industry personnel.

Information Security Management Functions

Planning

The information security manager is responsible for planning all aspects of the information security program including:

- The process for establishing or updating policies and standards encompassing regulatory and legislative security requirements as applicable.
- Design and implementation of procedures to implement the policies.
- System security facilities and the functional requirements for security mechanisms.
- Measures to ensure that information is not altered or lost during capture, storage, processing, communication, or translation from one coding system to another.
- Converting to different storage media, scheduling of retention, preservation of historical data, and secure disposal.
- Implementation and management of access control, including user identification and authentication, and assignment and removal of user access privileges.
- Measures to account for the origin of every data item, non-repudiation, integrity, transportability, multiple signatures, signature attributes, and countersignatures.
- Ensuring continuous availability of information, maintaining data integrity in the event of system failure, restoration of lost or damaged data, development of a disaster plan, planned drills to test the plan and recovery procedures, and the actual recovery of the information after a disaster.
- Audit trails and support for the performance of audits.
- Use of encryption and the management of encryption keys.

Organizing

The information security manager identifies the resources needed to maintain the effectiveness of the program and works with senior management to assign responsibilities throughout the organization. The information security manager also recommends priorities for reducing exposures and addressing outstanding information security issues.

The responsibilities for organizing include preparing budgets, performance plans and evaluations, training plans and career counseling, and conducting other administrative tasks related to the management of the information security function.

Directing and Implementing

The information security manager directs the activities of the information security staff. Optionally, the information security manager may also direct the activities of the computer access control administration staff

Specific responsibilities for directing the program include:

- Administering information security policy throughout the organization and making policy decisions on the adequacy of information security measures and procedures or ensuring that those decisions are made by the appropriate level of management.
- Identifying high-risk situations, apprising management of the risk, and coordinates activities to reduce the risk.
- Responding to information security incidents, determining corrective action to be taken, and designing and implementing preventative measures.
- Ensuring that information security resources are used most productively and that the appropriate parties are involved in information security decisions.
- Leading the risk assessment process for major systems and applications changes.

Reporting

The information security manager monitors overall organization compliance with the information security program. The information security manager determines the information to be collected for monitoring the program and consolidates this information for reports to the chief information officer and the chief executive officer. The information security manager may not typically perform audits, but utilizes the results of audits performed by internal and external auditors to improve the information security program.

Communicating

The information security manager promotes information security awareness throughout the organization to all levels of management and to all employees and professional staff members. The

information security manager provides a central source of information on state-of-the-art information security techniques and products and acts as the principal representative for information security on various teams, task forces, and committees.

In order for a health care provider to achieve an appropriate level of information protection, the policies and mechanisms for information security must be clearly communicated throughout the entire organization. While it is the responsibility of all levels of management to ensure compliance with established policies, It should be the responsibility of the security manager to provide for the communication of security policies and procedures. Suggested communication tools have been defined in the *Guidelines for Information Security Education Programs at Organizations Using Computer-based Record Systems (CPRI, 1995).*

Supporting Incident Response and Investigation

Breaches of confidentiality and violations or suspected violations of policy should be reported to the information security manager. Procedures for reporting potential exposures should be established. Reporting mechanisms for incidents and violations of policy should clearly define notification requirements, investigative procedures, and outcomes reporting procedures. The information security manager should be included on risk management committees.

Staffing Considerations

As with most functions in health care organizations, the success of the information security program is dependent upon the dedication, abilities, and performance of those performing information security management functions.

Selection of individuals to serve as information security manager and members of the information security staff, or to serve those functions is important.

Skills and Abilities

The information security manager should be an advocate for information security and have the following skills and abilities:

- Excellent communication skills.
- Management skills.
- Ability to organize and direct educational programs for all levels of staff on information security topics.
- Knowledgeable about the organization structure, methodologies, and organization culture.
- Ability to direct projects and participate in teams.
- Knowledge of current technical and procedural techniques in information security.
- Ability to identify and evaluate information security risks and exposures.

- Knowledgeable about state and federal regulations, accrediting organizations and healthcare industry standards, and litigation avoidance issues relative to information security matters.
- Knowledge of the information security requirements of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) Accreditation Manual.
- Ability to establish liaisons with internal and external constituencies with respect to information security matters.
- Knowledgeable about the relationship of computers and technology to the organization's environment and the impact of systems on the security of the organization's information.
- Certification as a Certified Information Systems Security Professional is preferred.

Determining the Number of Persons Required

Although the information security manager position is a part-time function in smaller organizations, larger organizations may require a full-time information security manager as well as several information security staff members to successfully implement and manage the information security program.

The staff resources for establishing a program are significantly greater than the resources required to manage a well-designed program. Additional resources will be required in those organizations in which the information security manager is also responsible for systems access control administration.

There does not appear to be a specific relationship between the size of the organization and the number of information security staff members required. The complexity of the organization, the status of the information security program, and the rate of change in the organization structure and systems and networks are more significant factors in determining the resources required.

References

Dick, R. S. and Steen, E.B., editors *The Computer-based Patient Record: An Essential Technology for Health Care.* Washington, DC: National Academy Press, 1991.

Donaldson, M.S. and Lohr, K.N., editors *Health Data in the Information Age: Use, Disclosure, and Privacy.* Washington, DC: National Academy Press, 1994.

Kunitz and Associates, Inc. *Final Report of the Task Force on the Privacy of Private-Sector Health Records.* Contract BHS-100-91-0036. Rockville: KAI, September 1995.

Louis Harris and Associates. *Harris-Equifax: Health Information Privacy Survey 1993.* New York: Louis Harris and Associates, 1993.

Louis Harris and Associates. *Equifax-Harris: Consumer Privacy Survey 1994.* New York: Louis Harris and Associates, 1994.

Madsen, W. *7he Handbook of Personal Data Protection.* New York: Stockton Press, 1992.

System Security Study Committee, National Research Council. *Computers at Risk: Safe Computing in the Information Age.* Washington, DC: National Academy Press, 1991.

US Congress, Office of Technology Assessment. *Protecting Privacy in Computerized Medical Information.* OTA-TCT-576. Washington, DC: Government Printing Office, September 1993.

CPRI Members

3M Hlth Info Sys
Adventist Hlth Sys/Sunbelt
ALLTEL Info Svcs - Hlthcare Div
Amer Aced of Family Physicians
Amer Aced of Pediatrics
Amer Assn for Med Transcription
Amer Board of Family Practice
Amer College of Physicians
Amer Hlth Info Mgmt Assn
Amer Hospital Assn
Amer Med Informatics Assn
Amer Medical Assn
Amer Org of Nurse Executives
Andersen Consulting, LLP
Arkive Information Systems
Assn of Operating Rm Nurses
Chi Systems
Coll of Amer Pathologists
Coll of Hlthcare Info Mgmt Execs
Columbia JHCA Hlthcare
Ctr for Hlthcare Info Mgmt
Ctrs for Disease Control & Prev
Dept of Veterans Affairs
Dynamic Hlthcare Tech
Eli Lilly and Company
Ernst & Young, LLP
Glaxo Wellcome
Group Hlth Assn of Amer
Harvard Comm Hlth Plan
HBO & Company
Hlth Industry Mnfrs Assn
Hlth Level Sam
Healthdyne
HealthVISION Corp
Inst for Clin Sys Irteg
Interpractice Sys
JCAHO
Kaiser Permanente
Management Systems Assoc
Mayo Foundation
Medic Alert Fnd US
Medical Connections
Medical Records Inst
MedicaLogic
Medicus Systems
Motorola
Natl Assn of Chain Drug Stores
Natl Cncl for Pres Drug Progs
NC Hlth Care Info & Comm Allnce
NEON Hlthcare Software
Northwestern Memorial Hosp
Oceania
PHAMIS
Physician Micro Systems
Prudential Insurance Co
SIDOCI Enr
Sisters of Mercy Hlth Sys
SoftMed/HIS
Systems Plus
The Permanente Med Group
ThetaPro
Unitron Med Comm
Univ Hlth System Consortium
Univ of IA Hosp & Clinics
Univ of VA Hlth Sci Ctr

CPRI is a non-profit membership organization committed to advancing improvements in health care quality, cost and access through routine use of information technology. CPRI serves as a neutral forum for bringing the diverse interests of all health care stakeholders together to develop common solutions.

CPRI functions primarily through the voluntary work of its work groups. All individuals are invited to participate in one of the following:

- Work Group on Codes & Structures
- Work Group on Confidentiality, Privacy & Security
- Work Group on CPR Description
- Work Group on CPR Systems Evaluation
- Work Group on Professional & Public Education

All Kids Count
National Immunization Program, Centers for Disease Control and Prevention

Information Security and Immunization Information Systems

rev. February 25, 1996

prepared by

Dr. Noam H. Arzt
Research Associate/Senior Fellow, Leonard Davis Institute of Health Economics
Suite 221A, 3401 Walnut Street, Philadelphia, PA 19104
215/898-3029 (Voice); 215/898-9348 (FAX)
arzt@isc.upenn.edu
URL: http://nextb.dccs.upenn.edu/noam.html

Introduction

Many states and territories, and municipalities are developing an electronic registry for immunization information (Immunization Information System, or IIS). Part of the acquisition or development of these systems is a process of dealing with threats to information security, and possible steps that can be taken to mitigate these threats. Information security is defined as ". . . a set of technical and administrative procedures designed to protect data systems against unwarranted disclosure, modification, or destruction and to safeguard the system itself."[1] The specific goals of this effort are:

- Maintain the integrity of the data under the Program's stewardship
- Make the data available easily to legitimate users
- Ensure the privacy and appropriate use of patient data[2]

The notion of information security and ease of access are often tradeoffs of one another: ease of access can compromise information security if not done carefully, and too much security can make an application difficult or impossible to use even by valid users. Yet many information technology professionals do not consider information security that critical. Consider a recent Ernst & Young Security Survey: Almost 50% of respondents rated information security issues as "less than important."[3]

Methodology

A six step methodologyis described in this paper:

1. Identify the information assets that need protecting
2. Describe the architecture of the information system to be deployed
3. Identify the threats to those information assets based on the architecture
4. Rank the threats on a high/medium/low scale and identify the most serious threats
5. Develop solutions to mitigate the threats as much as possible
6. Make specific recommendations of solutions for deployment

---

[1] Lawrence O. Gostin, *et al.*, "Privacy and Security of Personal Information in a New Health Care System," *Journal of the American Medical Association*, 270(20), Nov. 24, 1993, p 2487.

[2] *Idem.*

[3] Ernst & Young/Information Week, "2nd Annual Information Security Survey," Sept., 1994.

Information Assets

Before one can secure information, one has to identify the information itself and the reasons why a certain level of security may be necessary. An IIS database is typically described in a design document, and usually contains at minimum the core data set as defined by the National Immunization Program at the CDC. The major groupings of information are typically:

Information about **People**	Includes patient biographical/demographic data, aliases of names, information about relatives and guardians, immunization provider information
Information about **Patient Records**	Focuses on the relationship between a patient and an immunization provider
Information about **Immunizations**	Includes immunizations administered, normative schedule information, vaccine vendor information
Information about **Registry Output**	Patient/family outreach information
Information about **Technical Aspects**	Includes system user profiles and permissions, system access logs
Code tables	Various code tables for valid values of various database elements

Medical information systems containing data that can be linked to individual patients must take precautions to prevent the inappropriate disclosure of this information, and to protect the rights of the individuals whose information is contained in the system. Specifically, the United States Department of Health, Education and Welfare articulated these responsibilities in 1973 as follows (*note additional comments in italics*):[4]

- There must be no personal data record-keeping systems whose very existence is secret.

  Notice and disclosure: need to tell a patient the data system exists, and that their data may be in there.

- There must be a way for an individual to find our what information about him is in a record and how it is used.

- There must be a way for an individual to prevent information about him that was obtained for one purpose for being used or made available for other purposes without

[4] Based on a presentation by Dr. Christine Harbs, All Kids Count National Program Meeting, Atlanta, GA, March 3, 1995.

his consent.

The agency building the system itself needs to know how information is being used. Often a public relations brochure is helpful. A disclosure log is probably wise.

- There must be a way for an individual to correct or amend a record of identifiable information about him.

Just because the individual suggests a correction does not mean that the original data should be removed. The suggested correction can simply be noted.

- Any organization creating, maintaining, using,or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of data.

An IIS certainly qualifies as a medical information system whose policies should be sensitive to these concerns. In 1980, a federal court of appeals ruling[5] added some additional insight into balancing various factors in determining an appropriate approach to information security:

> (1) the type of health care record and information it contains; (2) the potential harm from any unauthorized disclosure; (3) the injury from disclosure to the relationship in which the record was generated; (4) the adequacy of safeguards to prevent non-consensual disclosure; and (5) the degree of need for access.[6]

Immunization data is not the *most* sensitive of medical information, and the potential harm from unauthorized disclosure is likely minimal. Nevertheless, Projects have a responsibility to protect the integrity of the system from inappropriate damage, and to respect the privacy of the individuals whose data is entrusted to the Project's care. Since the risk of communicable disease may be high in a given population, access to immunization information as an aid to reducing this risk is critical.

It is important, however, to recognize secondary effects that can result from improper access to the IIS, and from its improper use. Several examples illustrate these concerns:

> A manufacturer recall of a vaccine lot may result in patients having received vaccine that may be harmful. Inadvertent disclosure of this information improperly may violate the privacy of the patient involved.
>
> Certain adverse reactions, or pre-existing information (such as HIV infection), may violate the privacy of a patient if disclosed improperly. While it is not its intention, the IIS has the potential to store this information if a user enters it.
>
> Address/contact information in the IIS could inadvertently be used to locate a parent or child improperly (e.g. cases of adoption, legal restraining order, etc.).

[5] *United States v Westinghouse Electric Corp*, 638 F2d 570 (3rd Cir 1980).

[6] Gostin, *et al.*, p. 2489.

Policies developed for use with the IIS must address these issues. The IIS applications need to be created to support the objectives of these policies.

Individual state, territories, or municipalities may have local laws that relate to information security in general, or medical information in specific. It is important to research these local laws for applicability to the IIS project.

System Architecture

The IIS is usually deployed within a systems architecture which is often part of a larger technical architecture for the state, territory or municipality. A Technical Architecture is a blueprint for how future technology acquisitions and deployment will take place. It consists of standard, investment decisions, and product selections for hardware, software and communications. The Technical Architecture is developed first and foremost based on community direction and business requirements.

Additionally, principles are used rigorously to be sure the Technical Architecture is consistent with the community's information technology beliefs. The current (de facto) technical architecture is taken into consideration, as well as relevant industry and technology trends.

A typical systems architecture for an IIS is displayed in Figure 1.

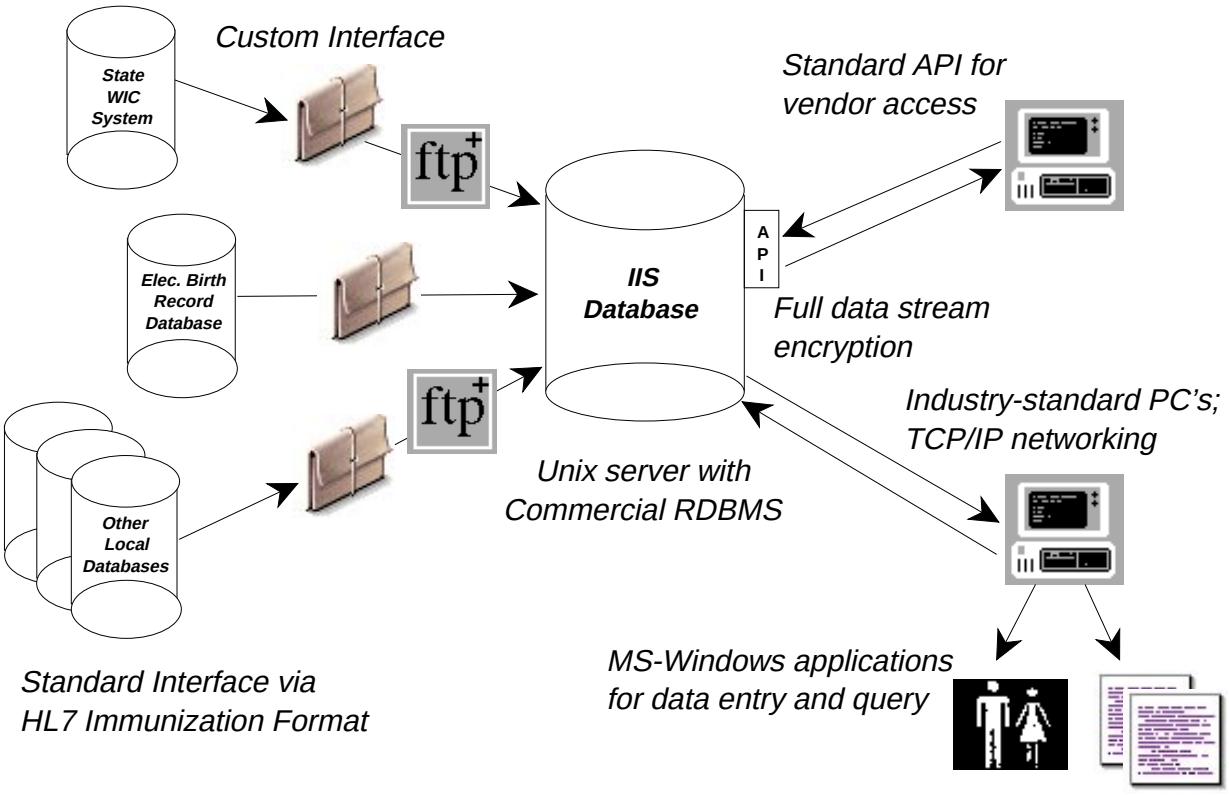


Figure 1 - Sample IIS Systems Architecture

The major components of an architecture are:

Database	The database management system (e.g.,Oracle 7) and the server upon which it runs.

Client Computers	The client computers (e.g. terminals, industry-standard personal computers) including hardware configuration and desktop operating system (if applicable).
Network Protocol	TCP/IP, SNA as appropriate.
Wide-area Network	Examples include proprietary networks, existing State-wide network, the Internet.
Applications	Description of client applications, whether they are host-based or client/server - what tools are used to create them, and how they connect to the IIS database, if applicable.
Query Tools	Additional "off-the-shelf" or custom-developed/provided query tools are expected to be deployed, and their connectivity to the IIS database.
Data Collection	Methods by which data will enter the IIS, either by being "harvested" via electronic interface from a WIC system, an Electronic Birth System, or from other local data systems found in clinical provider locations.
Data Access	Eventually, an applications program interface (API) might be developed to allow vendors to write software that accesses data in the IIS for transfer to local data systems found in clinical provider locations.
User Access	Methods by which on-line users receive direct or indirect access to the IIS

Once an architecture is defined, it helps set the framework for how the information assets will be protected. It helps to identify the threats and risks which are defined in the sections that follow.

Detailed Threat Analysis[7]

A set of possible threats to an IIS have been developed. The following table lists a description of each potential threat to Registry data. This table should be reviewed, and a ranking should be conducted of these threats on two scales:

> **Risk**: The likelihood that the particular threat to the information identified above will take place, based on the technical architecture for the Project.
>
> **Harm**: The severity of the harm if the threat in fact came to pass.

In other words, just because a threat is likely does not mean its impact is severe. And just because the impact of a threat may be severe it does not mean it is likely.

Risk and Harm should be assessed for each threat below on a High (H)/Medium (M)/Low (L) scale. When the analysis is complete, the search for solutions should focus on those threats where the likelihood of the risk occurring, and the harm that might be incurred should the risk occur, are reasonably high.

Threats are divided into three categories:

> **Desktop**: Those threats that relate to the desktop, whether it be a terminal or personal computer.
>
> **Server**: Those threats that relate to the IIS server and its integrity.
>
> **Network**: Those threats that relate to the network that connects users desktops to the IIS server.

Each description is followed by a rationale which describes a typical rating for each threat. The rationale for a particular IIS project may be different. The sample rationales most closely follow those of a client/server deployment.

A. DESKTOP THREATS

THREAT A-1: Unauthorized access to someone's desktop resulting in disclosure of sensitive data that has been stored on the desktop.

RATIONALE: Sensitive data is likely to either be stored on the desktop, or visible as the IIS application is on a user's screen. It is the deployment site's responsibility to control physical access to desktop computers within their facilities by preventing inappropriate access to desktop computers, and by ensuring that the IIS application is not left on a computer screen unattended.

[7] Based on a framework developed at the University of Pennsylvania in the fall of 1994.

THREAT A-2: Someone finds sensitive data stored on a workstation and alters or destroys the data.

RATIONALE: Unauthorized access to medical systems is possible, and risk of alteration is present.

THREAT A-3: Someone alters the application code on the desktop making it possible to use the modified code to change data on the database server or access sensitive data on the server.

RATIONALE: The RISK is typically LOW because it is usually be very difficult to modify object modules in a way the application would still function and also access and modify data on the server. The HARM might be rated HIGH because serious damage could be done to the data on the server, and potentially go undetected.

THREAT A-4: Someone violates a software license by running unlicensed copies of software.

RATIONALE: The RISK is usually LOW because it is unlikely that an unlicensed use of software would be detected. The HARM might be rated HIGH because a commercial vendor would have legal means to significantly penalize the Project (if applicable).

THREAT A-5: The user of a desktop accidentally deletes an important local file.

RATIONALE: The RISK is often rated HIGH in client/server systems because it is easy to delete files accidentally on a workstation. The HARM is usually rated MEDIUM because while local data files are not the Project's concern, local Project software could be rendered inoperable.

THREAT A-6: Someone accidentally or intentionally infects a desktop with a virus.

RATIONALE: The RISK is usually rated MEDIUM because virus are most prevalent on workstations, easily transmitted via floppy disks and it is believed a substantial number of users do not run virus protection software. The HARM is usually rated LOW because it should be possible to recover the workstation from the damage that most viruses cause.

THREAT A-7: Physical damage or destruction to a desktop (fire, broken water pipes, riot, etc.)

RATIONALE: The RISK is usually rated LOW because the occurrence of events that damage workstations is low. The HARM was rated MEDIUM because, in the event that there was destruction of a workstation, lack of off site backups and other recovery information would make it difficult to recover the data lost on the machine.

B. SERVER THREATS

THREAT B-1: Someone accesses the server and uses a program to guess passwords, or some similar tool, to find IDs and passwords that they can use to get on the system and read or alter data.

RATIONALE: The RISK varies depending on how accessible the server is. The HARM is usually rated HIGH because if someone ever did break into the server damage could be done.

THREAT B-2: Special accounts that have the authority to damage the system if not used properly, such as the root or system account, are compromised by an intruder and the intruder alters the system, sometimes with the intent of making subsequent access easier.

RATIONALE: The RISK is usually rated MEDIUM because most individuals trying to break into a system are likely to go after the special accounts. The HARM is usually rated HIGH because severe damage can be done from a special account.

THREAT B-3: System administrators with root authority (most privileged user status) use the account to make changes to the system that are not part of their responsibilities, or give themselves additional authority for future breaches of security.

RATIONALE: The RISK is usually rated LOW because it is not likely that the responsible individuals given that authority would abuse it. The HARM is usually rated HIGH because if they did abuse it, severe damage could be done.

THREAT B-4: Vulnerable accounts (dormant accounts, retired accounts, accounts without passwords, accounts with weak passwords, etc.) are used to gain access to data or set up future access to the system.

RATIONALE: The RISK is usually rated MEDIUM because people trying to break into an account also target carelessly managed accounts. The HARM is usually rated MEDIUM because these accounts typically don’t have the authority to damage the system.

THREAT B-5: Someone obtains an ID with authorization beyond what they should have been granted and uses it to read or delete files or to make changes to allow future access to the system.

RATIONALE: The RISK is usually rated LOW because there would be sufficient administrative policies in place to prevent such a request from being made with out the proper authorization. The HARM is usually rated MEDIUM because the account still would not be a special account and the potential for damage is not high.

THREAT B-6: An intruder gains access to a machine and has been detected. The system

administrator is unable to determine what damage was done, and so cannot recover from the damage.

RATIONALE: The RISK is usually rated MEDIUM because there are a number of people attempting to break into systems, and there is a good chance the could change something that would go undetected. The HARM is usually rated LOW because most break-ins are not with the intent of damaging the system and the account that would be compromised is not likely to be a special account.

THREAT B-7: Someone who has access to the system as part of their job responsibilities uses that access to destroy data or programs.

RATIONALE: The RISK is usually rated LOW because there are usually a small number of people with direct (*i.e.,* logon access) to the system. The HARM is usually rated LOW because they don't usually have the authority or knowledge to find programs or files that they shouldn't have access to.

THREAT B-8: Someone who has access to the system as part of their job responsibilities, uses that access to find and modify source code in order to execute it to make changes or read data they were not authorized to access.

RATIONALE: The RISK is usually rated LOW because it is unlikely that the user would be able to locate or change code to work as the planned. The HARM is usually rated HIGH because if they were successful, they could do severe, undetected damage to the integrity of the data.

THREAT B-9 Someone exploits weaknesses of network mounted file systems or NIS IDs or passwords and modifies or reads data not intended for them.

RATIONALE: The RISK is usually rated LOW because these services are not usually activated on an IIS server. The HARM is usually rated MEDIUM because it is unlikely valuable data will be NFS mounted or that an ID compromised would be a special account.

THREAT B-10: A user accidentally deletes or corrupts data or software in performing their job responsibilities.

RATIONALE: The RISK is usually rated LOW because the amount of damage an individual user can actually do to IIS data is usually fairly limited. The HARM is usually rated LOW because it should be possible to restore most files from a system backup.

THREAT B-11: A user with System Administrator responsibilities accidentally deletes or corrupts data or software in performing their job responsibilities.

RATIONALE: The RISK is usually rated MEDIUM because it is likely that *some*

errors will be made at some point in maintaining or deleting files. The HARM is usually rated HIGH because deleted files could impact the Project while waiting for it to be restored or rebuilt or if it couldn't be rebuilt.

THREAT B-12 A Production Control employee accidentally deletes or corrupts data or software in performing their job responsibilities.

RATIONALE: The RISK is usually rated MEDIUM because it is likely that *some* errors will be made at some point in maintaining or deleting files. The HARM is usually rated HIGH because deleted files could impact the Project while waiting for it to be restored or rebuilt or if it couldn't be rebuilt.

THREAT B-13: A data base administrator)/system administrator accidentally deletes or corrupts data or software in performing their job responsibilities.

RATIONALE: The RISK is usually rated MEDIUM because it is likely that errors will be made in maintaining or deleting files. The HARM was rated HIGH because deleted files could impact the Project while waiting for it to be restored or rebuilt or if it couldn't be rebuilt.

THREAT B-14: A virus is accidentally placed on the system by someone performing their job responsibilities.

RATIONALE: The RISK is usually rated LOW because server viruses are rare in most multi-user operating systems, and the ability to introduce them to the environment is limited (no floppy disks used, FTP is limited). The HARM is usually rated LOW because most viruses are not written to destroy data, and it is unlikely that the virus would do more than cause a minimal outage.

THREAT B-15: The server is destroyed or incapacitated by riots, flood, burst pipes, fire, power failure/surge, etc.

RATIONALE: The RISK is usually rated as MEDIUM because experience shows that problems such as leaking pipes and power failures are not exceedingly rare. The HARM is usually rated as HIGH because many services rely heavily on a few key servers.

C. NETWORK THREATS

THREAT C-1: Someone spoofs network addresses to gain access to servers, and uses that access to read/alter data or set up future access. Network spoofing involves someone having their host computer "impersonate" a trusted computer, thereby improperly gaining special permissions that only the trusted computer should have.

RATIONALE: RISK is usually rated LOW because it data, when stored in a

commercial RDBMS, is not easily interpreted. HARM is usually rated HIGH since if the data were acquired and disseminated, it could pose a serious legal threat or harm to the Project.

THREAT C-2: Someone uses a packet sniffing tool (a software package which allows a computer connected to the network to view data intended for another host computer) to read sensitive medical data being transmitted over the network.

RATIONALE: The RISK is usually rated only MEDIUM because even in the most promiscuous of networks, the difficulty of interpreting data as it travels the network mitigated the likelihood that someone would attempt this. The HARM is usually rated HIGH because of the legal ramifications of disclosing sensitive data.

THREAT C-3: Someone uses a packet sniffing tool to capture accounts and passwords to gain access to host systems containing sensitive medical data.

RATIONALE: The RISK is usually rated HIGH because the Computer Emergency Response Team reported in the Spring of 1994 that there was a high incidence of such attacks on networks, and that the accounts compromised numbered between the tens of thousands and hundreds of thousands. It is significantly easier to "sniff" for account access information than for actual transactions. The HARM is usually rated HIGH because of the extensive harm that someone could do by gaining access to numerous users' or system administrators' accounts.

THREAT C-4: Intentional denial of network service. Denial of network service is defined as interference with the availability of any part of the network or its services. This threat considers denial of service only by logical means through the network (for example by flooding a network with messages). Physical denial of service attacks (physical harm to network infrastructure) are considered separately in Threat C-8.

RATIONALE: The RISK is usually rated LOW because it is thought to be relatively unlikely that anyone could intentionally deny widespread network services through logical means. The HARM is usually rated as HIGH because it was thought that if anyone could actually inflict a widespread network outage, many services on a functioning network.

THREAT C-5: Break-in through the dial-up modem pool. This threat considers the possibility of an intruder somehow gaining unauthorized access to the network by coming in through the dial-in modem pool. This might be accomplished by guessing a Network Authentication System ID and password, by an authorized user sharing his or her network password, or by an authorized user writing down his or her network password and having it disclosed.

RATIONALE: The RISK is usually rated as MEDIUM because it is often common for account holders to share their password. The HARM is usually rated as LOW since further access to network-connected hosts is required before actual harm can be

inflicted.

THREAT C-6: Unauthorized access through an insecure modem pool. It is possible that there may be modems or modem pools providing network access without requiring a password.

RATIONALE: The RISK is usually rated as LOW because if there any such unauthenticated modems, it is not likely that their use is widespread, or widely known. The HARM is usually rated as LOW because further access to network-connected hosts is required before actual harm can be inflicted.

THREAT C-7: Accidental denial of network service. This threat considers a denial of service only by logical means (e.g. incorrect configuration of network components.). Denial of service by physical means is considered in threat C-8.

RATIONALE: The RISK is usually rated as MEDIUM because experience has indicated that network outages can sometimes be caused by such errors. The HARM is usually rated as LOW again because experience has indicated that generally such outages are brief in duration, and easily remedied.

THREAT C-8: Accidental or intentional denial of network service by physical means (e.g. riots, flood, burst pipes, fire, power outages,etc.).

RATIONALE: The RISK is usually rated as MEDIUM because experience shows that problems such as leaking pipes and power failures are not exceedingly rare. The HARM is usually rated as HIGH because a Project usually relies heavily on a functioning network.

Summary of Important Threats with Possible Solutions

Once the most serious threats are identified in the analysis above, some possible solutions are developed to mitigate these threats wherever possible. Here is a typical set of serious threats and possible solutions developed for one State IIS project deployed in a client/server architecture:

1. **Data in inappropriately disclosed or altered based on access to the IIS software** (Threats A-1 and A-2): Inappropriate access to a "live" IIS client inherently brings potential for disclosure or alteration of data.

Solutions: Develop an information security policy that addresses these concerns, and includes descriptions of appropriate behavior and sanctions for inappropriate behavior.

Develop the IIS application security with security profiles to only allow a given user to access and/or modify data appropriate to his or her role in the organization.

Promote awareness and good behavior to reduce the occurrence of IIS applications being left unattended in clinical settings.

2. **An important local file is deleted** (Threat A-5): Since client/server systems, especially those deployed over wide-area networks, will require some software to be located on the client desktop computer, there is reasonable risk that critical files could be lost or damaged at the provider site. Desktop computers at provider sites are the *least* controlled part of a client/server architecture.

Solutions: Develop an information security policy that requires regular data backups and compliance to participate in the Project.

Purchase and install software (or hardware) to secure Project files on provider site desktops.

Encourage sites to install Project software on local file servers which are likely better maintained and backed-up than individual desktops.

3. . **Attack on the server via the Internet** (Threats B-1 and B-2): Servers on the Internet are an attractive target for some individuals whose goal it is to read or alter data inappropriately or find a undetected location from which to perpetrate other exploits.

Solutions: Restrict the number of network services that are co-existing with the database server as much as possible.

Install the most secure version of the basic operating system as possible, and keep all security patches up-to-date. Specifically, use "secure" versions of operating systems (including shadow password files), one-time passwords (via smart card

[e.g., SecureID] or software [e.g., S/Key or Kerberos])

Install utilities that require frequent password changes, that enforce rules against easily-guessable passwords, and that scan the system for easily-guessable passwords.

Restrict access to the database server from certain network locations (either by inclusion or exclusion).

Deploy a network firewall to best protect the server from attack.

4. **Inadequate System Administration** (Threats B-11, B-12, and B-13): Multi-user operating systems and commercial RDBMS software packages are difficult products to learn, master, and properly maintain. Unless real careful, data can be corrupted or possible inappropriately disclosed due to administrator or operator error or ignorance.

Solutions: Invest in necessary training for all systems staff.

Be sure necessary staff are cross-trained to provide sufficient backup for critical skills.

5. **Physical threats to server or network** (Threats B-15 and C-8): Environmental threats are always a concern, especially in a wide-area implementation with a diverse set if sites.

Solutions: Locate server in a secure machine room.

Provide upgraded environmental conditions wherever the server is located, including uninterrupted power supply, redundant network connections, and redundant systems in different locations.

Implement a proper backup procedure, including off-site storage of backup media, to facilitate recovery from a catastrophic failure or accident.

6. **Promiscuous monitoring of network traffic** (Threats C-2 and C-3): Unscrupulous individuals may choose to monitor network traffic with the hopes of either capturing usernames and passwords to be used to attack systems, or to capture sensitive medical data inappropriately.

Solutions: Encrypt all data as it passes across the network.

Restrict database access from the public Internet by providing connectivity between the server and clients *behind* a firewall.

Recommendations

The set of possible solutions needs to be examined and analyzed. A set of specific recommendations then need to be made based on the technical, political, and financial constraints of the Project.

Here is a typical set of serious threats and possible solutions developed for one State IIS project deployed in a client/server architecture based on the possible solutions the Project developed above:

Policy: Develop an information security policy that delineates the roles and responsibilities of the Project staff and participants with respect to the IIS and its data. Include appropriate procedures to ensure local site data and software is properly managed.

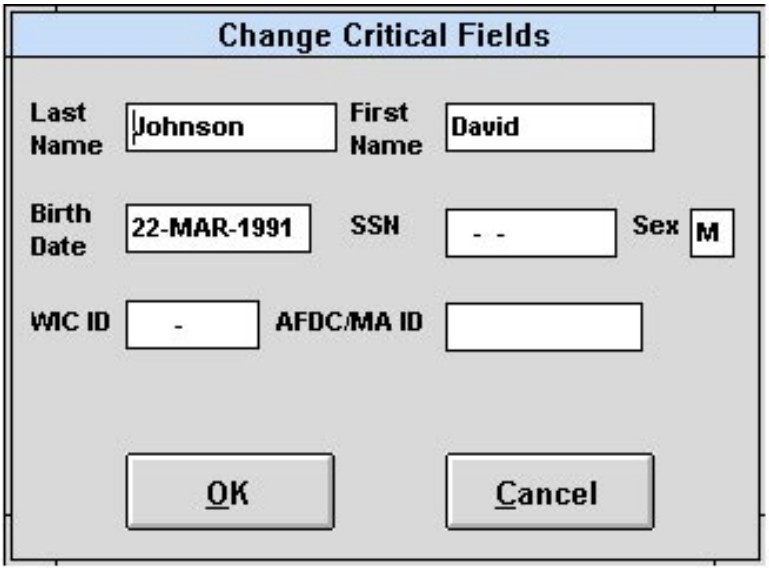
Create Security Levels for Applications: At least three security levels should be created:

- *General Reader:* Can view data on children but cannot add or modify data; limited access to standard reports; no access to outreach processes.

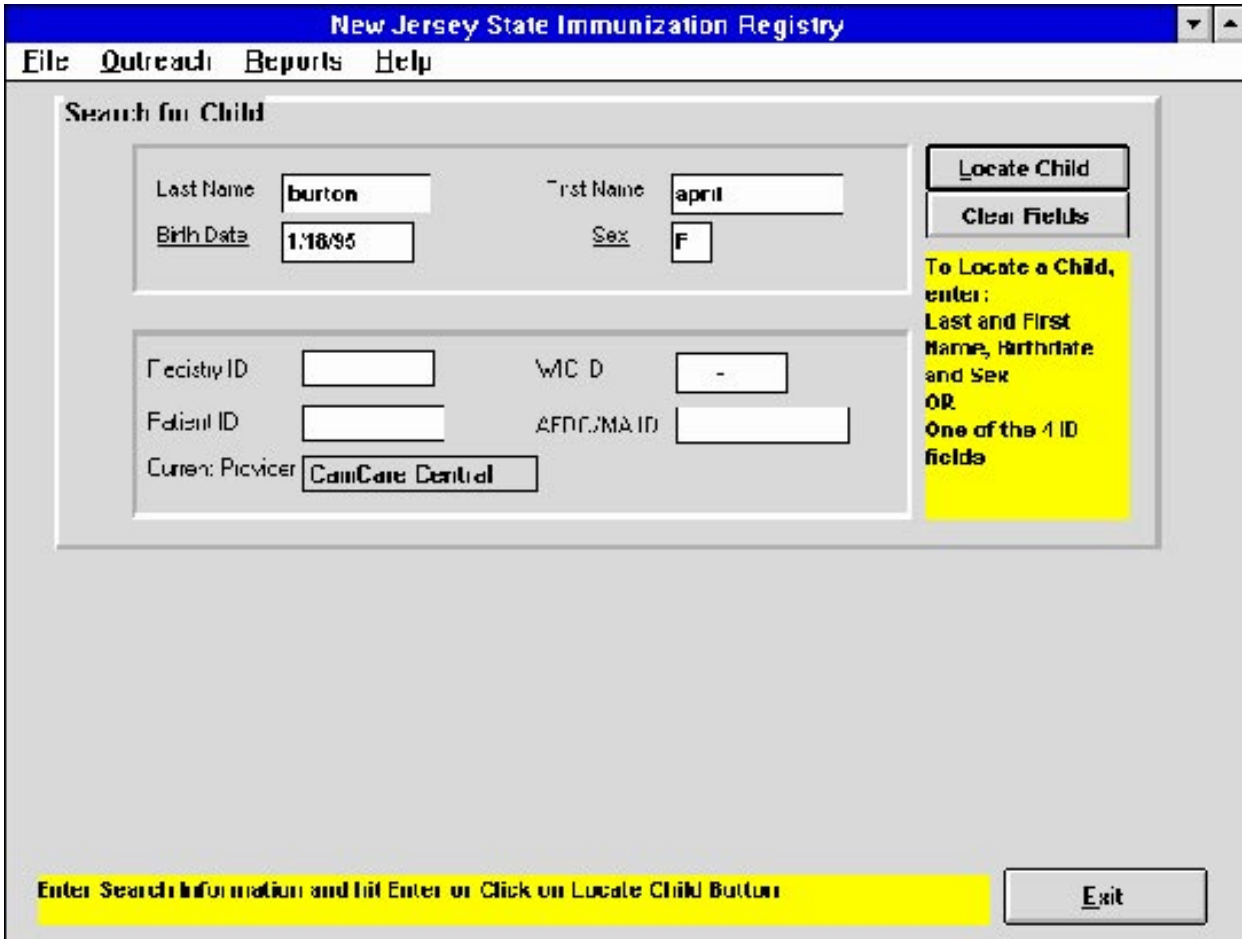
- *General User:* Can view and modify data on children *except* for "critical fields"; cannot add new children; limited access to standard reports and outreach processes.

- *Site Manager:* Can view and modify all data on children, including "critical fields"; can add children; full access to all standard reports and outreach processes.

  In this example, "critical fields" are defined as those fields required to establish the uniqueness of a record in the IIS. An IIS application might have a restricted screen or panel for addition/update of these fields:



Similarly, a look-up screen for an IIS record might restrict simple, free browsing to ensure confidentiality of records:



Note that on this application screen, a user must know specific information about the record being requested, and will not be shown any identifying information by the application that the user did not provide once a record is found.

Harden Server Against Network Attack: Several steps can be taken to harden the server against attack from the Internet:

- Keep operating system version current with all necessary security patches
- Install the "trusted" version of the operating system on the database server
- Remove any unnecessary services
- Implement frequent password aging and enforce non-guessable passwords
- Deny file transfer access to all accounts that do not require it
- Frequently audit system for security exposures
- Audit system services and access, and review audit logs for questionable events
- Purchase SQL<>Secure to provide user-changeable database passwords
- Purchase one-time password generator and smart cards for Project staff who require terminal-to-host connections for administrative functions.

Train Staff Appropriately: Appropriate systems and operations training needs to be provided for staff, including backup personnel. Consulting assistance needs to be provided when necessary.

Physically Secure the Server: The database server should be kept in a locked facility, alarmed whenever left unattended. Uninterrupted power should be provided. Data backups (including off-site storage of backup media) should be in place and functioning. Restoration from backups should be periodically tested.

Prevent Promiscuous Access to Data: Implement products to encrypt the full client/server data stream to prevent even accidental disclosure of data by promiscuous capture on the network.

Summary and Conclusions

Information security is a serious topic, and requires serious consideration at all stages of a Project's planning and implementation. The structured methodology described in this paper is not the only approach, but it does try to balance the need for a secure system with the realities of Project pressures and cost.

Health Information Risk Assessment and Management

Toolkit Section 4.5

Christopher J. Alberts
Sandra G. Behrens
William R. Wilson
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

The medical community has always relied on careful risk analysis for important decisions. When deciding whether or not to perform a complex procedure, physicians consider the tradeoffs, or impact, to the asset dependent upon that decision – in other words, the risk to a patient's morbidity, mortality, or general quality of life. Decisions about whether to expand the number of patient beds or to purchase a large piece of diagnostic equipment involves an analysis of the cost of that decision in relation to payoff, such as increased patient diagnostic capability, ability to attract specialists in a key medical research discipline, or likelihood of liability if a diagnostic procedure is not performed.

Today, virtually all information is captured, stored, and accessed in digital form. From patient records to personnel data, formulary inventory to national epidemiological databases, we rely on digital data that is accessible, dependable, and protected from misuse.

Risk to information security has become an even greater concern as networked computing has become more widespread in the medical community. For example, in a case reported by New Scotland Yard several years ago, an intruder broke into a medical facility and changed the test results on cancer biopsies from negative to positive, so several women thought they had cancer when they did not. Another case involved an intruder who changed data in a CAT scan. Scans had been done that were to be used for eye surgery, and the surgery had to be postponed until the system was rebuilt. In the U.S. there have been reports of hospitals being penetrated and the blood types in patient records being changed, which could be fatal if not detected.

What is needed is an approach to risk that enables medical organizations to systematically identify risks to information, prioritize those risks, and take appropriate steps to manage them.

1.0 Using Risk Evaluations in Risk Management

Risk is the possibility of suffering harm or loss. It is the potential for realization of unwanted negative consequences of an event [Rowe88]. It refers to a situation where a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in an impact or consequence.

The first step in managing risk is to understand what your risks are in relation to your organization's mission and its key assets. A comprehensive risk evaluation or assessment can help identify many of the risks. Once they are identified, personnel can put together plans to reduce the risks that are likely to have the highest impact on the organization's assets. The ongoing process of identifying risks and implementing plans to address them is risk management.

An effective enterprise-wide evaluation of information security risk comprises the following [Alberts99]:

- organizational evaluation – examines key areas of expertise within the organization to identify important information assets, the threats to those assets, the security requirements of the assets, what the organization is currently doing to protect its information assets (current protection strategy), and weaknesses in organizational policies and practice (organizational vulnerabilities)
- information infrastructure evaluation – examines the key operational components of the information infrastructure (technology and physical facilities) for weaknesses that can lead to unauthorized action (technology vulnerabilities)
- risk analysis – analyzes the information generated by the organizational and information infrastructure evaluations to identify risks to the enterprise, to prioritize the list of risks based on their impact to the organization's mission, and to develop a protection strategy for addressing the highest priority risks

In the next three sections, we will elaborate on these three components of information risk evaluations.

2.0 Organizational Evaluation

An enterprise consists of an organization and its information infrastructure. This can be as complex as an entire hospital or as focused as a physician's practice. The organization as used here refers to how the people are organized to achieve the mission of the enterprise. The organization includes both the mission-related and support functions. It basically consists of people performing tasks that help to meet the mission of the organization. Many of these tasks involve the security of information.

As part of their job responsibilities, all staff members should perform certain actions with respect to security; these actions are known as security practices. When people take inappropriate action or fail to take correct action, they can introduce weaknesses into the information infrastructure and expose critical information assets to adversaries and threats. Different job responsibilities within an enterprise require different types of security practices. We will discuss security practices in more detail later.

In a risk evaluation, the people in the organization must provide important pieces of information. The knowledge they have is used to identify the following information:

- the important information assets
- the threats to those assets
- the security requirements of the assets with respect to confidentiality, integrity, and availability
- what the organization is currently doing to protect its information assets (current protection strategy)
- weaknesses in organizational policies and practice (organizational vulnerabilities)

A comprehensive evaluation must include people from different departments within the organization as well as multiple organizational levels (from the staff level through senior management) [GAO99]. Thus, it must have both horizontal and vertical coverage of organizational responsibilities.

The remainder of this section will discuss the information that must be elicited from the people in an organization, beginning with assets.

Assets

An asset is something of value to the enterprise [Hutt95]. In general, information technology assets are the combination of logical and physical assets that can be grouped into the following classes[1]:

- information – documented (paper or electronic) information or intellectual assets used to meet the mission of the enterprise
- software – software applications (operating systems, database applications, networking software, office applications, custom applications, etc.)
- hardware – information technology physical devices (workstations, servers, etc.)
- people – the individuals in the enterprise, including their skills, training, knowledge, and experience

Note that the above list is an example of asset classification. Such lists are contextual for any enterprise and must be defined in order to conduct a meaningful evaluation [Fites89]. In general, asset classifications should

- be as complete as necessary
- be an appropriate length (not too long)
- contain no duplication

[1] This list was created using information in these references: [Fites89], [BSI95], [Hutt95], and [Caelli91].

Security Requirements and Outcomes

Security requirements outline the qualities of information assets that are important to an organization. Typical security requirements that organizations need to consider are

- confidentiality – the need to keep proprietary, sensitive, or personal information private and inaccessible to anyone who is not authorized to see it
- integrity – the authenticity, accuracy, and completeness of an asset
- availability – when or how often an asset must be present or ready for use

When the security requirements of an asset are violated, certain outcomes are possible (outcomes are directly related to security requirements in the table below). The following list defines typical outcomes[2].

- disclosure – the viewing of confidential or proprietary information by someone who should not see the information
- modification – an unauthorized changing of an asset
- destruction – the removal of an asset from existence; the asset cannot be recovered
- loss – the limiting of an asset's availability; the asset still exists but is temporarily unavailable
- interruption – the limiting of an asset's availability; interruption refers mainly to services

Relationship of Security Requirements to Outcomes	
Security Requirement	**Outcome**
confidentiality	• disclosure of asset
availability	• modification of asset
integrity	• destruction of asset • loss of asset • interruption of asset

[2] This list was created using these references: [Fites89], [BSI95], [Hutt95], and [Caelli91].

Asset Valuation

Asset values are based on the impact to the organization if the asset is lost. For some tangible assets, standard accounting procedures or replacement costs can be used. Acquired value for intangible assets can be estimated based on the loss to the enterprise [Hutt95].

The traditional measure of an asset is in terms of dollars. Reducing all assets to dollars makes for an easy comparison, and people are often comfortable thinking in terms of dollar values for assets. It can be very difficult, however, to reduce some intangible assets to dollar values. The cost of estimating statistically can be high in some cases, and statistical estimates may depend on subjective assumptions. Historical data, if available, can be useful in estimating the value of assets. In many cases relative rankings of asset values are sufficient [Fites89]. Often, orders of magnitude of values are used.

One way to estimate the value of assets is to consider what would happen if their security requirements were violated. Let's consider an example in which a medical center wants to protect its patient records. Staff are concerned about the possibility of disclosing the patient records because this would violate the security requirement that sensitive information must remain confidential. If the information is disclosed to an unauthorized party, the fact that the information is no longer confidential has an impact on the organization. If the impact affects private medical diagnostic results or treatment plans, the value of the asset would be extremely high. On the other hand, disclosure of staffing assignments for nursing shifts, for example, might not have a serious impact on operations, so the asset value would be low.

Threats

A threat is an indication of a potential undesirable event [NSTISSC98]. It refers to a situation in which a person could do something undesirable (a hacker initiating a denial-of-service attack against a hospital's email server) or a natural occurrence could cause an undesirable outcome (a fire damaging a hospital's information technology hardware). Threats consist of the following properties:

- asset – something of value to the enterprise
- actor – who or what may violate the security requirements (confidentiality, integrity, availability) of an asset
- motive (or objective) – defines whether the actor's intentions are deliberate or accidental
- access – how the asset will be accessed by the actor (network access, physical access)
- outcome – the immediate outcome (disclosure, modification, destruction, loss, interruption) of violating the security requirements of an asset

Threat Actors

There are several types of actors with respect to threat. Below is a typical classification of threat actors[3].

- non-malicious employees – actors within the enterprise who accidentally abuse or misuse computer systems and their information
- disgruntled employees – actors within the enterprise who deliberately abuse or misuse computer systems and their information
- hackers – actors who attack computer systems for challenge, status, or thrill
- spies – actors who attack computer systems for political gain
- terrorists – actors who attack computer systems to cause fear for political gain
- competitors – actors who attack computer systems for economic gain
- criminals – actors who attack computer systems for personal financial gain
- vandals – actors who attack computer systems to cause damage
- environment – natural disasters that can affect computer systems and their information

In general, actors that are non-environmental in nature can be grouped as people inside the organization or outside the organization. The categories of inside, outside, and environment are the most basic categories for threat actors.

Note that the above list is one example of threat actor classification. As with asset classification, threat actors are contextual and, therefore, need to be defined in order to have an effective evaluation [Fites89]. In general, threat actor classifications should

- be as complete as necessary
- be an appropriate length (not too long)
- contain no duplication

Security Practices

Security practices are actions that help initiate, implement, and maintain security within an enterprise [BSI95]. A specific practice is normally focused on a specific audience. The audiences for practices include managers, users (general staff), and information technology staff.

Practices focus on organizational and technological issues. Organizational issues include policy, business continuity planning, management sponsorship, and training and awareness. The

---

[3] This list was created using these references: [Howard98], [Parker98], and [Hutt95].

technology practices include system and network management, authentication and authorization, monitoring and auditing, and encryption.

Because practices focus on actions that enhance security, they have a major role in evaluations. Organizations can be evaluated against known good practices. This identifies activities currently in place that protect their assets. Also identified are missing practices, which can be indications of organizational vulnerabilities. Organizational vulnerabilities are weaknesses in organizational policy or practice that can result in unauthorized actions occurring.

Note that technology vulnerabilities also exist. They are weaknesses in systems that can directly lead to unauthorized action [NSTISSC98]. In many cases, poor organizational practices can lead to the existence of technology vulnerabilities. We will discuss technology vulnerabilities more thoroughly later.

Practice Categories

Security practices can be grouped around certain themes, called practice categories. There are two basic types of practices – organizational or management practices and technology practices. The following lists describe organizational and technology practice categories[4].

Organizational (management) practice categories

- general management – areas on which managers focus to enable information security activities in their organizations
- policy – the organizational and management direction for information security
- security program management/security organization – how information security is implemented and managed within an organization
- user issues – security practices employed by the organization to enable system users to effectively and securely perform their job duties
- physical security – the physical access to information technology assets and the methods employed for retiring or disposing those assets
- contingency planning/disaster recovery – plans (their existence and effectiveness) to counteract disruptions in business activities and in systems and networks

Technology practice categories

- incident management – standard procedures for handling security incidents

[4] This list is based on previous work at the Software Engineering Institute and on information from these references: [BSI95] and [Swanson96].

- system and network management – security practices to enable secure operation of systems and networks
- authentication and authorization – mechanisms for verifying users to systems and controlling access to networks, systems, and applications
- monitoring and auditing – techniques and methods employed by an organization to identify, understand, and control issues relating to the security of systems and networks, according to security policies and standards
- encryption – security practices for using encryption to protect an enterprise's information

Evaluating Security Practice

One way of evaluating the security practice of an enterprise is to understand how the staff behaves in relation to known security practices. The result will be the identification of known enterprise practices and missing practices. The known practices form the current protection strategy for the enterprise.

When the information security risks have been identified, organizations develop a revised protection strategy to address the highest priority risks to the organization [Alberts99]. The revised protection strategy will include a plan for deploying many of the practices that were found to be missing, as well as continuing to perform the practices that are being used effectively. Developing protection strategies based on enterprise risk will be discussed in more detail later.

Performing an Organizational Evaluation

Recall that an organizational evaluation examines key areas of the staff's expertise. In essence, this part of the risk evaluation focuses on mining the knowledge of the people in the enterprise; the organizational evaluation identifies the following important pieces of information:

- the important information assets
- the threats to those assets
- the security requirements of the assets with respect to confidentiality, integrity, and availability
- the current protection strategy
- organizational vulnerabilities

Also recall that a comprehensive evaluation of an organization must include people from different departments within the organization as well as multiple organizational levels (from the

staff level through senior management level). In the remainder of this section we will highlight the basic activities required in an organizational evaluation.

1. **Identify areas of concern** – Construct plausible scenarios outlining concerns about the threats to important information assets. These areas of concern are likely to lack sufficient detail with respect to the components of threat, and they must be further examined in the next step.
2. **Identify threats** – Extract key information about the components of each threat (assets, actor, motive, access, outcome) from the previously identified areas of concern. This provides more detail about the concerns of the staff than was elicited in the previous step. It also provides sufficient detail for later analysis of threat and risk.
3. **Review organizational practices** – Evaluate the staff's security practices in relation to known good security practices. The results of this evaluation will identify the current protection strategy of the enterprise as well as organizational vulnerabilities.
4. **Determine important information assets and values** – Examine information assets to determine which are most important to the enterprise, and estimate their value. The important assets are carried forward in the risk evaluation; unimportant assets are not carried forward.
5. **Construct an enterprise-wide threat profile (integrate results from each enterprise level)** – Create an integrated view of the important information assets, the threats to those assets, the security requirements of the assets, the current protection strategy of the enterprise, and organizational vulnerabilities. This view is created by consolidating the perspectives elicited from the different organizational levels.
6. **Develop security requirements for each important asset** – Create and document the requirements for each important asset with respect to its confidentiality, integrity, and availability.

In the next section, we look at how the information infrastructure is examined for vulnerabilities.

3.0 Information Infrastructure Evaluation

The information infrastructure evaluation builds on the results of the organizational evaluation. The high-priority information assets identified previously are first mapped to the information infrastructure components (considering both the physical environment and the networked information technology environment). This mapping results in the identification of the high-priority components of the infrastructure. A technology vulnerability assessment is then performed on all (or a representative set) of the high-priority components.

In this paper, we will not elaborate on the physical environment part of the evaluation; rather, we will concentrate on the information technology part.

Vulnerability

In order to access an information asset to effect a desired outcome, a threat must take advantage of a vulnerability. A vulnerability is a weakness in an information system, system security practices and procedures, administrative controls, internal controls, implementation, or physical layout that could be exploited by a threat to gain unauthorized access to information or disrupt processing.

An information infrastructure evaluation targets vulnerabilities located in the technology base of the enterprise. Technology vulnerabilities are present in and apply to network services, architecture, operating systems, and applications. Technology vulnerabilities are often grouped into three categories [Howard98]:

1. design vulnerabilities – a vulnerability inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a vulnerability
2. implementation vulnerabilities – a vulnerability resulting from an error made in the software or hardware implementation of a satisfactory design
3. configuration vulnerabilities – a vulnerability resulting from an error in the configuration and administration of a system or component

In addition, the technology vulnerability evaluation identifies technical vulnerabilities that can be used to refine the picture of organizational vulnerabilities. A vulnerability can result from a user's lack of awareness regarding information security policy and practice, deliberate avoidance or circumventing of existing policy and practice, insufficient training and readiness to address information security vulnerabilities, misplaced or inappropriate trust, etc. For example, staff members may say that they perform a practice, but the technical vulnerability evaluation might show evidence to the contrary.

Vulnerability Assessment

A vulnerability assessment is a systematic examination of the information infrastructure to determine the adequacy of an organization's security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of security measures after implementation [NSTISSC98].

Vulnerability assessments test the information infrastructure components for potential weaknesses. The assessments often include attempts to imitate and use the methods and tools a threat actor would use to gain unauthorized access to an information asset. Vulnerability assessment tools (including tools for file integrity checking, virus scanning, password protection,

system scanning, network scanning, and network mapping) are used to interrogate components of the information infrastructure. The vulnerability assessment attempts to identify and evaluate the configuration and strength of devices on the enterprise network(s). Example concerns and checks include

- review of firewall configuration
- security of public web servers
- comprehensive review of all operating systems
- inventory of services running and/or available
- listing of all system user accounts
- known vulnerabilities in routers, switches, remote access servers, operating systems, and specific services and applications
- configuration errors
- existing signs of intrusion (Trojan horses, backdoor programs, integrity checks of critical system files, etc.)
- file ownership and permissions
- password usage and strength

Performing an Information Infrastructure Evaluation

The infrastructure evaluation identifies the following pieces of important information:

- the high-priority information infrastructure components
- known design, implementation, and configuration vulnerabilities present in one or more high-priority infrastructure components that could provide access to important information assets
- refinement of the organizational view created by the organizational evaluation

The following basic activities are required in an information infrastructure evaluation:

1. **Identify the configuration of the information infrastructure** – Capture the present state of the computing and physical infrastructures by using documented artifacts, the knowledge of the information technology staff, and network mapping tools.
2. **Identify the high-priority infrastructure components** – Map the important information assets identified during the organizational evaluation to the information infrastructure. An examination of the information asset locations will determine

which components are critical to the enterprise. The technology vulnerability assessment will be focused on these high-priority components.

3. **Refine the scope of the evaluation** – Refine the scope of the evaluation considering access paths to and data flows for important assets in both the physical and network environments.
4. **Examine the information infrastructure for vulnerabilities** – Perform a vulnerability assessment, supported by network and software tools, to identify technology vulnerabilities. The security posture of the networked environment should be assessed from three perspectives: outside the enterprise, inside the enterprise, and from individual systems within the enterprise.

Exploitable vulnerabilities exist in many components of an organization's information infrastructure, and the volume of known vulnerabilities can overwhelm an organization's capacity to implement corrective action. As a result, scarce resources are often devoted to highly visible but relatively low-impact vulnerabilities. In addition, poor organizational practice can lead to the reappearance of technology vulnerabilities. Therefore, organizations should remember to emphasize the mitigation of vulnerabilities posing the greatest risk and to reflect these decisions in a revised protection strategy. Identified vulnerabilities must also be placed in the context of the organizational evaluation results. This occurs during risk analysis, which is described in the next section.

4. 0 Risk Analysis

Armed with the results of the organizational evaluation and the information infrastructure vulnerability assessment, an organization is positioned to understand the information security risks to the enterprise. Once the risks have been identified, they must be prioritized based on probability (the likelihood that a given threat will exploit a vulnerability to gain access to an information asset) and impact (the consequence and outcome of the threat's actions) to gauge the impact to the enterprise's mission. Risk analysis helps establish a relative priority for the actions necessary to improve or maintain the level of information security by evaluating, classifying, and prioritizing risks.

Actionable Risks

At its core, a risk describes how an adversary or threat can violate the security requirements of an information asset, resulting in a negative impact on the organization. A risk consists of an impact along with the threat properties noted in the "Threats" section under "2.0 Organizational Evaluation."

Briefly, the threat properties are **asset, actor, motive, access, and outcome. Impact,** then, is the loss to the organization that would result from a successful attack by the identified threat.

The information gathered in the earlier steps should be formed into statements of risk that make explicit statements about threat properties. An individual statement of risk can be generated for every condition in which there is a likelihood that a unique threat actor may attempt to compromise a unique asset resulting in a specific outcome. After the risks have been identified, they must be analyzed as a group to determine which risks should be addressed, when the risks should be addressed, and in what sequence they should be addressed.

Analyzing Information Security Risks

Risk analysis involves the following activities:

1. **Evaluate the risks** – Assign values to the risk attributes (likelihood of threat, impact to the organization) for each identified risk. The first step in risk evaluation is the selection of a measurement scale. Choose a scale that best matches the accuracy and precision required (and possible) for evaluation. Risk evaluation can be either qualitative or quantitative in nature. Qualitative information requires a nominal or ordinal scale. Quantitative information requires a cardinal or ratio scale. [Charette89]
2. **Prioritize the risks** – Rank the evaluated risks by their effect on the organization (by examining the product of the probability of occurrence and the impact to the organization, represented qualitatively or quantitatively).
3. **Categorize the risks** – Classify the risks into themes, based on the common characteristics of the risks. Risks may be classified by their properties (threat, asset, infrastructure component, outcome, impact to the organization, etc.). It is more effective and efficient to address risk themes than it is to address each risk individually. In another activity, a protection strategy (with its associated countermeasures and safeguards) will be developed to address the risk themes.
4. **Determine interrelationships among themes** – Identify the cause-and-effect relationships among the identified risk themes. This activity helps to increase the understanding of a set of risks and to determine interrelationships and dependencies to consider when developing protection strategies later.
5. **Prioritize the resulting themes and risks** – Rank the risk themes based on a review of the interrelationships among themes as well as the location of the highest priority individual risks within the themes. In a later activity, candidate mitigation approaches will be investigated for the high-priority risk themes.

After the risk analysis has been completed, the goal is to reduce the risk to the enterprise by using a combination of these objectives:

- implementing new security practices within the organization (adding practices that were found to be missing)

- taking the actions necessary to maintain the existing security practices
- fixing identified vulnerabilities

Protection Strategy

An information security risk evaluation helps an organization determine where it is positioned in terms of protecting its information assets. The development of a protection strategy helps the organization define approaches to satisfying its security requirements. A protection strategy leads to a series of steps that an organization can take to raise or maintain the existing level of security. The objective of a protection strategy is to provide a direction for future information security efforts rather than to find an immediate solution to every security vulnerability and concern [Dempsey97].

Information security affects the entire organization. It is ultimately a business problem whose solution involves more than the deployment of information technology. An organization must take a strategic view to address their information security risks. The following list describes the recommended components of an effective protection strategy.

Protection strategy components

- principles – the collection of corporate values and beliefs that defines the information security philosophy under which policies and practices may be developed
- policies – the set of laws, rules, objectives, and instructions that regulate how an organization manages, protects, and distributes important information assets; security policies provide a framework that is essential in a networked environment to ensure the enterprise's important information assets are secured with a governing policy
- standards – mandatory control objectives, descriptions, and implementation principles to be applied within the enterprise
- practices – organizational and technological actions that help initiate, implement, and maintain information security within an enterprise
- resources – personnel, budget, facilities, and technology available to the organization
- training and awareness – formal and informal communication programs, including comprehensive training, that encourage and ensure effective implementation of the protection strategy. Training should be kept current and should address the applicable principles, policies, standards, and practices.

Developing a Protection Strategy

These activities are required for developing a protection strategy:

1. **Define information security objectives** – Capture the requirements and objectives that the protection strategy is intended to satisfy.
2. **Identify candidate mitigation approaches** – Develop candidate approaches for mitigating the high-priority risks and themes by considering existing and missing policies and practices, threats, assets, vulnerabilities, and available technology.
3. **Assess alternative approaches** – After candidate mitigation approaches have been agreed upon, a search for potential solutions is conducted. Alternatives should be rated for their ability to address information security requirements, their ability to address information security risks, their applicability to the organization's existing information infrastructure, and the associated costs and impact to the organization.
4. **Recommend/select solutions and courses of action** – Recommendations can range from the purchase of technology products to the commission of a study in the area of policy development.
5. **Do it** – Implement and monitor elements of the protection strategy for effectiveness.

5.0 Summary

In today's medical environment, virtually all medical information is stored electronically. Because networked computing is so common in the medical community, legitimate users have greater access to information than ever before. Unfortunately, this also exposes the medical community to a variety of new threats that can have impact on the confidentiality, integrity, and availability of information. Organizations need a way to understand their information risks and to create new strategies for addressing those risks.

A systematic approach to assessing information security risks and developing an appropriate protection strategy is a major component of an effective information security program. By adopting such an approach, organizations can understand their current security posture and use it as a benchmark for improvement.

References

[Alberts99] Alberts, Christopher J.; Behrens, Sandra G.; Pethia, Richard D.; & Wilson, William R. *Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) Framework, Version 1.0* (CMU/SEI-99-TR-017). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 1999.

[BSI95] British Standard Institution. *Information Security Management, Part 1: Code of Practice for Information Security Management of Systems* (BS7799 : Part 1 : 1995). London, England: British Standard Institution, February 1995.

[Caelli91] Caelli, William; Longley, Dennis; & Shain, Michael. *Information Security Handbook*. New York, NY: Stockton Press. 1991.

[Charette89] Charette, Robert N. *Software Engineering Risk Analysis and Management*. New York: Intertext Publications/Multiscience Press, Inc., 1989.

[Demsey97] Dempsey, Rob & Bruce, Glen. *Security in Distributed Computing*. Upper Saddle River, NJ: Prentice-Hall, Inc., 1997.

[Fites89] Fites, Philip E.; Kratz, Martin P. J.; & Brebner, Alan F. *Control and Security of Computer Information Systems*. Rockville, MD: Computer Science Press, Inc. 1989.

[GAO99] United States General Accounting Office. *Information Security Risk Assessment, Practices of Leading Organizations* (GAO/AIMD-00-33). Washington, D.C.: GAO, November 1999.

[Howard98] Howard, John D. & Longstaff, Thomas A. *A Common Language for Computer Security Incidents* (SAND98-8667). Albuquerque, NM: Sandia National Laboratories, 1998.

[Hutt95] Hutt, Authur E.; Bosworth, Seymour; & Hoyt, Douglas B. *Computer Security Handbook, 3rd ed*. New York, NY: John Wiley & Sons, Inc. 1995.

[NSTISSC98] National Security Telecommunications and Information Systems Security Committee. *Index of National Security Telecommunications Information Systems Security Issuances* (NSTISSI No. 4014). Ft. Mead, MD: NSTISSC Secretariat, January 1998.

[Parker98] Parker, Donna B. *Fighting Computer Crime*. New York, NY: John Wiley & Sons, Inc. 1998.

[Rowe88] Rowe, William D. *An Anatomy of Risk*. Malibu, FL: Robert E. Crier, 1988.

[Swanson96] Swanson, Marianne & Guttman, Barbara. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. Washington, D.: National Institute of Standards and Technology, June 1996.

Risk Analysis of Electronic Renal Care Patient Management System

Project Phoenix - Protecting the Security and Confidentiality of Patient Information

Anya Kim*, Marion C. Meissner, Lance J. Hoffman*, Jeff Collmann**, Seong K. Mun****

*** Cyberspace Policy Institute, School of Engineering and Applied Science**
The George Washington University
Washington, DC 20052

**** ISIS Center, Radiology Department**
Georgetown University Medical Center
Washington, DC 20007

March 31, 1997

Table of Contents

1. INTRODUCTION 3

2. SYSTEM DESCRIPTION 3

2.1 PHYSICAL ENVIRONMENT 4
2.1.1 Dialysis Unit at Union Plaza 4
2.1.2 Nephrologist's office at GUMC 6
2.1.3 Nephrologist's Home 6
2.1.4 ISIS Center (Long-term Archive) 6
2.2 EQUIPMENT 7
2.2.1 Dialysis Telemedicine Unit 8
2.3 PROCEDURES 10
2.3.1 Dialysis - New Patient 10
2.3.2 Dialysis - Telemedicine Consultation 10
2.3.3 Archiving 11
2.3.4 Equipment maintenance 11
2.4 PERSONNEL 12
2.5 INTANGIBLES 13

3. RISK ANALYSIS 13

3.1 THREATS AND VULNERABILITIES 13
3.1.1 Data integrity 15
3.1.2 Availability 15
3.1.3 Confidentiality 16
3.2 EXPECTED LOSS ANALYSIS 17

4. RECOMMENDATIONS 18

4.1 POSSIBLE COUNTERMEASURES 18
4.2 EVALUATION OF COUNTERMEASURES 20
4.3 RECOMMENDATION OF COUNTERMEASURES 21

5. CONCLUSION 22

6. REFERENCES 24

7. ANNEXES 25

Annex A - Patient Care Forms
Annex B - Consent Forms, Patient Education
Annex C - Provider (TRC) Policies
Annex D - Floor Plans
Annex E - Dialysis Machine Maintenance
Annex F - Operations Manual

1. Introduction

This risk analysis is part of Georgetown University Medical Center's (GUMC) Project Phoenix: Scrutinizing a Telemedicine Testbed, a joint effort of the Imaging Science and Information Systems (ISIS) Center, Department of Radiology, and the Clinical Economics Research Unit (CERU), Department of Medicine, at GUMC. Project Phoenix sponsors evaluation studies on clinical economics and data security. The system analyzed in this document is a telemedicine-based kidney dialysis unit at Union Plaza in Washington, DC, and the other sites which comprise the telemedicine testbed. The unit is owned and managed by Total Renal Care, Inc. (TRC) in conjunction with GUMC. It serves as the test site for Project Phoenix, and represents the risks possible in an electronic Renal Care Patient Management (RCPM) network. Data from this analysis and from a previously conducted risk analysis of the paper-based control site at GUMC, will be used to test the hypothesis that electronic telemedicine systems, when managed according to established information security practices, provide increased access to and maintain the security of patient information, compared to paper-based medical records.

This risk analysis assesses the current level of information security and patient confidentiality achieved at the dialysis unit and the other sites which are part of the telemedicine system and proposes cost-effective measures to improve security. Section 2 describes the entire telemedicine system and the environment in which it operates. The risks and vulnerabilities of the telemedicine testbed are examined in Section 3. Section 4 proposes countermeasures to minimize the threats to the telemedicine system and evaluates them based on their cost-effectiveness and ability to protect against the identified security risks. Section 5 gives a conclusion of the risk analysis, Section 6 is a list of references, and Section 7 is the appendices.

2. System Description

This section describes the Georgetown University telemedicine kidney dialysis system. The telemedicine system spans several different locations: the dialysis treatment facility at Union Plaza, a nephrologist's office at Georgetown University Medical Center, the nephrologist's home in McLean, VA, and a long-term magnetic tape archive for patient data located at the ISIS Center, a research laboratory at GUMC. The analysis includes all these locations because telemedicine workstations or storage facilities reside in separate locations as they are used to access and manage patient records. To meet the requirements of the District of Columbia, the first patient was dialyzed at the Union Plaza location on December 1, 1996 and the dialysis unit opened officially on December 6. The District of Columbia gave its official permission for the unit to operate clinically on December 15, 1996.

The nephrologist makes weekly rounds in person as at the conventional paper-based control site, and also using the telemedicine system once per week. The telemedicine system allows the physician to make rounds from a remote location while providing the same service, such as patient-doctor conversations and emergency assistance, as before.

When the physician is making rounds or doing emergency consultations remotely, the telemedicine unit is wheeled to the patient, hooked up to the patient's kidney dialysis machine, and the patient's data is sent across a telecommunications link to the physician at a remote location.

2.1 Physical Environment

2.1.1 Dialysis Unit at Union Plaza

The GUMC/TRC telemedicine kidney dialysis unit is located in an office building in downtown Washington, DC, where all patient treatment occurs and all paper-based patient records for these patients are stored. The building is located one block away from the Union Station Metro station in a business district with many similar office buildings. The neighborhood is not very safe; the immediate surroundings contain many vacant buildings and vagrants, giving it an ominous atmosphere.

The entrance to the unit is at the side of the building, where there is no security guard on duty. The entrance is kept unlocked during regular operating hours, and locked at all other times. There is a video camera located outside the entrance of the unit that is operating only when the unit is closed, and an alarm system is installed at the entrance and is in use at all times. The lack of adequate physical security is demonstrated by the fact that shortly after the opening of the center two patient chairs were stolen from the unit. The hours of operation are from 6 a.m. to 8 p.m. Monday to Saturday. Only the nurse manager, the charge nurses, and the unit secretary have access to the keys to the main entrance. Besides the main entrance, there are three other entrances/exits from the unit (see Figure 1). One is the delivery entrance, another leads to the hall of the main entrance to the building, and the third entrance leads to a staircase internal to the building. These entrances are kept locked unless in use.

The dialysis unit consists of the treatment area, a reception area, the unit secretary's office, the head nurse's office, a conference room, and several rest rooms. Towards the rear of the unit are the nephrologist's office, several examination rooms, a storage room connected to the delivery entrance, maintenance rooms, and the staff lounge. The entire site is equipped with fire alarms and a water sprinkler system according to Washington, DC building code. Exits are marked with signs. Windows throughout the unit cannot be opened.

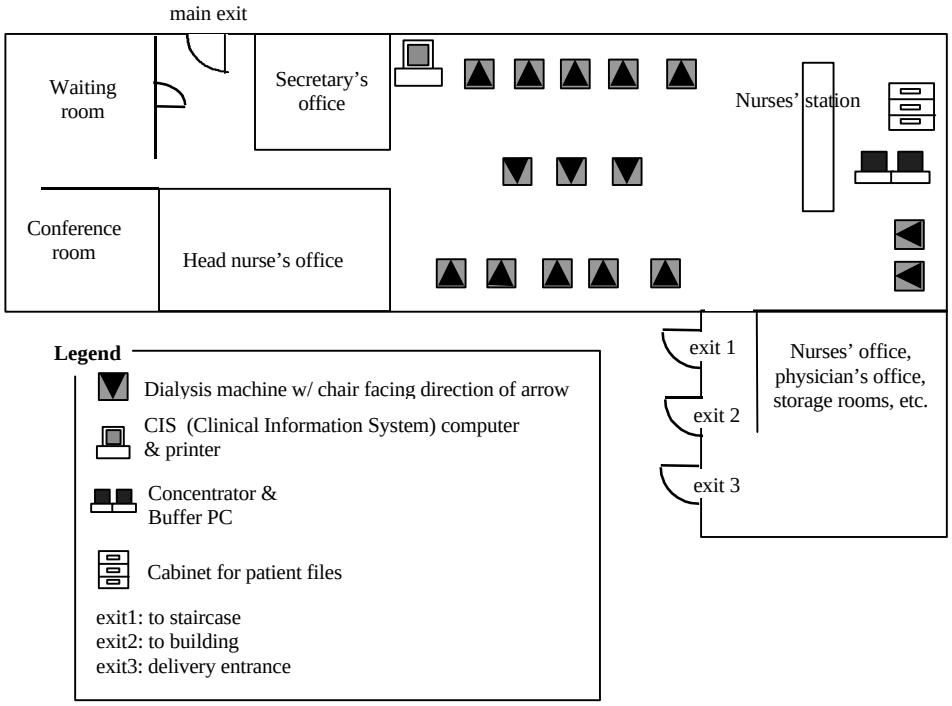


Figure 1. Layout of Dialysis Unit

In the treatment area, the dialysis machines are arranged in three rows, alternating with patient chairs. The first row has five dialysis machines and the second row has three. These two rows face each other. The third row has five dialysis machines and faces large windows to the outside. The glass is frosted to prevent passersby from seeing inside the unit. Although the large dialysis machines and the noises they make obscure patients' views and hearing, it is still possible to hold a conversation between adjacent patients, or overhear other patients' conversations. Because some of the patient chairs face each other, it is possible for patients to read the digital information shown on the dialysis machine of patients sitting across from them. To the back of the treatment area is a nurses' station. The arrangement of the dialysis machines makes it difficult for the nurses to overlook all the patients when situated at the nurses' station. Patient files are kept in a locked cabinet behind this station when they are not being used. Medications are also kept behind the desk in a locked refrigerator and cabinet. There are two separate dialysis machines and patient chairs in an alcove next to the nurses' station for patients requiring isolation.

The reception area is used by patients waiting to begin treatment. If a patient brings a friend or relative, this person usually waits in the reception area during the duration of the treatment.

The telemedicine equipment is stored during off hours in the rear of the dialysis unit, in a locked room next to the nephrologist's office. Only the physician has a key to this room. Once the telemedicine system is used on a regular basis, the nurse or other staff member

responsible for the telemedicine equipment will also have a key to this room. The telemedicine system is wheeled out to the treatment area during business hours.

2.1.2 Nephrologist's office at GUMC

The nephrologist’s office, one of the remote telemedicine sites, is located on the sixth floor of the Pasquerilla Health Care Center at Georgetown University Medical Center. To gain entrance to the hallway of the doctor’s office one must enter a door that is supposed to be kept locked at all times. During our visits there, we have always found this door to be unlocked allowing anyone to enter at will. The physician’s office is kept locked when he is away, but the secretary has a key.

The telemedicine equipment is always kept in the nephrologist’s office. It is mounted to a rolling cart that is especially fitted to hold the equipment. A dedicated T-1 line runs directly to the nephrologist's office so that the telemedicine unit can connect to the other telemedicine sites.

2.1.3 Nephrologist's Home

The third remote site, the physician’s residence, is in a secluded residential area in McLean, Virginia. The neighborhood is reported to have a low crime rate and neighbors seem to show an interest in the comings and goings at other houses. The back of the house looks onto a large wooded area. The building has a sophisticated security system installed. It includes noise, motion and smoke detectors and fire alarms, which are all connected to the security company's dispatcher. The security system has three levels of sensitivity that can be set by the residents. When someone is at home, the security system is set to the lowest level, level one, which registers when someone leaves or enters the house. When the house is empty, the security system is set to three, detecting all motion in the house and sharp sounds such as the sound of breaking glass. The nephrologist's family owns two dogs, one of which is always in the house. There are four entrances to the house: the front door, garage, back door, and French door. All unused doors are kept locked and double bolted.

The telemedicine equipment is placed in a room on the second floor of the house. The unit is mounted on a large desk fitted to hold the equipment. There is a noise detector located in the room and a surge protector on the power outlet for the telemedicine system. Like the nephrologist's office, his home is equipped with a dedicated T-1 line. The T-1 connection box is located in the garage of the residence. Although water pipes are located directly adjacent to the box, a heating unit prevents the pipes from freezing during cold weather.

2.1.4 ISIS Center (Long-term Archive)

The ISIS Center at Georgetown University Medical Center is part of the Project Phoenix telemedicine testbed, housing a StorageTek magnetic tape silo, the long-term archive facility for all electronic patient information. The ISIS Center is on the top floor of an office building in Washington, DC. This building is freely accessible to anyone during

office hours but requires a keycard for entry during off hours. The ISIS Center office suite has several locked entrances, each equipped with a combination or keycard lock. The main entrance is staffed by a receptionist during office hours. Visitors must be let in by the receptionist and are required to sign in. A security guard is stationed in the main hallway and patrols the suite regularly.

The ISIS Center has a staff of approximately 30 people, including researchers, some technical personnel and a few administrative staff. Each of these staff members has a keycard and knows the number combination on the locked doors. Various other University employees, such as couriers, maintenance staff, building managers, etc., also know the code of the combination locks. Due to the large number of visitors to the facility, visitors unknown to most staff members are common.

The StorageTek tape archive is located in an unlocked computer room within the ISIS Center. The computer room is equipped with a special air-conditioning unit. Although the office building has a policy of shutting down some electrical circuits during holidays and weekends, the computer room power supply is not affected by these shutdowns. However, when the building power goes out for any reason, the computer room and its air-conditioning system also lose power.

2.2 Equipment

Much of the equipment used at the Union Plaza dialysis unit is similar to that used at the control site at GUMC. It is described in that site's risk analysis and is not further explained here unless there are significant differences between the two sites. The following equipment produces or affects patient information in the telemedicine testbed:

- Fresenius dialysis machines (18 machines, 3 spares)
- Blood pressure gauges
- Thermometers
- Scale
- Unit secretary's PC and printer: The unit secretary has a PC on her desk in her office, which she uses to track inventories of epogen, etc. and for correspondence. The Clinical Information System (CIS) also resides on this machine. The Clinical Information System, developed by TRC, maintains cumulative patient care reports for monitoring and managing the quality of care provided by TRC. These reports include lab values and incident reports. Lab values are cumulative monthly and quarterly test results, and incident reports are reports of hospitalizations per year, infection information, deaths per year. At the end of every month the unit secretary e-mails the local CIS database to TRC's central office. The unit administrator and unit secretary are trained to use the CIS. Only the unit secretary has the password to this computer.

- Lab computer and printer: The laboratory terminal and printer are located in the treatment area behind the secretary's office, a few feet away from the closest dialysis machine, making them easily readable by nearby patients or visitors. Results of blood tests are transmitted from the laboratory over a modem and printed on the attached printer twice a week during office hours. The lab computer is also used by unit staff to access lab results on-line. The staff members who have passwords for this computer are the nurse manager, charge nurses, and unit secretary. From our several visits to the unit, we have noticed that the terminal is usually left logged on.

- Telemedicine equipment: The dialysis telemedicine unit assists the physician in monitoring dialysis patients over a telecommunication link. The unit is an integration of two systems: the Fresenius Dialysis System and the MMS Carelink system. A buffer PC is located between the two systems. The Fresenius Dialysis system consists of the dialysis machines and the Fresenius Dialysis Concentrator which collects dialysis parameters from the dialysis machines. The Carelink system collects data from the concentrator and sends them over a telecommunication link. The concentrator, Buffer PC, and Carelink system are described in more detail in the following section (Section 2.2.1).

- Tape Archive: The long-term archive to be used for Project Phoenix is a StorageTek WolfCreek magnetic tape library located at the ISIS Center at GUMC. This device can store almost 1 Terabyte of data on 800 MB magnetic tapes. It is connected to other computers at the ISIS Center over a local area Ethernet network which has open access to the University network and the Internet.

2.2.1 Dialysis Telemedicine Unit

All 16 dialysis machines are may be connected to the local telemedicine unit. Data from each dialysis session is captured and transmitted to the telemedicine unit via a series of intermediate computers:

- Concentrator PC: The concentrator is a low-end PC, running the DOS operating system, that connects to all of the functioning Fresenius dialysis machines in the dialysis unit and displays the dialysis parameters received from these machines on its screen. Each dialysis machine is given a station number, and the corresponding row in the screen represents all of the data of one dialysis machine. Figure 2 shows how data is displayed on the concentrator. The station IDs are shown in the first column, and each row displays dialysis parameters such as Arterial Pressure, Venous Pressure, Conductivity, etc. received from each dialysis machine. The concentrator is the first link in the process of downloading dialysis parameters from the dialysis machines to the telemedicine system. It is not protected by any password and displays data on its screen whenever it is active. The concentrator can display up to 32 stations at a time.

Station	Mod Alm Art Ven TMP Cond Temp Dflw BFlw UFR SYS DIA MAP PLS UFV BVP
1	
2	
:	
32	

Figure 2. Display of the Concentrator

- Buffer PC: The Buffer PC lies between the concentrator and the Carelink system. The Buffer PC receives the patient record from the concentrator and writes it to the database on the telemedicine system. The Buffer PC has a patient ID-station ID lookup table. The Buffer PC reads the station ID from the record, uses the lookup table to obtain the corresponding patient ID and writes to the appropriate patient's folder. If the patient folder does not exist on the telemedicine system, it is created. At the beginning of each session the nurse must input the corresponding patient ID into one of the 16 slots representing the station ID for the lookup table to work properly.

- MMS Carelink System: Each telemedicine machine consists of a computer, monitor, video camera, head set, microphone, speakers, an electronic stethoscope, and a disk drive. It is connected via a T-1 line to one of the remote telemedicine systems when the nephrologist wants to talk to a nurse or patient via video conferencing. The headset and microphone are used for private communication between the physician and patient or nurse. Patient information is stored in the database on each telemedicine unit and can be transmitted between sites. The master database of telemedicine patient records will reside on the telemedicine unit at the treatment site at Union Plaza. Data, such as dialysis parameters from the Fresenius dialysis machines or, separately from TRC's CIS database, can also be stored on the telemedicine system. Other data that can be stored include the sounds from the electronic stethoscope, conversations between patient and doctor, and still video images. A high-capacity external disk drive for removable data cartridges is attached to the telemedicine computer. These cartridges will be used to transfer patient information from the telemedicine system to the long-term archive facility. MMS Carelink, the telemedicine application, currently runs under the Windows 3.11 operating system with minimal security features built in. There are plans to upgrade to the Windows NT operating system and Carelink software running on Windows NT in the near future. The Windows NT version will have strong password protection mechanisms, audit logs, access control lists, digital signatures, and the ability to encrypt data sent over a network, none of which exist in the present version. At present, we are looking at ways to provide security without having to upgrading to a new system.

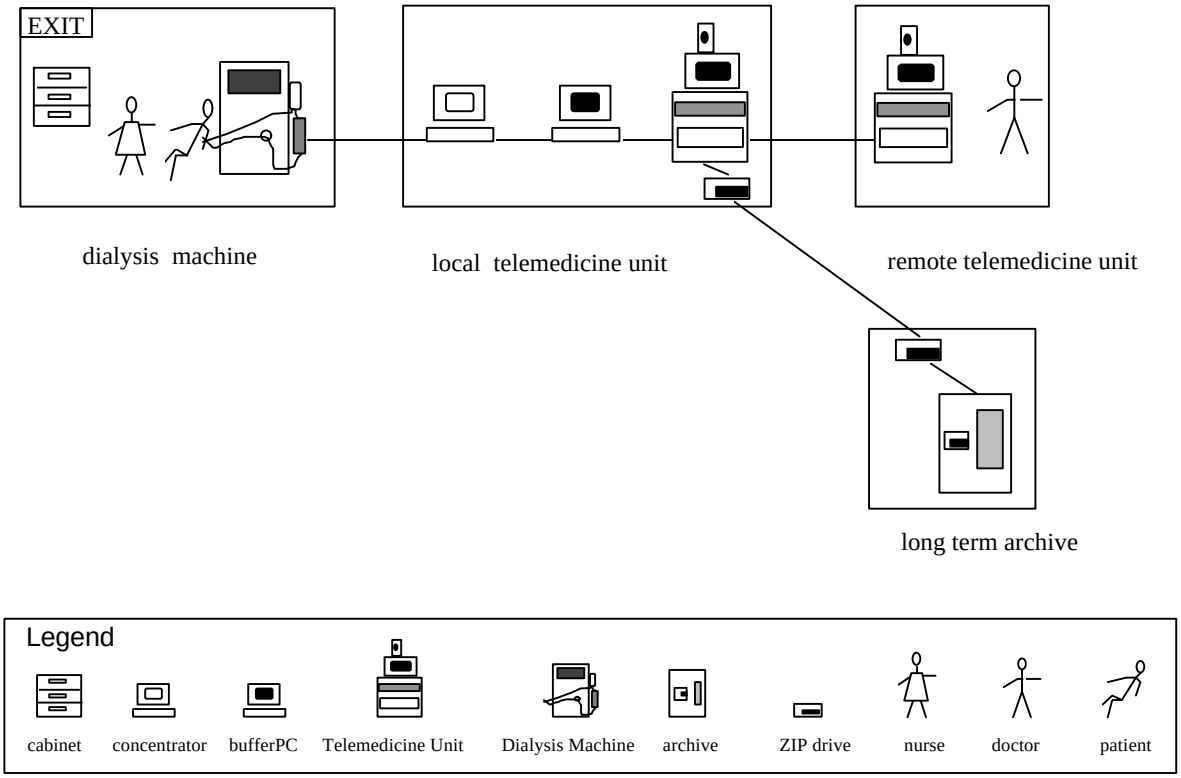


Figure 3. Telemedicine System

2.3 Procedures

This section describes procedures relevant to telemedicine and any areas where clinical and administrative procedures differ from those used at the control site at GUMC. Figure 3 provides a description of the layout of the overall telemedicine system. The common procedures associated with kidney dialysis and the management of paper-based patient data are discussed in the previous document, Risk Analysis of Paper-Based Kidney Dialysis System[Meis].

2.3.1 Dialysis - New Patient

In addition to creating a new patient chart, explaining dialysis procedures and obtaining informed consent for dialysis, as described in the previous risk analysis, dialysis unit staff perform some procedures specific to telemedicine. Most importantly, they inform patients of the telemedicine procedures and ask for patient consent to participate in the telemedicine experiment. If a patient agrees, his or her name will be added to the lookup table in the buffer PC (see Section 2.2.1) and an electronic patient folder will be automatically created in the course of his or her next dialysis session.

2.3.2 Dialysis - Telemedicine Consultation

In addition to normal rounds, the nephrologist consults with each patient once per week over the telemedicine system. The telemedicine system is also used in emergencies. When the physician makes rounds using the telemedicine system, the nurse wheels the

telemedicine machine to each patient in turn. The patient and physician can communicate using earphones, a microphone, and a camera mounted on each telemedicine system. They can see each other on the system's computer monitors. The doctor may also view the patient's downloaded dialysis parameters on the telemedicine system monitor. He can listen to the patient’s heartbeat through an electronic stethoscope, and retrieve other electronically stored patient information such as video stills.

The following procedure is intended to be used once the system is clinically used on a regular basis.

At the beginning of each dialysis day, the nurse wheels the telemedicine system from its locked storage room to the treatment area and hooks it up to the buffer PC which is connected to the concentrator. The nurse will also input the patient ID into the corresponding machine ID slot in the lookup table on the buffer PC. Whenever the telemedicine system is connected to the buffer PC, that PC will automatically download the stored dialysis parameter information of all dialysis machines into the telemedicine database. Using the machine ID- patient ID lookup table, the telemedicine system finds the appropriate patient folder in which to store the data.

In order to hold a telemedicine consultation, the telemedicine system is wheeled next to the patient. The nephrologist at the remote site starts the telemedicine application and establishes the connection with the dialysis site. The nephrologist may then review the patient information on the telemedicine system and talk to the patient. At the dialysis unit, a nurse assists the patient and, where appropriate, confers with the physician over the telemedicine link.

At the end of each dialysis day, the nurse makes sure that all dialysis parameters have been downloaded, disconnects the telemedicine system and locks it up in the secure room.

2.3.3 Archiving

At regular intervals to be established later, the physician or nurse will copy old or outdated patient information from the telemedicine system to the attached disk drive, using the option provided by the telemedicine application software. Because the telemedicine system is not connected to a network, the data cartridge must then be taken by hand to the long-term archive facility at the ISIS Center. There, it will be loaded onto another PC. The engineer assigned to Project Phoenix (discussed in Section 2.4) will retrieve the telemedicine patient data from the cartridge and send it over the ISIS Center LAN to the StorageTek tape archive. The cartridge will be returned to the dialysis unit reuse. The ISIS Center LAN can be accessed directly from the Internet.

2.3.4 Equipment maintenance

Much of the equipment used at the dialysis unit directly affects the integrity of the electronic patient data stored in the telemedicine system. Therefore, the security of equipment such as the dialysis machines and temperature and blood pressure gauges is

extremely relevant to risks associated with the telemedicine system. The maintenance of most of this equipment is evaluated in the previous document, Risk Analysis of Paper-Based Kidney Dialysis System. This section discusses the maintenance of the telemedicine system itself, the telecommunications lines, the interface to the Fresenius dialysis machines, and the long-term archive facility.

Basic maintenance of the telemedicine system will be performed by the telemedicine nurse hired and trained specifically to manage the telemedicine system (see Section 2.4). This nurse will be able to connect and disconnect the system, and handle any minor problems as they occur. The telemedicine nurse will also be given a detailed user manual (Annex F) that he or she will use to fix any problems. If an error occurs that the nurse is not capable of handling, the nurse will page the engineer who works at the ISIS center. This engineer has been involved in setting up the system from the beginning and is knowledgeable about its operations. He wrote the user manual. If there is a problem that neither the nurse nor the engineer can solve, the technician will call Multimedia Medical Systems (MMS) for service.

2.4 Personnel

The clinical staff of the Union Plaza dialysis unit is very similar to the staff of the control site at the GUMC. In fact, some members were transferred from Georgetown University Medical Center. Therefore, these staff members will not be further described here unless their duties differ. The telemedicine site has two new positions associated with the project: a nurse responsible for telemedicine at the site and an engineer to maintain the telemedicine infrastructure.

Telemedicine Nurse
This nurse will be recruited and trained specifically to perform telemedicine-related duties at the dialysis unit and to assist the nephrologist during telemedicine consultations. The telemedicine nurse is an employee of TRC, but will report to Dr. Winchester, the nephrologist.

Engineer
The engineer is a staff member of the ISIS Center, who will work at the Union Plaza dialysis unit as needed. He is responsible for configuring, maintaining, and troubleshooting the telemedicine equipment and, if necessary, contacting the vendor for additional support. This person has worked closely with the telemedicine vendor in developing the interface to the dialysis machines and in making the telemedicine system operational. He is known to all clinical staff members at the dialysis unit.

Cleaning Staff
Besides the dialysis unit personnel, the cleaning staff have access to the unit. The cleaning staff comes in to clean daily, after the close of business and has a master key for the unit. The cleaning staff is hired by the maintenance office of the building.

2.5 Intangibles

In addition to the concrete information, equipment and procedures described above, there are other, more intangible assets at the dialysis unit that must be protected. If the goals of Project Phoenix, which include providing information security and patient confidentiality, are achieved, Georgetown University Medical Center and Total Renal Care, Inc. will increase their academic and clinical reputation. However, if breaches of security or confidentiality negatively affect the success of the project, these institutions stand to lose some credibility and suffer financially.

Patient satisfaction and confidence in the institution that provides their dialysis is an important concern of the dialysis unit staff and management. One of the problems of kidney dialysis is that patients sometimes become bored or frustrated with the lengthy treatment and opt to finish their dialysis sessions early. Studies have shown that such shortening of dialysis can negatively affect the quality of the patient's treatment [Yang]. It is therefore important to minimize the conditions that cause patients to leave the unit early. Telemedicine may help with this problem by providing additional contact between the patient and the physician, whereby the physician may convince the patient of the benefits of completing their treatment. If telemedicine can provide secure management of patient medical information, it may become a viable addition to the routine treatment of dialysis patients.

These and other intangibles contribute significantly to the success of the telemedicine testbed and must be taken into account when managing risks to information security and patient confidentiality.

3. Risk Analysis

3.1 Threats and Vulnerabilities

This section examines possible threats and vulnerabilities to the security of the electronic patient records stored, and used within the dialysis unit. Although the traditional paper records used at this dialysis unit may also be subject to security and confidentiality risks, these risks are examined in the Risk Analysis of the paper-based system[Meis] and will not be repeated in this report. Threats to the data include anything that could affect the accuracy, completeness, availability, and confidentiality of electronic patient information. Threats and vulnerabilities are listed in three categories according their impact: data integrity, availability, and confidentiality. Some are listed in multiple categories. Each threat is described and its likelihood and potential for damage are evaluated.

For each threat, a frequency of occurrence of Low, Medium or High is given. These ratings are relative, with a frequency of Low meaning rarely or never, Medium meaning occasionally or a few times a year, and High meaning regularly or on a weekly basis (Table 1).

Frequency Rating	Meaning
Low	rarely or never occurs
Medium	occurs occasionally or a few times per year
High	occurs regularly or on a weekly basis

Table 1. Description of Frequency Ratings

Expected loss is also rated Low, Medium, or High. This value refers to the potential for damage should each threat occur. For data integrity, the expected loss from an occurring threat is rated High if the changed data is critical to the patient's care, or if the change is permanent or unlikely to be detected. Low expected loss indicates changes to old or non-vital data or if the change is likely to be detected through normal operating procedures (Table 2). For availability, a High expected loss means that the unavailable data is critical and very time-consuming to replace or that the loss is permanent. A rating of Low shows losses of non-critical data or that can be replaced easily (Table 3). For confidentiality, the rating of expected loss depends mostly on the intentions of the person who gains access to confidential information illegitimately. Breach of patient confidentiality by someone who has no intention of using the information would incur a Low expected loss. If, on the other hand, someone could use the information to harm the patient's care or reputation or for financial gain, the expected loss might be rated as High (Table 4).

Expected Loss Rating	Meaning
Low	data is old or non-vital, change is likely to be detected through normal procedures
Medium	data is important to patient care, change may be detected through normal procedures or cross-checking
High	data is critical to patient care, change is permanent or unlikely to be detected

Table 2. Description of Expected Loss Ratings for Data Integrity

Expected Loss Rating	Meaning
Low	non-critical data, may be replaced easily
Medium	important data, may be replaced with some effort, may be a one-time loss
High	data is critical, loss is permanent or very time-consuming to replace

Table 3. Description of Expected Loss Ratings for Availability

Expected Loss Rating	Meaning
Low	disclosed information is not sensitive, person receiving confidential information has no intention of using it
Medium	disclosed information is somewhat sensitive, person receiving information does not intend to use it for malicious purposes
High	disclosed information is sensitive, person receiving confidential information intends to use it to harm the patient's care or reputation or for financial gain

Table 4. Description of Expected Loss Ratings for Confidentiality

3.1.1 Data integrity

In order for patients to be treated appropriately for their medical condition, physicians and other clinical staff must have accurate and complete information on the patient. Unit staff rely upon and trust the information produced by the dialysis machines and stored in the telemedicine unit. The integrity of this information depends upon four conditions: 1) the reliability of the sensing and display devices monitoring the hemodialysis process, 2) the accuracy and reliability with which unit staff record information in the chart, 3) the accuracy and reliability of the telemedicine unit and 4) the security measures in place to protect patient data stored either electronically or paper-based.

I1. Electronic Data Alteration/Destruction(error/deliberate):

A staff member, visitor or outsider might be able to modify or delete patient information stored electronically in the telemedicine system or any of the computers. This could be due to unfamiliarity with the system or to malicious intent. A deliberate alteration by dialysis unit staff members is unlikely because they are healthcare professionals trained in the importance of accurate information to their patients' condition.

Frequency: Low **Expected Loss:** Medium

I2. Data is input incorrectly in the telemedicine system:

When patient information is entered into the telemedicine database manually, there is always the possibility of data entry errors. The frequency of such an occurrence is low because most data will not be typed in but transferred electronically.

Frequency: Low **Expected Loss:** Medium

I3. No control over outside software in system:

Software brought by staff members from outside the dialysis unit could malfunction, crash the telemedicine system, totally erase files, or be virus-infected. So far, no cases of outside software use have occurred.

Frequency: Low. **Expected Loss:** High

3.1.2 Availability

Since the physician will make rounds and respond to emergencies using the telemedicine unit, it is important that the unit itself and all the data stored inside it is immediately accessible whenever needed.

A1. Electronic Data Alteration/Destruction(error/deliberate):

A staff member, visitor or outsider could delete any electronically stored patient information, making the information unavailable for treatment purposes. This could be due to unfamiliarity with the system, or to malicious intent.

Frequency: Low **Expected Loss:** Medium

A2. Telemedicine unit does not function properly:

If the telemedicine system does not function properly, for instance if it cannot transmit the selected data from the concentrator, or if the video camera does not work, patients will not be able to be diagnosed properly and efficiently. This threat can be minimized by proper design and sufficient testing and maintenance of the system.

Frequency: Medium **Expected Loss:** Medium

A3. Personnel are not sufficiently equipped to handle the telemedicine unit:

If the staff are not familiar with the system, they may make mistakes such as deleting files, or not storing files correctly. This is highly unlikely since staff members will be trained on how to use the unit. Also, an extensive operations manual has been prepared and will be kept nearby.

Frequency: Low. **Expected Loss:** Medium

A4. Telemedicine system destroyed/damaged by: water, other spills, fire, wind, earthquake, explosion:

Even though there have been no such occurrences so far, as with any computers in the dialysis unit, if for instance, water or coffee spills were to fall on a keyboard or mouse, it would temporarily make the computer unavailable, leading to unavailability of data.

Frequency: Low **Expected Loss:** Medium

A5. No Universal Power Supply (UPS):

In the case of a complete power failure at the treatment center during use of the telemedicine system, parts of the electronic patient information in the database could be irretrievably lost.

Frequency: Low **Expected Loss:** Medium

3.1.3 Confidentiality

Patient confidentiality is breached whenever anyone other than the patient, the patient's physician or other healthcare professional directly responsible for the patient's care learns any private patient information.

C1. System is susceptible to interception during transmission - e.g. eavesdropping, tapping, snooping:

When data is being transmitted over the network from one telemedicine unit to another, an eavesdropper could tap into the network. This way it is possible to intercept conversations between the physician and the patient, or obtain any patient information being transmitted. The likelihood of such an occurrence are thought to be low because this requires skill, and an eavesdropper would not have any way of knowing when which patient is being remotely diagnosed.

Frequency: Low. **Expected Loss:** Medium

C2. Data is intercepted in transit between data cartridge and long term archive:

When data is transferred to the StorageTek tape archive, it is transmitted over a LAN accessible from the Internet. This makes it susceptible to eavesdropping over the network. Although the information transferred is not recent, the potential damage of disclosure could be high, depending on the sensitivity of the information.

Frequency: Low **Expected Loss:** High

C3. Inadequate password management process:

Even when passwords are used, if passwords are easy to guess or are not changed frequently, or if users remain logged on and leave the computer unattended, it is easy for unauthorized persons to view/delete/modify the data on the computers and telemedicine unit. Currently, the criteria for password selection for the telemedicine unit do not require any special characters or a minimum length password.

Frequency: High. **Expected Loss:** Medium

C4. Poor user password protection practices:

Even when hard-to-guess passwords are used, if passwords are written down or given to other people, the system is still susceptible to unauthorized access. In interviewing some of the nurses, we discovered that people borrowed passwords from other staff members because they had forgotten theirs, or they had received incorrect passwords. Even if passwords are passed around, it will not be a huge threat because the personnel would not hand over their password to an unauthorized user.

Frequency: High **Expected Loss:** Medium

C5. Off-site archive susceptible to unauthorized building access:

All visitors to the ISIS Center enter through a staffed entrance and are asked to sign-in. Once inside the Center however, they could easily access the computer room where archives are kept because this room is always unlocked. The ISIS Center has a large number of visitors and staff members are used to seeing unfamiliar faces, so they might not challenge an unauthorized intruder.

Frequency: Low **Expected Loss:** Medium

C6. Loss of confidentiality due to no/inadequate audit trail log:

No electronic auditing is currently in place on the telemedicine system. In the event of a breach in patient confidentiality, an electronic audit log could be used to trace the actions of personnel and aid in discovering if there was any unauthorized access to the system.

Frequency: Low **Expected Loss:** Medium

C7. Violation of patient confidentiality due to no/inadequate system access control procedures:

Access control mechanisms limit access to electronic information based on the identity or role of an individual in an organization.

Frequency: Low **Expected Loss:** Medium

3.2 Expected Loss Analysis

The following table lists all threats and their frequency of occurrence and expected loss, sorted by threat category, expected loss, and frequency. For each threat category, the threats are listed in the order of severity.

Threat	Frequency	Exp. Loss
I3. No control over outside software in system	Low	High
I1. Electronic data alteration/destruction (error/deliberate)	Low	Medium
I2. Data is input incorrectly in the telemedicine system	Low	Medium
A2. Telemedicine unit does not function properly	Medium	Medium
A3. Personnel are not sufficiently equipped to handle the telemedicine unit	Low	High
A1. Electronic data alteration/destruction (error/deliberate)	Low	Medium
A4. Telemedicine system destroyed/damaged by: water, spills, fire, wind, earthquake, explosion	Low	Medium
A5. No UPS	Low	Medium
C2. Data is intercepted in transit between data cartridge and long term archive	Low	High
C3. Inadequate password management process	High	Medium
C4. Poor user password protection practices	High	Medium
C1. System is susceptible to interception during transmission- eavesdropping, tapping, snooping	Low	Medium
C5. Offsite archive susceptible to unauthorized building access	Low	Medium
C6. Loss of confidentiality due to no/inadequate audit trail	Low	Medium
C7. Violation of patient confidentiality due to no/inadequate system access control procedures	Low	Medium

Table 5. List of Threats

4. Recommendations

4.1 Possible Countermeasures

The following potential controls can be used at electronic dialysis unit to counteract the threats to data integrity, availability and confidentiality of patient information in a telemedicine system.

The cost to implement each countermeasure is described. These costs refer to not only financial costs but also the additional time and effort required to implement the countermeasures. Costs are ranked on a scale of 1 to 7 where 1 is the least expensive and 7 is the most expensive. For example, a cost of 1 would indicate little or no inconvenience and/or a negligible dollar amount. A countermeasure is given a higher (lower) cost ranking than another countermeasure if it requires decidedly more (less) effort and/or financial investment. Where precise cost information was unavailable, the ratings were given on a qualitative basis using the judgment of the risk analysis team. Costs refer to maintaining the countermeasure for one year unless otherwise noted.

R1. Increase security awareness training for all staff:

Most staff members are aware of security problems and do their best to protect patient confidentiality and integrity of the data. Nevertheless, the dialysis unit may benefit from regular training sessions on the unit's policies, the importance of information security and patient confidentiality, what staff can do to improve security, and on the consequences of breaches to the institution and to themselves.

Cost: 3 (time for staff, time for trainer, educational materials)

R2. Hire personnel to handle telemedicine unit:

All personnel should have some basic training on the use of the telemedicine unit. Anytime the unit is used, there should be at least one person on duty who is trained in every aspect of the telemedicine unit. The physician himself should be extensively trained on the entire telemedicine system because he often will be the only person present at the remote telemedicine site.

Cost: 7 ($37,000 cost of hiring additional person + cost of training)

R3. Use of encryption during transfer between telemedicine units:

Since private information such as patient data, images, and conversations are being electronically transmitted over telephone lines, this data should be encrypted during transmission between the sending and receiving telemedicine units.

Cost: 2 (encryption algorithm, minor inconvenience)

R4. Use of encryption between data cartridge and archive over network:

When data is being transferred between data cartridges and the off-site archive at the ISIS Center, data is transferred over a LAN accessible from the Internet. To protect data from being captured en route, encryption between the data cartridge and the archive should be used.

Cost: 2 (encryption algorithm, minor inconvenience)

R5. Control access to telemedicine application:

Through access control mechanisms, access should be limited to the telemedicine system and the data stored there. For example, in role-based access control only the doctor could delete or modify patient information stored on the database, and the telemedicine nurse could only view patient records in the database.

Cost: 2 (access control mechanism)

R6. Require the use of audit logs:

Audit logs should be kept of who logs in, the time of use, and activities performed using this account. Audit logs can prevent persons from doing something unauthorized as well as help discover who the perpetrator was in the event an intrusion is detected.

Cost: 3 (install audit mechanism, minor inconvenience)

R7. Enforce password management practices:

For the members of the staff that have access to the computers, there should be a policy regarding passwords. This policy should enforce the use of hard-to-guess passwords, train staff not to write down or share passwords, and to change their password frequently.

Cost: 1 (minor inconvenience to personnel)

R8. Install virus detection/protection software:

A virus protection program should be installed to detect and disable any viruses that came into the system. Viruses will most likely enter the system from an outside source.

Cost: 1 ($100: cost of the software)

R9. Develop a preventive maintenance program for the telemedicine system:

A proper preventive maintenance program should be developed. This program would require scheduled maintenance and testing of the system. It would check if data is sent correctly from the concentrator to the telemedicine unit, between telemedicine units, if all components of the system - headset, microphone, video camera, speakers, etc. - worked correctly, and order any spare parts required for the system.

Cost: 4 ($100/month engineer's time = $1200)

R10. Better access control for off-site archive:
A lock should be installed and used on the computer room that contains the StorageTek in the off-site long term archive.
Cost: 1 (cost of lock, minor inconvenience to users)

R11. Install Uninterruptible Power Supply (UPS) for local telemedicine site:
An Uninterruptible Power Supply should be installed to allow for graceful degradation and shutdown in the case of a power failure.
Cost: 3 ($500: cost of UPS)

R12. Upgrade to Windows NT version as soon as possible:
Upgrading to MMS Carelink's Windows NT version will take care of many of the threats mentioned above. The upgraded version reportedly comes with better password protection, encryption capabilities, audit logs, and improved operating system security.
Cost: 6 (cost of upgrading to Windows NT, upgrading to new Carelink version, installing and testing the system)

4.2 Evaluation of Countermeasures

The above countermeasures are evaluated by considering their cost, which threats they diminish, and by how much. To do this, the threats themselves are assigned a severity according to their frequency of occurrence and expected loss as shown in Table 6 below.

Expected Loss/Frequency	Low	Medium	High
Low	1	2	3
Medium	2	4	6
High	3	6	9

Table 6. Severity of Threats

The next table, Table 7, analyses the countermeasures suggested above based on the severity of threats given in Table 6, and reduction of a threat's severity achieved by the corresponding countermeasure. The reduction of severity is a qualitative measure given to each countermeasure based on the strength of the countermeasure, and the experience of the risk analysis team members.

Table 7 lists the threats in the leftmost column, followed by their severity. Countermeasures are listed in the top row. At each intersection between a threat and a countermeasure, a percentage indicates the amount of reduction in the threat's severity achieved by the corresponding countermeasure.

At the bottom of the table, each countermeasure is evaluated. The total severity reduction is a sum of the reductions in severity for all the threats that the countermeasure can

mitigate. For example, countermeasure R9, Develop a preventive maintenance program for the telemedicine system, mitigates threats A2 and A4 by 90% and 20%, respectively. Threat A2's severity is reduced by 90% from 4 to 0.4, and A4's severity is reduced by 20% from 2 to 1.6. Thus a total severity reduction by countermeasure R9 is given by the sum of severity reductions of each corresponding threat. The sum, 4.0, and is entered in the row showing total severity reduction. The greater the total reduction in severity, the greater is the perceived benefit from the countermeasure.

The cost of each countermeasure, defined in section 4.1 is also listed. For each countermeasure, the cost/benefit ratio is the cost of the countermeasure divided by the total severity reduction. For reasons listed below (Section 4.3), a ratio of less than 0.8 was decided to be favorable because it provides a reasonable cut-off point between intuitively effective and non-effective countermeasures. The row labeled Y/N shows a decision of whether or not each countermeasure should be recommended based on the cost/benefit ratio. The recommendations of this risk analysis are not based solely on the numerical results of the cost/benefit analysis as indicated by an * next to some of the Y/N decisions and explained below.

Threat	**Severity**	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**	**R8**	**R9**	**R10**	**R11**	**R12**
I1	2	50%	90%			90%	30%	20%					
I2	2	20%	80%				10%						
I3	2	70%	60%			90%	30%		70%				
A1	2	50%	90%			90%	30%	20%					
A2	4		10%							90%			
A3	3		80%										
A4	2	10%	20%							20%			
A5	2											100%	
C1	2			100%									100%
C2	3				100%								
C3	6	70%						70%					70%
C4	6	70%					20%	70%					
C5	2										90%		
C6	2						100%						100%
C7	2					100%							100%
total severity reduction		12.40	9.60	2.00	3.00	7.40	5.20	9.20	1.40	4.00	1.80	2.00	10.20
cost of countermeasure		3	7	2	2	2	3	1	1	4	1	3	6
cost/benefit		0.24	0.73	1.00	0.67	0.27	0.58	0.11	0.71	1.00	0.56	1.50	0.59
Y/N		Y	Y	N*	Y	Y	Y	Y	Y	N*	Y	N	Y*

Table 7. Analysis of Countermeasures

4.3 Recommendation of Countermeasures

Many of the threats pertaining to the telemedicine system that were noticed in this risk analysis will reportedly no longer be present in the new version of Carelink for Windows NT. The Windows NT version will require stronger passwords, provide various levels of access control, keep audit logs, and allow encryption between networks. Therefore, by recommending the upgrade to the Windows NT version as soon as possible, some countermeasures need not be recommended regardless of their cost/benefit ratio.

Recommended

R1. Increase security awareness training for all staff
R2. Hire personnel to handle telemedicine unit
R3. Use of encryption during transfer between telemedicine units*

Although this recommendation has a high cost/benefit ratio, it is recommended in this risk analysis because it is the only countermeasure that mitigates eavesdropping threats and the cost of implementation is relatively low.

R4. Use of encryption between data cartridge and Archive over the Internet
R5. Control access to telemedicine application
R6. Require the use of audit logs
R7. Enforce password management practices
R8. Install virus detection/protection software
R9. Develop a preventive maintenance program of the telemedicine system*

Even though this recommendation has a high cost/benefit ratio, it is recommended by this risk analysis. The cost of implementing a preventive maintenance program is relatively low and preventive maintenance is very important to the availability of the telemedicine equipment and the data stored on the equipment.

R10. Better access control for off-site archive
R12. Upgrade to Windows NT version as soon as possible*

Upgrading to MMS Carelink's Windows NT version should take care of many of the threats mentioned above. The upgraded version comes with better password protection, encryption capabilities, audit logs, etc. When upgrading to the Windows NT version, it will be much easier to implement countermeasures R3, R5, and R6.

Not Recommended

R11. Install Uninterruptible Power System(UPS) for local telemedicine site

5. Conclusion

As shown in this risk analysis, the risks to a telemedicine system include threats different from those to a paper-based patient record management system. The data is more widely accessible and its security depends on the proper functioning of computer hardware and software, such as an auditing capability, as well as procedural measures like the practice of good password management. On the other hand, using an electronic patient record management system also makes available more sophisticated countermeasures to protect against security threats. For example, storing the data in electronic form gives staff members more control over who has access to the data and easier and more effective mechanisms to archive it.

The results of this risk analysis show that it is necessary to increase security awareness training for all staff. Although most staff members are health care professionals, trained in the need for protecting patient confidentiality, the use of computerized records raises new issues which may be unfamiliar to the staff. An increase in the security awareness of all staff members, especially in regard to electronic patient records, will mitigate many of the

risks related to unintended threats to the system. Intended threats from staff members are viewed as unlikely.

Because confidential information will be transmitted over telephone lines and a network accessible from the Internet, it is crucial to protect this information from eavesdroppers. Encryption is currently the only viable method to do this and is strongly recommended by this risk analysis.

If possible, one of the greatest benefit to the security of electronic patient records will be upgrading to the Carelink Windows NT version. This recommendation encompasses other recommendations such as maintaining audit logs, and implementing access control. The upgrade to the new system is expected in the near future (possibly in the fall of 1997). Until then, the separate countermeasures recommended, such as the use of encryption between telemedicine units, access control mechanisms and audit logs, should be implemented.

6. References

[Yang] Yang C.-S., Chen S.-W., Wang M, Peng S.-J., Kan Y.-T., Effects of Increasing Dialysis Dose on Serum Albumin and Mortality in Hemodialysis Patients, American Journal of Kidney Diseases, Vol. 27, No 3 (March), 1996.

[Meis] Meissner M.*, Kim A.**, Hoffman L. J.**, Collmann J.**, Risk Analysis of Paper-Based Kidney Dialysis System, * ISIS Center, Radiology Dept., Georgetown University Medical Center, Washington, D.C., ** Cyberspace Policy Institute, School of Engineering and Applied Science, The George Washington University, Washington, DC.

[CPI] Checklist of threats, vulnerabilities, and countermeasures for risk analysis. WWW site of Cyberspace Policy Institute, School of Engineering and Applied Science, The George Washington University, Washington, DC.
http://www.cpi.seas.gwu.edu/courses/cs229/threats.wpd

7. Annexes

The following documents were used in preparing this risk analysis. They are not included here for briefness but are available from the authors upon request.

Annex A - Patient Care Forms

Initial Patient Interview and Assessment
Admission Nursing Assessment
Initial Hemodialysis Treatments Orders
Initial Care Plan
Patient Care Plan (short term)
Long Term Program
Dialysis Session F1ow Sheet
Patient Education Flow Sheet

Annex B - Consent Forms, Patient Education

Consent to Chronic Hemodialysis Treatment
Consent for administration of blood and/or blood components
Consent for HIV Testing
Consent for Infed Therapy
Consent for Calcijex Administration
Consent for Erythropoietin Therapy
Consent for Reprocessing of Dialyzer and Dialyzer Caps
Evacuation Procedure - Instructions for Patients
Drug Evaluation Monographs

Annex C - Provider (TRC) Policies

Medical Records Policy
Working with Confidential Documents
Corporate Code of Conduct
Corporate Compliance Program

Annex D - Floor Plans

PHC Sixth Floor P08 - general floor plan
Dialysis Suite - Plumbing
Dialysis Suite - Power

Annex E - Dialysis Machine Maintenance

Hydraulic Flow Diagram - A2008
Maintenance Checklist
Electronic Adjustment Points Diagram

Annex F - Operations Manual

Telemedicine Machine Operations Manual

Plan for Managing Risks

Project Phoenix - Safeguarding the Security and Confidentiality of Patient Information

Marion C. Meissner*, Anya Kim, Jeff Collmann*, Lance J. Hoffman**, Seong K. Mun***

*** ISIS Center, Radiology Department**
Georgetown University Medical Center
Washington, DC 20007

**** Cyberspace Policy Institute, School of Engineering and Applied Science**
The George Washington University
Washington, DC 20052

March 31, 1997

1. Introduction

This document is part of Georgetown University Medical Center's (GUMC) Project Phoenix: Scrutinizing a Telemedicine Testbed. Project Phoenix is a joint effort of the Imaging Science and Information Systems (ISIS) Center, Department of Radiology, and the Clinical Economics Research Unit (CERU), Department of Medicine, at GUMC, to perform evaluation studies on clinical economics and data security. Data from the study on clinical data security will be used to test the hypothesis that electronic telemedicine systems, when managed according to established information security practices, provide increased access to and maintain the security of patient information, compared to paper-based medical records.

This risk management plan is based on the findings of the preceding risk analyses of the Project Phoenix control site, a traditional kidney dialysis unit at Georgetown University Medical Center, the telemedicine-based kidney dialysis unit at Union Plaza in Washington, DC, and other the sites comprising the telemedicine testbed. It discusses how the risks to data integrity, availability and confidentiality of patient information in the Paper-Based Kidney Dialysis System and the Electronic Renal Care Patient Management Network (RCPM) will be managed. Security measures recommended by the risk analyses are reviewed. A timeline summarizes the plans to implement these measures and the projected schedule of Phase II of Project Phoenix.

2. Security Measures

2.1 Paper-Based Kidney Dialysis System

The following countermeasures were recommended by the Risk Analysis of the Paper-Based Kidney Dialysis System (Annex **):

Countermeasure	Cost (rated from 1 to 10)
Move lab computer and printer to a less accessible area (R12)	Cost: 1
Lock filing cabinet with old patient records (R14)	Cost: 1 (minor inconvenience to staff)
Develop visitor sign-in/escort procedures (R3)	Cost: 1
Limit/disallow visitors in treatment area (R13)	Cost: 1 (minor discomfort to patients)
Lock PCs/terminals to desks (R15)	Cost: 1
Increase security awareness training for all staff (R7)	Cost: 2 (time for staff, time for trainer, educational materials)
Secure unit secretary's PC (R18)	Cost: 2 (some inconvenience to unit secretary)
Store patient charts in a locked, weatherproof cabinet (R16)	Cost: 3 (cabinet, minor inconvenience for staff)
Assign responsibility for security of patient records (R1)	Cost: 4 ($4000: raise of $2000/year + overhead)

Improve access control to unit (R5)	Cost: 4 (for access control without biometrics)
Reevaluate the unit policies on patient confidentiality and data security	Cost: 5
Install security cameras to monitor access (R10)	Cost: 6
Keep secure backup copies of all data (R11)	Cost: 8 (photocopying, extra storage space, time to copy and put in storage)

The investigators will present these findings, which pertain to the patient records at the control site at GUMC as well as to all paper-based records at the telemedicine site at Union Plaza, to the management of Total Renal Care, Inc. (TRC). TRC can then decide whether to implement each recommendation. While the costs of many of the recommended measures may seem low compared to the risks of not adequately protecting patient records, TRC must act according to its own strategic plan and cost/benefit analysis. The investigators will help TRC in carrying out its decisions in improving the security of patient records if TRC so desires.

At a later time, scheduled now for the 3rd quarter of Phase II, we will repeat the risk analysis of the Paper-Based Kidney Dialysis System so see whether and how any implemented security measures improved the overall security and confidentiality of the paper-based patient records.

2.2 Electronic Kidney Dialysis Patient Management Network

For the electronic patient records stored in the telemedicine system, the members of Project Phoenix bear some responsibility for the security of the data and have greater control over which recommended security measures will be implemented. The recommended countermeasures from the Risk Analysis of the Electronic Renal Care Patient Management Network (Annex **) and their costs are listed below:

Countermeasure	Cost (rated from 1 to 7)
Install virus detection/protection software (R8)	Cost: 1 ($100 : cost of the software)
Improve access control for off-site archive (R10)	Cost: 1 (cost of lock, minor inconvenience to users)
Enforce password management practices (R7)	Cost: 1 (minor inconvenience to personnel)
Control access to telemedicine application (R5)	Cost: 2 (access control mechanism)
Use encryption during transfer between telemedicine units (R3)	Cost: 2 (encryption algorithm, minor inconvenience)
Use encryption between data cartridge and archive over the Internet (R4)	Cost: 2 (encryption algorithm, minor inconvenience)
Require the use of audit logs (R6)	Cost: 3 (install audit mechanism, minor inconvenience)
Increase security awareness training for all staff (R1)	Cost: 3 (time for staff, time for trainer,

	educational materials)
Develop a preventive maintenance program for the telemedicine system (R9)	Cost: 4 ($100/month engineer's time = $1200)
Upgrade to Windows NT version as soon as possible (R12)	Cost: 6 (cost of upgrading to Windows NT, upgrading to higher Carelink version, installing and testing the system)
Recruit and train personnel to manage telemedicine unit (R2)	Cost: 7 ($37,000 cost of hiring additional person + cost of training)

For each of the following security measures, the investigators will research possible technical solutions and select a product or freeware program by the end of April, 1997. The selected solutions will be implemented and tested during May 1997. As these measures become operational, we will train the clinical and engineering staff as appropriate. More detailed scheduling information can be found on the timeline (Section 4).

Install virus detection/protection software
Improve access control for off-site archive
Enforce password management practices
Control access to telemedicine application
Use encryption during transfer between telemedicine units
Use encryption between data cartridge and archive over the Internet
Require the use of audit logs

Increase security awareness training for all staff
During the first week of May, 1997, the clinical staff will be trained on data security policies and procedures according to the Staff Training Outline (Annex **). To prepare for these training sessions, the investigators will complete the Policies and Procedure on Patient Confidentiality specific to Project Phoenix. They will also compile other training materials such as overheads and handouts to conduct the training sessions. These materials also will include the patient informational materials used as part of the informed consent procedure (Annex **) and GUMC and TRC policies.

Develop a preventive maintenance program for the telemedicine system
The investigators will develop preventive maintenance procedures, a schedule, and appropriate documentation for the regular maintenance of the telemedicine system during the 3rd quarter of Project Phoenix.

Upgrade to Windows NT version as soon as possible
Upgrading the telemedicine equipment to the Windows NT operating system and to the Windows NT version of the Carelink application is expected to make many of the above security measures much easier and more transparent to the user. For example, the new version of Carelink will include role-based access controls and automatic transaction logging. Therefore, it would be highly advantageous to upgrade the system as soon as

possible. However, delays in the delivery schedule of the new software and problems coordinating the upgrade may make it impossible to move to the Windows NT version any time soon. The investigators will continue to advocate the upgrade but, in the meantime, they will focus their efforts on other technologies to implement the recommended security measures as described above.

Recruit and train personnel to manage telemedicine unit
GUMC and TRC are in the process of recruiting a nurse who will manage the telemedicine equipment for all routine operations and minor maintenance. As soon as this person is hired he/she will be trained in the telemedicine unit's operations and the security policies and procedures of GUMC, TRC, and Project Phoenix. This process is intended to be complete by the end of the general training phase of the project, or around the first week of May, 1997.

Evaluate and address security implications of changing telecommunications service from T-1 to ISDN
After completion of the risk analysis of the RCPM, the project management team of Project Phoenix began considering changing the telecommunications service between telemedicine site from T-1 to ISDN. In as much as this changeover takes place, we will evaluate the security implications of such a change, determine additional security measures if necessary, and implement these measures.

3. Budget

3.1 Paper-Based Kidney Dialysis System

Move lab computer and printer to a less accessible area (R12)	$0
Lock filing cabinet with old patient records (R14)	$0
Develop visitor sign-in/escort procedures (R3)	$100
Limit/disallow visitors in treatment area (R13)	$0
Lock PCs/terminals to desks (R15)	$200
Increase security awareness training for all staff (R7)	$1000
Secure unit secretary's PC (R18)	$400
Store patient charts in a locked, weatherproof cabinet (R16)	$300
Assign responsibility for security of patient records (R1)	$4,000
Improve access control to unit (R5)	$5,000
Reevaluate the unit policies on patient confidentiality and data security	$5,000
Install security cameras to monitor access (R10)	$8,000
Keep secure backup copies of all data (R11)	$10,000
Total	$33,900

3.2 Electronic Kidney Dialysis Patient Management Network

Install virus detection/protection software (R8)	$100
Improve access control for off-site archive (R10)	$50
Enforce password management practices (R7)	$500
Control access to telemedicine application (R5)	$3,000
Evaluate and address security implications of changing telecommunications service from T-1 to ISDN	$1,000
Use encryption during transfer between telemedicine units (R3)	$1,000
Use encryption between data cartridge and archive over the Internet (R4)	$1,000
Require the use of audit logs (R6)	$2,000
Increase security awareness training for all staff (R1)	$2,000
Develop a P.M. for the telemedicine system (R9)	$1,200
Upgrade to Windows NT version as soon as possible (R12)	$15,000
Recruit and train personnel to manage telemedicine unit (R2)	$38,000
Total	$64,850

4. Timeline

(see attached)

Toolkit Section 4.6

Organizing Security Training

Introduction

When health care organizations require staff to follow strict policies, procedures, and practices for maintaining the confidentiality of patient records, they also assume responsibility for providing the necessary continuing education. The effort of health care organizations to inform staff about Universal Precautions in Blood-born Pathogens represents a good model to follow in security training. Health care organizations either purchase or prepare standard educational programs in Universal Precautions that occur regularly and which all staff must attend. Like Universal Precautions themselves, education in Universal Precautions composes part of any hospital's annual schedule of continuing medical education. Health care organizations should adopt the same approach to educating staff about issues in managing the security and confidentiality of patient information. CPRI has prepared the following booklet that outlines an approach to information security education. Sample materials and information about sources for obtaining kits follow the text of the CPRI Guidelines.

Guidelines

For

Information Security Education Programs

At

Organizations Using Computer-based Patient Records

Prepared by
CPRI Work Group on
Confidentiality, Privacy & Security

June 1995

Computer-based Patient Record Institute
Advancing health care through information technology

Guidelines
For
Information Security Education Programs
At
Organizations Using Computer-based Patient Records

Prepared by
CPRI Work Group on
Confidentiality, Privacy & Security

June 1995

Computer-based Patient Record Institute
Advancing health care through information technology

Computer-based Patient Record Institute
Advancing health care through information technology

Guidelines for Establishing Information Security Education Programs.
© Copyright 1996, by the Computer-based Patient Record Institute. All rights reserved.

No part of this publication may be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without permission in writing from the publisher.

Printed in the United States of America

This book was prepared camera-ready.

Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Record Systems

Overview

The Computer-based Patient Record Institute, Inc. (CPRI) has recognized the importance of providing for information security in the implementation of computer-based patient records. Therefore, the Work Group on Confidentiality, Privacy, and Security was established as one of the original work groups of the CPRI. The work group was chartered to encourage the creation of policies and mechanisms to protect patient and caregiver privacy and ensure information security. It is developing a series of security guidelines for organizations implementing computer-based patient record (CPR) systems.

The first in the series is the:

- *Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Record Systems*

This second in the series is:

- *Guidelines for Establishing Information Security Education Programs at Organizations Using Computer-based Patient Record Systems*

The remaining guidelines will address:

- Information security manager responsibilities and procedures
- Technological methods to identify and authorize access to computer-based patient record systems
- Assignment and control of used access identifiers
- Security audit functions and processes
- Application and system security functions

Need for Security Guidelines

Computer-based patient records offer the potential for achieving greater protection of health information over paper-based patient records. However, to ensure an appropriate and consistent level of information security for computer-based patient records, both within individual health care organizations and throughout the health care delivery system, formal information security programs must be established by each organization entrusted with health care information.

A complete information security program consists of policies, standards, training, technical and procedural controls, risk assessment, auditing and monitoring, and assigned responsibility for management of the program.

Acknowledgments

This document was prepared by members of the Project Team on Information Security Education Programs under the direction of Carol A. Romano, PhD, RN, FAAN, Team Leader. The co-chairs of the Work Group on Confidentiality, Privacy and Security (Kathleen Frawley, JD and Dale Miller) and Project Team leader are indebted to the many volunteers who participated in the work group meetings, provided input, and prepared and reviewed the drafts of this document.

Table of Contents

Introduction 1

Objectives 1

Scope 2

System security Issues 2
- Social Context 2
- Technical context 3
- Legal-Regulatory Context 3

Information Security Education Program 3
- Goals and Objectives 3
  - Involved individuals having access to health information 3
  - Management 3
  - Patients and general public 4
- Content 4
  - Suggested content for all involved individuals 4
  - Management 6
  - Patients and clients, and general public 7
- Methodologies 7
  - Instructional technologies and strategies 7
  - Sources of delivery 7
- Methods of Program Implementation 8
  - Strategies for developing training and education programs 8
  - Training and education programs categories 9
- Evaluation 9
  - Evaluation of teaching and learning 10
  - Evaluation methodologies 10
  - Evaluation of education effectiveness 10
  - Examples of methodologies 10

Summary 11

Glossary 12

References 14

Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Records

Introduction

While issues related to the privacy, confidentiality, and security of health information are not new, the context of handling such information electronically heralds the need to reexamine and reinterpret these issues. The cultural norms and traditional measures used to secure the privacy of paper-based health records may not be appropriate in the emerging environment of networks, telecommunications, and electronic superhighways. An information security education program is viewed as an important vehicle to sensitize individuals to these issues, increase their awareness, teach individuals to use the security features of computer-based patient record systems, and affect the implementation and management of appropriate information security practices.

Formal information security policies and procedures in organizations that handle health information are increasing and are acknowledged as important and necessary parts of emerging health care services. However, individual members of the organization must understand the value of the information entrusted to their care. They must believe that privacy and confidentiality are their responsibility. To a large extent, the organizational culture and management style significantly influence the degree to which individuals value and are concerned with protection of information.

A formal information security education program is one mechanism to assess, develop and maintain an individual's competence to meet the expectations, internal and external standards, and mission of the organization. The information security education training program should be designed to provide individuals with the expectations, knowledge, and skills related to information security. It should be strategically designed to address information security during all phases of staff development-orientation,- inservice education, and continuing education.

These guidelines are designed to assist large, multicenter organizations as well as solo practitioners in the design and implementation of information security education programs. The guidelines recognize and account for the complexities of the information security management concept in the framework of electronic communications and the issue of privacy and confidentiality. The information presented is intended to serve a widely diverse set of users working in widely diverse situations, including but not limited to vendors, contractors, students, volunteers, researchers, educators, caregivers, employers, employees, managers, providers, consumers, and insurers.

Objectives

The objectives of these guidelines are:

1. To inform all users about the complexity of system security issues and training needs.

2. To provide assistance in the development and implementation of information security education programs.
3. To promote consistency in the quality of system security awareness training.
4. To identify the responsibilities of all involved individuals for information security.
5. To provide a method to evaluate the outcomes of an organization's information security education program.
6. To contribute to the protection of the privacy and confidentiality of health information.

Scope

The information security education program is intended for all individuals and organizations involved with handling health data information -- at all organizational levels, including management, clinicians, patients, vendors, and the general public. Commitment to security must be made at the highest level of an organization and then emphasized throughout all levels. Education programs should be tailored to meet the needs of individuals and situations and may range from classroom lectures and workshops to written material adequately outlining the organization's security practices.

The scope of educational programs for information security should encompass the impact of information technology on issues of privacy and confidentiality. It should address required practices related to security that must be followed by each individual commensurate with the person's role. In addition, a special training component should address managers' and supervisors' responsibilities related to managing information security.

System Security Issues

Today's technology presents a multitude of security risks in addition to those readily recognizable and acknowledged, such as those related to the use of mainframe computers, minicomputer systems, and personal computers. These may also include but are not limited to digital dictation systems, fax machines, answering machines, cellular phones, couriers, and samples of work sent to vendors. In addition, human errors may account for a significant number of information security problems. Examples of human error include leaving computer devices unattended, incorrectly recording or transferring data, failing to monitor confidential facsimiles, and disregarding access code procedures.

The adequacy of practices in addressing current and future information management security concerns must be addressed in the following areas:

Social Context

The adequacy of current security practices in protecting the rights of all individuals must be determined. This includes the extent to which privacy can be maintained and the extent to which confidentiality may be compromised given the social interests, demands, and needs for patient/client information (i.e., third party payers, quality management, law enforcement agencies, etc.)

Technical Context

The adequacy of current security practices is of particular interest in light of the increased use of communication technology and computerization and the emergence of information highways. This results in increased vulnerability of information systems. With this risk, however, comes the benefit of increased ability to control part or total release of a complete record of health information.

Legal-Regulatory Context

The type and scope of the legal regulations and requirements at the Federal, state, and local levels have an impact on the organization's information security practices. In addition, information management standards of the Joint Commission on Accreditation of Healthcare Organizations address requirements for information security and information management.

Information Security Education Program: Goals and Objectives

The goals of an information security education program are to educate individuals regarding the need for security awareness, to improve information security practices, and to protect individual confidentiality.

The training program should be designed to stimulate learner participation to the greatest extent possible, should include a discussion of the learner's personal responsibilities for the success of the security program, and should include the objectives listed below, or variations thereof. Using these guidelines and existing laws, program content should address the following objectives:

Involved individuals having access to health information:

1. Examine the impact of technology on issues of privacy and confidentiality.
2. Identify types of information and information resources that need to be protected.
3. Identify who is responsible for system security and security management at each organizational level.
4. Identify existing system security practices.
5. Examine how information can be protected.
6. Identify threats to security and vulnerability of information.
7. Identify actions that can be taken to protect information security.
8. Communicate the consequences of system security breaches to involved individuals and to health care goals.

Management

1. Identify responsibilities for establishing information security education programs.
2. Identify existing system security practices.

3. Develop methods to assess, implement, monitor, and evaluate system security procedures and policies, and to investigate system security tracking methods and violations.
4. Differentiate between acceptable and unacceptable information management practices for the organization.
5. Examine the consequences of system security breaches to involved individuals, to patients and clients, and to health care goals.

Patients and general public

1. Identify individual rights and responsibilities related to information, confidentiality, storage, retrieval, privacy, access, disclosure, and use.
2. Identify basic system security practices relating to health care information.

Information Security Education Program: Content

The education program should be developed as a collaborative program with input from the education and training staff, system security staff, management, patients, and other involved individuals. At a minimum, it should contain the content listed below, or variations thereof.

Suggested content for all involved individuals includes the following.

1. Concepts of privacy, confidentiality, disclosure, system security, information security and integrity, including what constitutes a violation or breach and why breaches (intentional and unintentional) occur.

2. Impact of information technology on privacy, confidentiality, and security including:

    a. benefits, risks, and process changes related to computerization
    b. legislation and regulatory requirements
    c. code of ethics and professional obligations
    d. social interests and demands for health data
    e. policies, procedures, and expectations
    f. issues specific to remote access

3. Personal responsibility of trainees for information security management, and the extent to which scope and accountability vary within positions.

4. Sensitivity of health data and the type and degree of protection needed in relation to the role and context of the data and the role of the user.

5. Sensitivity of employee data and the type and degree of protection needed.

6. Types of threats to information security:

    a. Human error (erasures, accidental damage, deliberate acts, improper disposal of paper and disks, etc.)
    b. Nature (fire, water, lightning, earthquake, etc.)
    c. Technical (lack of backup, system failure, virus, loss of power, etc.)
    d. Deliberate (unauthorized disclosure, modification)

7. Methods of data protection.

    a. Physical security (environmental, installation)
        (1.) Area access controls
        (2.) Accountability controls
        (3.) Equipment enclosures, lockdown, locks
        (4.) Fire protection systems
        (5.) Encryption
        (6.) System security software (mainframes, networks etc.)
    b. Technical controls (i.e., what data may be accessed or removed from original location to remote areas)
        (1.) Disaster recovery
    c. Operational security (the who, which, what, where, when, why, and how often actions):
        (1.) Standard operational policies and procedures
        (2.) Accountability controls
        (3.) Nondisclosure contracts and confidentiality statements
        (4.) Regular scheduled inservices
        (5.) Definitions of levels of information security
        (6.) Need-to-know basis
        (7.) Backing up data
        (8.) Audit trails
    d. Individual responsibilities
        (1.) Knowledge of organization's information security policies and procedures
        (2.) Collection of valid, accurate data
        (3.) Challenging unauthorized users
        (4.) Protection of passwords, codes, etc.
        (5.) Reporting security irregularities
        (6.) Protection of hardware and software
        (7.) Attending inservices and participating in continuing quality improvements

8. Consequences and sanctions of security breaches to the involved individual, the organization, patients, and the health care goals.

9. Methods of continuous review and assessment for quality improvement.

Suggested content for managers includes the following in addition to the above content.

1. Management's responsibilities to establish information security education programs for all involved individuals as well as the general public. Programs may be formal and/or informal. Content may include, but is not limited to:

    a. Initial orientation of individuals new to the organization (to include certification and credentialing programs)
    b. Volunteer, student, or temporary employee orientation
    c. Vendor and contractor orientation (sales, maintenance, etc.)
    d. Contract employee orientation
    e. Outreach programs
    f. Annual inservices; and reviews
    g. Continuing education programs
    h. Statement regarding confidentiality and security expectations in policy and personnel manuals
    i. Employee and patient handbooks
    j. Management of access (assignment and termination of access)
    l. Signed agreement related to understanding of confidentiality and information security responsibilities.

2. Strategies for assessing, implementing monitoring, and evaluating information security policies and practices include, but are not limited to:

    a. Implementation
        (1.) develop and establish written policies and procedures (a plan for protection, sanctions for violations, training requirements)
        (2.) provide training in policies and procedures
        (3.) define access level for each job category and type of involved individuals
        (4.) develop confidentiality and security agreements and contracts
        (5.) track and monitor access
        (6.) develop adequate job descriptions or elements for security management staff
    b. Monitor and evaluate effectiveness of training.
    c. Conduct risk analysis to monitor and evaluate effectiveness of security practices.

3. Development of authorized and unauthorized information practices for all types of individuals. This may include addressing rights and responsibilities in terms of specific internal and external activities of the organization. It alto includes developing guidelines for the release of information to third parties.

4. Management's responsibility to be knowledgeable about emerging technologies that may affect security techniques. Managers need to be knowledgeable about regulatory activity that may affect security programs in terms of responsibilities and procedures and need to assure that public information and education are adequate.

5. Establishment of an employee suggestion program to improve security practices with appropriate incentives and awards.

6. Legal requirements for information security and the criminal or civil penalties that may result from inappropriate disclosure.

7. Appropriate and consistent responses and/or disciplinary actions following security violations.

Suggested content for patients and clients, and general public includes the following:

1. Rights and responsibilities of patient and public in terms of ownership of information, use, disclosure, and access.

2. Basic system security practices used by organizations to protect information.

3. Responsibilities to make informed decisions.

Information Security Education Program: Methodologies

Methodologies utilized during the information security education program should be designed to address the specific objectives identified for each target audience. The program should challenge learners to participate in a critical and productive discussion of the issues. Adequate time should be allotted for questions and answers, and training times should be flexible to accommodate the learners' needs.

Examples of instructional technologies and strategies

1. Discussion, case studies
2. Scenarios or role playing
3. Audiovisuals, videotaped instructions
4. Computer-based training
5. Interactive technology
6. Handouts, written materials, references, and self study information
7. Briefings and lectures during staff meetings
8. Reviews during performance evaluations
9. Network (e-mail) briefings, Internet

Sources of delivery

1 Professional health care organizations
2. Incorporate into a core curriculum for healthcare workers
3. Policy makers (internal and external)
4. Professional and technical staff
5. Contractor

6. Self-study programs

Methods of Program Implementation

There are many different ways to implement an information security education program, depending on the size of the organization, the status of existing policies and security programs, available resources, and above all, level of management commitment. In a solo practitioner's office, the training could consist of a brief statement regarding the needs and current proposed level of security in the office, a question and answer period, and signed statements of understanding and nondisclosure. On the other hand, in a large, multicenter organization, the implementation of an effective information security education program might require hiring additional training staff or a contractor.

Regardless of the size of the organization, the strategies and categories listed below should assist in the implementation of the program.

Strategies for developing training and education programs

1. Review and revise existing policies as appropriate or develop new policies as needed to assure compliance with regulatory requirements

2. Examine current educational process

   - Redesign training and education as appropriate in order to facilitate system, organizational, follow-up, and public awareness

3. Develop long-range training and education strategic plan
4. Conduct learning needs assessment

5. Assign training and education responsibilities

6. Conduct resource inventory
   a. Identify what equipment and space is available
   b. Identify internal and external human resources within the organization and the community
      (1.) educators
      (2.) peer-to-peer education
      (3.) vendors and contractors
   c. Budget funds and evaluate costs of setting up programs

7. Develop management consensus on content to be taught and use of confidentiality and security agreements

8. Plan new employee and continuing training and other education processes

9. Provide training and education stratified by job description, department, level of access, type of customer and user

10. Define in the information security guidelines the content, frequency of training, specific training and education programs and material.

11. Conduct continuing evaluation of training and/or education.

12. Conduct continuing evaluation of security practices

13. Use results of evaluation and audits

Training and education program categories

1. First-time training and/or education

    a. Conduct training and/or education at two levels:
        (1.) generic institutional level
        (2.) specific to job function level
    b. Document trainee attendance
    c. Grant access only after training is completed and agreements are signed
    d. Focus on concrete examples
    e. Use appropriate outside resources
    f. Choose attention-getting themes, (e.g., patient-centered focus)

2. Continuing education and training

    a. Renew confidentiality and security statements and inservices annually
    b. Conduct continuing awareness campaigns to provide organizational reinforcement
    c. Ensure familiarity with specially protected information
    d. Make information security training a precondition for any credentialing processes
    e. Focus on training as part of risk reduction strategy
    f. Identify champion of security awareness and offer awards and/or incentives
    g. Conduct patient/client surveys that include questions regarding privacy and confidentiality Give feedback to staff (surveys should be done with concepts of reliability and validity incorporated into the design and preparation of a survey)

Evaluation

Evaluation studies should be conducted to determine the value of each individual information security education program or offering as well as the effectiveness of the overall information security education program. Evaluation studies assist organizations in determining the effectiveness of current security practices, in establishing administrative priorities, and in determining program directions for improvement.

To be effective, evaluation studies are incorporated as a component of the strategic education and training program and conducted on a continuing basis.

Evaluation of *teaching and learning*

Evaluation of individual information security education programs and/or offerings should include the following criteria.

1. Learner achievement of program objectives
2. Learner achievement of personal objectives
3. Teaching effectiveness of faculty (trainers)
4. Relevance of content to objective and/or job performance (i.e., can the learner apply the information to their practice?)
5. Appropriateness of faculty (trainers)
6. Appropriateness of teaching methodologies
7. Appropriateness of the teaching/learning environment
8. Recommendations for improvement

Examples of *evaluation methodologies for individual information security programs and/or offerings:*

1. Participant evaluation teams (focus group) sessions
2. Questionnaires
3. Group discussions
4. Tests
5. Simulations and case study reviews

Evaluation of education effectiveness

Evaluation of the total information security education program should be performed. Total program evaluation refers to the educational and administrative initiatives. The type of program evaluation method selected will depend on the organization's current needs and available resources.

Examples of methodologies for evaluation of the total program:

1. Quality improvement risk assessments
2. Comparison of number and severity of security violations with pretraining statistics to assess levels of improvement
3. Pattern analysis methods
4. Discrepancy evaluation models
5. Audit evaluation models
6. Impact evaluation models

Summary

A formal information security education program should be a major and supportive factor in the establishment of organizational and individual commitment to improved information security practices. Management's responsibility is to provide and promote security awareness and training.

Glossary

Most terms in these guidelines are intended to be interpreted according to their generally accepted usage and meaning. The following terms have been defined to help add clarity to their usage in this document.

Access to information. The ability to enter, view, or modify information. Access includes the ability to copy or print information as well as the ability to cause it to be transmitted via a computer network or facsimile machine.

Breach of Security. Any action by an authorized or unauthorized user which results in a negative impact upon the data in the system or the system itself, or which causes data or services within a system to suffer unauthorized disclosure, modification, destruction, or denial of service.

Caregiver. An individual who directly or indirectly provides health services, the goal of which is to heal, promote health, and improve the well being of another individual.

C**onfidentiality.** "The status accorded to data or information indicating that it is sensitive for some reason, and that therefore it needs to be protected against theft or improper use and must be disseminated only to individuals or organizations authorized to have it." (Ball and Collen, 1992).

Confidentiality is the professional and/or contractual duty of healthcare providers to safeguard the privacy of any patient/client information regardless of how it is acquired, collected, stored, processed, generated, retrieved, or transmitted in a healthcare institution (Waters and Murphy 1979; Romano 1987; Griesser 1989).

Data Integrity. The soundness or completeness of the data that are being used. Data integrity can be maintained by implementing security measures, by implementing procedural controls, by assigning responsibility, and by establishing audit trails (Schechter, 1988; Ball and Collen, 1992)

Data Security. The protection of data from accidental or intentional disclosure to unauthorized persons and from unauthorized alteration. Techniques for security include software and hardware features, physical measures such as locks, badges, etc., and an informed, security-conscious staff (Schraffenberger 1988; Ball and Collen, 1992).

Disclosure. The release of information to third parties within or outside the organization from an individual's record with or without the consent of the individual to whom the record pertains.

Information Security. The process of safeguarding information; generally refers not only to safeguarding confidentiality but integrity of data, unauthorized disclosure, modification, or destruction.

Information Security Education Program. The systematic, defined method to provide information and to teach skills related to all activities of the organization related to information

security. A complete information security education program addresses policies, standards, training, controls, risk assessment, auditing and monitoring, and assigned responsibility for management of the program.

Information Security Program. All activities of the organization related to information security. A complete information security program consists of policies, standards, training, technical and procedural controls, risk assessment, auditing and monitoring, and assigned responsibility for management of the program.

Involved Individuals. Organizations or persons involved in the handling of health information. Includes but is not limited to employees, employers, managers, providers, consumers, insurers, vendors, contractors, volunteers, students, researchers, educators, and clinicians.

Organization. Anyone or any entity who collects, stores, transmits, or otherwise processes health care information.

Patient Information. Refers to data collected about or related to the health status and health care of a specific identifiable individual.

Privacy. The right of an individual to be left alone, to withdraw from the influence of his/her environment; to be secluded, not annoyed, and not intruded upon by extension of the right to be protected against physical or psychological invasion or against the misuse or abuse of something legally owned by an individual or normally considered by society to be his or her property (Westin 1976; Ball and Collen 1992). Privacy relates to the decision of an individual to determine how much personal information to share.

System Security. Protection from unauthorized access, including provision for hardware, software, communications, and system users and uses determinations based on organizational computer security programs (Martin 1983; Ball and Collen 1992).

References

Ball, M.J. and Collen, M.F. (Eds.) 1992. Aspects of the Computer-based Patient Record. New York: Springer-Verlag.

Computer-based Patient Record Institute, "Guidelines for Establishing Information Security Policies at Organizations Using Computer-Based Patient Records. Workgroup on Confidentiality, Privacy, and Legislation. 1995.

Griecser, G. (1989). Data protection in hospital information systems: 1. Definition and overview. Implementing Health-care Information Systems. New York: Springer-Verlag.

Hannah, K.J., Ball, M-J. and Edwards, MJA. (Eds) (1994). Computers in Health Care: Introduction to Nursing Informatics. New York: Springer-Verlag.

Kelly, K.J. (1992). Nursing Staff Development: Current Competence, Future Focus. Philadelphia: J.B. Lippincott Company.

Madsen, W. (1992). Handbook of Personal Data Protection. New York: MacMillan Publishers.

Romano, C.A. (1987). Privacy, confidentiality, and security of computerized systems: The Nursing responsibility. Computers in Nursing, 5(3): 99-104.

Schechter, K.S. (1988). Conversion issues and data integrity: A consultant's perspective. Topics in Health Record Management. -Q(2): 62-69.

Schraffenberger, L.A. (1988). Practice bulletin, data security. JAMRA , 59.(8): 46-47.

Shaffer, S.L. and Simon, A.R. (1994). Network Security: Boston: AP Professional.

Waters, K. and Murphy, G. (1982). System Analysis and Computer Applications in Health Information Management. Silver Spring, MD: Aspen Systems.

Westin, A. (1976). Computer Health Records and Citizen Rights. National Bureau of Standards, Monograph 157. Gaithersburg, MD: National Bureau of Standards, 348.

CPRI Members

3M Hlth Info Sys
Adventist Hlth Sys/Sunbeft
ALLTEL Info Svcs - Hlthcare Div
Amer Acad of Family Physicians
Amer Acad of Pediatrics
Amer Assn for Med Transcription
Amer Board of Family Practice
Amer College of Physicians
Amer Hlth Info Mgmt Assn
Amer Hospital Assn
Amer Med Informatics Assn
Amer Medical Assn
Amer Org of Nurse Executives
Andersen Consulting, LLP
Arkive Information Systems
Assn of Operating Rm Nurses
Chi Systems
Coll of Amer Pathologists
Coll of Hlth Care Info Mgmt Execs
Columbia/HCA Hlth care
Ctr for Hlth Care Info Mgmt
Ctrs for Disease Control & Prev
Dept of Veterans Affairs
Dynamic Hlth care Tech
Eli Lilly and Company
Ernst & Young, LLP
Glaxo Wellcome
Group Hlth Assn of Amer
Harvard Comm Hlth Plan
HBO & Company
Hlth Industry Mnfrs Assn
Hlth Level Seven
Healthdyne
HealthVISION Corp
Inst for Clin Sys Integ
InterPractice Sys
JCAHO
Kaiser Permanente
Management Systems Assoc
Mayo Foundation
Medic Alert Fnd US
Medical Connections
Medical Records Inst
MedicaLogic
Medicus Systems
Motorola
Natl Assn of Chain Drug Stores
Natl Cncl for Pres Drug Progs;
NC Hlth Care Info & Comm AlInce
NEON Hlth care Softmre
Northwestern Memorial Hosp
Oceania
PHAMIS
Physician Micro Systems
Prudential Insurance Co
SIDOCI Enr
Sisters of Mercy Hlth Sys
SoftMed/HIS
Systems Plus
The Permanente Med Group
ThetaPro
Unitron Med Comm
Univ Hlth System Consortium
Univ of IA Hosp & Clinics
Univ of VA Hlth Sci Ctr

CPRI is a nonprofit membership organization committed to advancing improvements in health care quality, cost, and access through routine use of information technology. CPRl serves as a neutral forum for bringing the diverse interests of all health care stakeholders together to develop common solutions.

CPRI functions primarily through the voluntary work of its work groups. All individuals are invited to participate in one of the following:

- Work Group on Codes & Structures
- Work Group on Confidentiality, Privacy & Security
- Work Group on CPR Description
- Work Group on CPR Systems Evaluation
- Work Group on Professional & Public Education

Toolkit Section 4.6.2

Sample Training Materials

The sample slides and instructor's guide that follow are intended to provide a starting point for persons who are developing a health care information confidentiality, protection, and security training program. In tailoring these materials to your needs, consider the following:

Audience:

- Who will you be addressing? If you use technical terms for one set of students, you might completely lose another. Modify your vocabulary accordingly.
- If English comprehension is an issue, consider printing materials or conducting sessions in another language.
- Information Technology staff need training too!
- Don't forget administration, executives, and the auditors!

Logistics:

- Scale the presentation to fit available time. You may have a 90-minute block during a staff meeting or a 10-minute session during break. Any opportunity for training, no matter how small, should not be missed, but try to be sure staff gives this the time it deserves! Minimize potential disruptions.
- Don't forget shift workers. You may have to schedule some sessions at 9:00 p.m. or 4:00 a.m.
- If you are conducting noontime sessions, invite class to bring their lunches.
- Cookies/snacks are always an incentive!
- Be flexible. Even if you cannot get the time you want, you may be able to negotiate for the time you need. Managers are generally short-staffed and will appreciate any effort you make to accommodate their requirements.

Methods:

- Vary presentation tools – mix slides, flip charts, videos, and posters.
- Consider putting slides on workstations and distributing presentation materials to create self-study modules.
- Include anecdotes and real-life examples of what can happen. Case studies and "what's wrong with this situation?" can also be helpful.
- Seek class participation. Ask for examples of poor security practices and solicit questions.
- If you want to use humor, be careful. Remember this is a topic that you want to have taken seriously.

Resources:

- Other organizational staff can be called upon to assist in developing or delivering the training, e.g. Human Resources and Legal Departments, to ensure that the policies are sound and fair.
- Training – to help develop or administer the training.
- Internal Audit – to ensure that policies are fully implemented and that staff are in compliance.
- Clinical leadership – to include training components that are relevant to clinicians and ensure that clinicians attend training and abide by policies.

Evaluations of programs:

- Use tests to assess student understanding (clear this with Human Resources to avoid bargaining unit issues)
- Ask students to evaluate the program and what they have learned

Audit and compare the number of security incidents pre- and post-training.

Toolkit Section 4.6.2.1

Instructor's Guide to Slide Presentation on Protecting Patient Information

This document provides background for an information confidentiality, protection, and security training session presented in a classroom setting.

Title (slide 1) -

Introduce yourself, and tell briefly what the purpose of the class is.

What is information? (slide 2) -

This provides the basic definition of "information."

Why protect information? (slides 3-5) -

Discuss reasons for protecting information: what information is used for and why it needs to be treated with the same - or greater - care and respect as any other organizational asset. Stress that everyone has a role in information protection.

Ethics, Law, and Regulation (slides 6-9) -

Discuss the ethical and legal reasons for protecting information, and connection between protection, confidentiality, and privacy, i.e.,

- **"**Confidentiality" is the practice of permitting only certain authorized persons to look at or use information. Information is kept confidential if its general knowledge could be used to harm someone (example: causing public embarrassment by revealing a medical condition) or something (example: causing loss of revenue by revealing business plans). Any type of health care information that can be linked to an identifiable person must ALWAYS be considered confidential and treated as such.

- "Privacy" refers to a person's right to keep certain personal information to him or herself, and to assume that the information will not be disclosed to others or used inappropriately without his or her permission. Clinicians and other health care staff who access or use someone's personal information guard the individual's right to privacy by following practices that ensure the information remains confidential.

Patients may or may not be allowed to review their own health care records in accordance with state law. Health care information may not be disclosed to any other party (including family members) without the consent of the patient. Minor children may also have the right to keep their records concealed from their parents. This is especially true when regarding treatment for STDs, contraception, etc.

Some information may be need to be released outside of the health care entity, to authorized parties, in accordance with law, regulation, contractual agreement, and under rules specified in organizational procedures.

While slide 9 is displayed, remind students that the patient's right to privacy may have first been officially recognized by Hippocrates some 2400 years ago. Also discuss your state's health care law, regulation, accreditation (by JCAHO and/or NCQA), pending Federal standards under HIPAA.

What are threats to information? (slide 10) -

Information is subject to a variety of threats. Confidentiality and patient privacy is at risk when information is accessed or possessed by an unauthorized party, or is inappropriately disclosed. Health care information that is inaccurate or is missing can lead clinicians and staff to make decisions with possibly tragic consequences**.**

What are the sources of threats? (slides 11-13) -

Threats come from many sources - internal and external; human- and machine-based. Some security incidents are purely accidental and result from human error, lack of training, or lapses in judgement. Incidents involving outsiders, such as "hackers," occur least frequently but are best publicized.

What can happen? (slide 14) -

This is one place to tell "horror stories" of what can happen when information protection controls are lacking - or even when they are not. Many health care organizations have been sued by patients who contended that their personal or medical information was inappropriately disclosed or used. Costs of this type of litigation are not only measured in dollars, but also in the bad public relations and loss of consumer confidence which result.

Two well-know examples:

- *A rumor began that patient mental health information collected by Harvard Community Health Plan could be easily accessed by unauthorized persons. HCHP had to do extensive damage control, including full-page ads in the* Boston Globe.

- *A worker in a Florida hospital took her teenaged daughter to work with her. While there, the daughter accessed computer records of patients who had recently been seen there. The daughter then called patients on the list and told them that they had had positive tests for HIV and pregnancy. One person the daughter called attempted suicide. The mother was discharged and the daughter reportedly served time in juvenile hall.*

What are ways to protect information? (slide 15) -

Lists control mechanisms to be discussed in following slides.

Policy/Administrative Controls (slides 16-17) -

A number of policies may be established to express management's intent and commitment to information confidentiality and protection. At this point, discuss those policies in effect within your organization. If failure to comply with policy is grounds for disciplinary action, be sure to state that as well.

If information confidentiality and protection is governed by a specific group within the organization, name the group and describe its membership. Include a contact party if possible.

Describe the types of administrative controls in place, plus where to go for additional information regarding procedures for issuing user accounts, etc.

Physical Controls (slides 18-19) -

Explain/give details for each of the physical controls that are used in your organization:

Servers, routers, and other equipment must be protected from damage, theft, and misuse - and not only because of their monetary worth. Servers can contain patient information that must be closely guarded. Routers can be manipulated so that messages are sent to unintended parties. These machines must be closely controlled so that only authorized maintenance staff are allowed access to them.

Hard copies, diskettes, CDs, and tapes containing confidential information must be locked up when not in use.

Before storing confidential information on a hard drive, an individual must make certain that all parties that can access the drive (and the directory on which the information resides) are authorized users of the information. Any confidential information stored on a hard drive should be secured via software access controls and/or encrypted with a key known only to authorized parties.

Confidential hard copy must be destroyed by shredding on site or kept secured until it can be removed for destruction by a bonded disposal firm. Many corporate secrets have been uncovered by "dumpster divers" looking through intact paper trash.

Deleting a file from a diskette, CD, or hard drive does not remove the information. Confidential information should be written over to ensure that it is unrecoverable. There are utilities available for this purpose.

Persons using laptops must take special precautions to protect against theft of both the equipment and data. Confidential data should not be stored on the hard drive unless it is encrypted. Diskettes, access tokens, dial-in numbers, encryption keys, etc. should not be stored in the same case as the computer.

Software Controls (slides 20-21) -

Explain/give details for each of the software controls that are used in your organization:

Changing passwords regularly and creating hard-to-guess passwords helps deter masqueraders, or persons who login under someone else's identity. Suspending user accounts after three unsuccessful login attempts also helps to deter masqueraders.

If an individual no longer requires a user account, the account should be deleted immediately. However, management may forget to contact security administration. Therefore, any user account that is inactive for a certain period of time should be suspended automatically to prevent its use by a masquerader or individual who is no longer authorized.

If an individual logs in to a workstation then leaves it standing idle he or she risks becoming the victim of a masquerader because anyone can use the device. Although an unattended workstation should be logged off by the person who logged in, a good fallback measure is to have the session set to automatically time out after a specified period.

Access to systems and information is based upon an individual's job function and "need to know." For example, a physician has information requirements that a clerk does not, therefore their levels of access are different.

Workstations, networks, and information can be seriously damaged by malicious computer program code such as viruses. Products to scan for and eradicate viruses should be installed on every workstation and/or server.

Computer programs should be so designed that user errors will not cause serious damage such as deletion of entire records or files.

Critical systems and information are automatically copied on a regular basis, and the copies are stored on another medium and/or offsite. That way, in the event of a machine or software failure, the system and information can be restored with a minimum of disruption to operations.

Safe Information Practices (slides 22-26) -

Review these rules and practices:

The most important rule: always make sure that anyone to whom you communicate confidential information is authorized to receive it and has a business "need to know."

When communicating by phone or in person, first ensure that the other party (or parties) is authorized to receive the information. This is especially important to remember when answering calls from patients or family members. For example, callers will sometimes pose as the patient or family member to gain information that the patient wishes to keep private.

Ensure that phone and face-to-face conversations and meetings cannot be overheard. Use caution with cellular phones because calls can sometimes be heard by other parties.

Printed documents that contain confidential information should not be kept in areas accessible to unauthorized persons.

Before releasing any information to an external party, consult organizational procedures and contact management, public relations, etc., as appropriate.

Faxing documents is a risk to confidentiality. Some fax machines are able to encrypt the information for decoding by the destination machine; however, faxing is not as secure a means of communication as hand-carrying or mailing a document. Persons who fax confidential documents should take precautions when dialing the phone number; and should verify that the document is received by the appropriate party. Persons who know that they have a confidential incoming fax should try to be at the fax machine when it arrives. Fax machines should not be in areas accessible to the general public.

Every individual is responsible for the activities that are conducted under his or her user account. Therefore, sharing user accounts or passwords IS PROHIBITED.

Work areas should be arranged so that monitor displays are out of the view of authorized persons, especially the general public.

Individuals should exit to a menu screen or generic display after completing a confidential transaction - don't leave confidential information displayed.

Sign off when leaving the work area.

Everyone is responsible for information security! (slides 27-29) -

Any person who does business with or on behalf of the organization as an employee, contract employee, student, or volunteer must:

- Understand the reasons for confidentiality and agree to abide by confidentiality policies and procedures
- Keep confidential information confidential at all times
- Report suspected or known breaches of confidentiality to the management or information security administration

In addition to the above, managers are to:

- Report staff changes such as terminations and transfers to information security administration immediately
- Inform staff of their responsibilities regarding confidentiality and information protection
- Include information confidentiality and protection compliance as a part of regular job duties and performance criteria
- Most importantly, SET A GOOD EXAMPLE for staff to follow!

Questions? (slide 30)

Slide 1

Information Security: It's up to YOU!

[Name of Presenter
and Organization]

[Logo]

1

Slide 2

What is “information”?

- Information is knowledge or intelligence obtained from facts or data.
- Its value is determined by the person or organization who possesses it.
- It can be priceless or worthless.

2

Slide 3

Why protect information?

- Information is an asset.
- It takes time and costs money to gather or produce information.
- Information gives businesses competitive advantage.
- Incomplete or inaccurate business information can lead to poor decisions and loss of revenue.

3

Slide 4

Why protect information?

….HOWEVER…..

In health care, the accuracy and completeness of information is even more critical. Incomplete or inaccurate health care information can lead to misdiagnoses, improper treatment, and other potentially

life-threatening situations!

4

Slide 5

Therefore, it is up to **EVERYONE** who works in health care - either as part of the patient care team or as another type of resource - to learn, understand, and practice

INFORMATION SECURITY.

5

Slide 6

Ethics, Law, and Regulation

Suppliers of health care are morally, ethically, and legally obligated to create a secure environment for the information they gather, and thus help to preserve its confidentiality and protect patient privacy.

6

Slide 7

Ethics, Law, and Regulation (cont'd)

"Confidentiality"

Confidentiality is the practice of permitting only certain authorized individuals to access information, with the understanding that they will disclose it only to other authorized individuals.

7

Slide 8

Ethics, Law, and Regulation (cont'd)

"Privacy"

Privacy is the individual's right to keep certain information to him or herself, with the understanding that the information will only be used or disclosed with his or her permission.

8

Slide 9

Ethics, Law, and Regulation (cont'd)

Examples:

- Hippocratic Oath
- [State code]
- JCAHO and NCQA standards and review criteria
- HIPAA

9

Slide 10

What are threats to information?

Unauthorized or inappropriate:

- access
- possession
- disclosure
- modification
- destruction

…both accidental and intentional.

10

Slide 11

What are the sources of threats?

Employees

- Unintentional - acting in good faith
- Intentional - disgruntled or unhappy staff
- Software errors

11

Slide 12

What are the sources of threats? (cont'd)

Environment

- Equipment failure
- Fire, flood, earthquake

12

Slide 13

What are the sources of threats? (cont'd)

Outsiders

- Ex-employees
- Hackers, "social engineers"

13

Slide 14

What can happen?

- Many individuals have successfully sued healthcare institutions and caregivers for breaches of confidentiality.
- Lawsuits are costly - not only in dollars, but in intangibles such as goodwill.
- [Cite examples]

14

Slide 15

What are ways to protect information?

- Policy/Administrative Controls
- Physical Controls
- Software Controls
- “Safe Information Practices”

15

Slide 16

Policy/Administrative Controls

Company Policy

- Human Resources policies
- Confidentiality Agreements (renewed regularly)
- accreditation/licensing
- Information Technology policies
- Governance of policies and standards

16

Slide 17

Policy/Administrative Controls (cont'd)

Administrative Controls

- requesting, creating, and controlling user accounts
- assigning user access rights
- modifying or deleting accounts and access rights when users no longer have a "need to know"
- responsibility for administrative controls.

17

Slide 18

Physical Controls

- restricted access to servers, routers, and other equipment
- secured (locked up) media (paper, diskettes, CDs)
- restricted access to hard drives containing sensitive information
- uninterruptible power supplies and backup systems

18

Slide 19

Physical Controls (cont'd)

- confidential hard copy shredded on-site or stored in a locked area for removal and destruction by a bonded disposal service
- diskettes and CDs erased in a manner that prevents recovery of data.
- laptop users take special precautions.

19

Slide 20

Software Controls

- passwords are changed often and are so constructed as not to be easily guessed
- suspension of user accounts after [*n*] attempts to login with an incorrect password
- automatic suspension of user accounts after [*n*] days of non-use.
- automatic time out of workstations after [*n*] minutes of non-use

20

Slide 21

Software Controls (cont'd)

- access granted to systems and information according to individuals' job functions
- current versions of anti-virus software run on all workstations/servers
- data are protected from accidental misuse
- automatic backup of critical systems.

21

Slide 22

"Safe Information Practices"

"RULE NUMBER ONE":

Any person to whom information is communicated must:

- be ***authorized*** to receive the information and
- have a "***need to know.***"

22

Slide 23

"Safe Information Practices" (cont'd)

- confidential subjects are discussed only in a private setting
- cautious use of cellular phones for confidential conversations

23

Slide 24

"Safe Information Practices" (cont'd)

- hard copy is secured/kept out of sight of unauthorized persons.
- written organizational procedures give complete instructions for release/disclosure of information

24

Slide 25

"Safe Information Practices" (cont'd)

- faxing is done with caution:
  - number verified and dialed carefully
  - recipient informed of pending transmission
  - receipt verified as appropriate.

25

Slide 26

"Safe Information Practices" (cont'd)

- SHARING USER ACCOUNTS OR PASSWORDS IS PROHIBITED
- workstations are placed so that displays cannot be seen by unauthorized persons
- users exit to menus or generic displays after completing confidential transactions
- users log off when leaving the work area.

26

Slide 27

Everyone is Responsible for Information Security!

All staff:

- know what data is considered confidential
- understand confidentiality policies
- comply with confidentiality policies
- report suspected or known breaches of confidentiality to management or security administration immediately.

27

Slide 28

Everyone is Responsible for Information Security! (cont'd)

In addition, managers will:

- report staff changes (terminations and transfers) to security administration immediately
- educate staff in their responsibilities regarding information security

28

Slide 29

Everyone is Responsible for Information Security! (cont'd)

In addition, managers will (cont'd):

- include security and confidentiality compliance as part of job duties and performance appraisals
- *SET A GOOD EXAMPLE!*

29

Slide 30

Questions?

30

Toolkit Section 4.6.3

Contact Information about Conferences on Information Security

The following Web sites and contact addresses provide information about seminars, conferences, and other meetings being sponsored to educate the health care professions about information security.

American Health Information Management Association (AHIMA)

1. Web site: www.ahima.org "Products and Events"
2. Address: 919 N. Michigan Ave, Suite 1400, Chicago, IL 60611
3. Telephone: (312) 787-2672
4. Fax: (312) 787-9793

American Medical Informatics Association (AMIA)

1. Web site: www.amia.org
2. Address: 4915 St. Elmo Avenue, #401, Bethesda, MD 20814
3. Telephone: (301) 657-1291
4. Fax: (301) 657-1296

Center for Healthcare Information Management (CHIM)

1. Web site: www.chim.org "Events Calendar"
2. Address: 3800 Packard Road, #150, Ann Arbor, MI 48108
3. Telephone: (734) 973-6116
4. Fax: (734) 973-6996

College of Healthcare Information Management Executives (CHIME)

1. Web site: http://chime-net.org "Services CHIME Courses"
2. Address: 3300 Washtenaw Ave, #225, Ann Arbor, MI 48104
3. Telephone: (734) 665-0000
4. Fax: (734) 665-4922

Computer-based Patient Records Institute (CPRI)

1. Web site: www.cpri.org
2. Address: 4915 St. Elmo Avenue, #401, Bethesda, MD 20814
3. Telephone: (301) 657-1291
4. Fax: (301) 657-1296

Healthcare Information Management Systems Society

1. Web site: www.himss.org "Education"
2. Address: 230 East Ohio Street, Suite 500, Chicago, IL 60611-3269
3. Telephone: (312) 664-HIMS or (312) 664-4467
4. Fax: (312) 664-6143

Joint Healthcare Information Technology Alliance

1. Web site: www.jhita.org "Calendar" and "Education Programs"

MIS Training Institute,

1. Web site: www.misti.com
2. Address: 498 Concord St., Framingham, MA 01702-2357
3. Telephone: (508) 879-7999
4. Fax: (508) 872-1153

Tunitas Group

1. Web site: http://home.earthlink.net/~tunitas
2. Address: 728 Augusta Drive, Moraga, CA 94556
3. Telephone: (925) 631-1244
4. Fax: (925) 631-6640

Toolkit Section 4.7

Additional Resources

The American Health Information Management Association has produced a ready-made tool for instructing health care workers about data security. Written by Mary Brandt, MBA, RRA, CHE and Sandra R. Fuller, MA, RRA, *Program in a Box: Information Security: Protecting Paper-and Computer-based Health Information* covers the major issues and provides a complete, polished general presentation on maintaining privacy and confidentiality.

Description of Contents

Complete 60 to 75 minute presentation "to educate… health care professionals about privacy and confidentiality issues…" The Packet contains paper documentation, overhead transparencies, and two 3 ½ inch floppy diskettes containing documentation. The packet is divided into three sections:

1. **Participant Materials:** This section is a complete handout for the participant. It is copy ready and can be bound by staple, spiral, or notebook format. It includes the following:
   Section 1: Copies of security presentation overheads printed in standard PowerPoint format of three slides to a page with notes section in right hand column. Although no PowerPoint slideshow is enclosed, the overheads can easily be put into a PowerPoint or other slide presentation format.
   Section 2: Sample Staff Confidentiality agreements
   Section 3: Sample Contractor or vendor confidentiality agreements
   Sample Electronic data interchange Non-disclosure agreement
   Section 4: Information security resources
   Section 5: Selected readings in information security

2. **Presenter Materials:** This is a spiral-bound booklet that contains the presenter's script for each overhead transparency. In the back of the booklet are two diskettes containing three files:

- Presenter's script (word-for-word presentation for each overhead transparency) in MS Word
- Text for overheads in MS Word Rich Text Format
- Blank PowerPoint AHIMA format slide

3. **Overhead Transparencies:** A complete set of transparencies ready for use.

Ordering Information:
Title: *Program in a Box: Information Security: Protecting Paper and Computer-based Health Information*
Authors: Mary Brandt, MBA, RRA, CHE and Sandra R. Fuller, MA, RRA
Publisher: American Health Information Management Association (AHIMA), 1997
Price: $175.00

Computer Security Institute. "Manager's Guide to Computer Security Awareness." San Francisco, CSI.

Computer-based Patient Record Institute. "Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Record Systems." Schaumburg, IL: CPRI, 1995.

Siwicki, Bill. "Teaching Effective Security," Health Data Management, November 1998, pp. 84-87.

Toolkit Section 4.8

Enforcing Security Policy

Once in place, security policies must be acknowledged and enforced. All organizational staff as well as consultants, contractors, vendors, and trading partners accessing confidential information should sign a confidentiality agreement acknowledging that they understand and will adhere to that organization's security practices. Policy enforcement is important in delivering the message to staff that organizational security is a serious issue and that breach of confidentiality is a punishable offense. Policies must be administered consistently across all levels of staff and throughout all sites and departments. A process should spell out the following:

1. What to do if a breach of confidentiality is witnessed
2. To whom and how a breach should be reported
3. How a breach should be investigated and reviewed
4. How a breach should be discussed and shared in relation to the affected patient (if any), the staff person who discovered it, the staff person who committed it, and the staff person's supervisor (confidentiality of the patient, the offender, and the reporter are important)
5. How a breach should be punished
6. How overall patterns of breach behavior should be reported and monitored

A common approach classifies breaches and subsequent discipline into levels assigning more importance to malicious breaches (i.e., looking up information in a colleague's record in an attempt to get him fired) than to inadvertent breaches (leaving a computer terminal signed on to a patient's record). Staff should thoroughly understand the classification of breaches and associated disciplinary action.

- **Level I – Inadvertent breach:** accidental, often due to lack of education or awareness. Examples may include failing to log off a computer terminal or sharing passwords. Often these breaches do not result in actual patient information being exposed or shared. Punishment might include verbal warning and mandatory re-education for first offense up to termination for repeated offenses.
- **Level II – Intentional breach without malice:** accessing a patient record with no legitimate business purpose for doing so. This might mean accessing a friend's or relative's record out of curiosity or releasing patient information inappropriately. Punishment might include written warning for first offense up to termination for repeated offenses.

Level III – Intentional breach with malice: accessing a patient record with the intent to use it for personal gain or to harm someone. Punishment would include termination for cause.

Sample Confidentiality Statements and Agreements

For

Organizations Using Computer-based Patient Record Systems

Prepared by
CPRI Work Group on
Confidentiality, Privacy and Security

May 1996

Computer-based Patient Record Institute
Creating information solutions for health care

Sample Confidentiality Statements and Agreements

For

Organizations Using Computer-based Patient Record Systems

Prepared by
CPRI Work Group on
Confidentiality, Privacy, and Security

May 1996

Computer-based Patient Record Institute
Creating information solutions for health care

Computer-based Patient Record Institute
Creating information solutions for health care

Sample Confidentiality Statements and Agreements
For Organizations Using Computer-based Patient Record Systems

© Copyright 1996, by the Computer-based Patient Record Institute. All rights reserved.

No part of this publication may be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

Printed in the United States of America

This book was prepared camera-ready.

Sample Confidentiality Statements and Agreements for Organizations Using Computer-based Patient Record Systems

Overview

The Computer-based Patient Record Institute Work Group on Confidentiality, Privacy, and Security was established to encourage creation of policies and the implementation of mechanisms which protect patient and caregiver privacy as well, as preserve the confidentiality, protect the integrity, and ensure the availability of information in computer-based patient record systems.

During the early phases of its efforts, the Work Group determined that although computer-based patient records (CPRs) offer the potential for achieving greater protection of health information than can be provided with paper-based records, it is necessary that formal information security programs be established by each organization entrusted with health information in order to achieve an appropriate and consistent level of protection.

Therefore, in addition to its other activities, the Work Group is developing a series of information security guidelines to assist organizations implementing computer-based patient record systems to establish formal information security programs.

The other documents in this series that have been published are:

- *Guidelines for Establishing Information Security Policies at Organizations Using Computer--based Patient Record Systems*
- *Guidelines for Information Security Education Programs at Organizations Using Computer--based Patient Record Systems*
- *Guidelines for Managing Information Security Programs at Organizations Using Computer-based Patient Record Systems*

Additional guidelines are being developed to address:

- Information security terms.
- Implementing electronic signatures.
- Methods for identifying and authenticating users of computer-based patient records.
- System and application security features.
- Security audit functions and processes.

Acknowledgments

This document was prepared by members of the Work Group on Confidentiality, Privacy, and Security, Kathleen A. Frawley and Dale W. Miller, Co-Chairpersons. The material for the document and the initial versions were prepared by the Project Team on Model Confidentiality Agreements led by Cindy Beery.

The Project Team Leader and Work Group Co-Chairpersons are indebted to the many volunteers who participated in the work group meetings, provided input, and prepared and reviewed the drafts of this document.

Table of Contents

Overview iii

Acknowledgments iv

Introduction 1

Objectives 1

Scope 1

Sample Confidentiality Statements and Agreements 2

- Sample Computer and Information Usage Agreement (Employee/Volunteer/Student) 3
- Sample Computer and Information Usage Agreement (Physician) 9
- Sample Access and Confidentiality Agreement (Employee/Volunteer/Student) 15
- Sample Access and Confidentiality Agreement (Physician) 19
- Sample Vendor Confidentiality Statement for Access to Information Systems 23
- Sample Vendor Data Security and Confidentiality Agreement 27

Sample Confidentiality Statements and Agreements for Organizations Using Computer-based Patient Record Systems

Introduction

Ensuring that health information is protected from unauthorized disclosure and safeguarded to prevent unauthorized modification or destruction is an essential prerequisite for implementing computer-based patient record systems'. Because of the diversity of the organizational issues and the technical complexity of the systems and networks, protecting health information can be achieved most effectively with an organization-wide program.

A comprehensive information security program consists of written policies, standards, training, technical and procedural controls, risk assessment, auditing and monitoring, and assigned responsibility for management of the information security program. Any individual who is permitted access to the organization's information system should be required to sign an agreement documenting their understanding of their responsibilities in preserving the confidentiality and security of information.

This document has been prepared by the Work Group on Confidentiality, Privacy, and Security to provide model confidentiality statements and agreements at organizations using computer-based patient record systems.

Objectives

The objectives of the work group in developing these guidelines are to:

- foster the recognition of the need for all employees, students, volunteers, physicians and vendors who access information systems to sign confidentiality agreements
- provide model agreements that organizations can use to increase awareness of staff, physicians and vendors that the information they are accessing is confidential and should be treated as such

Scope

This document is intended to be applicable to organizations that utilize computer-based patient record systems to collect, create, receive, store, report, and process health information. All health care provider organizations - hospitals, physician offices, home health agencies, pharmacies, nursing homes, and others - will benefit from developing confidentiality agreements as displayed in these guidelines.

Sample Confidentiality Statements and Agreements

Following are sample confidentiality agreements for employees of health care provider organization, for physicians, and for vendors. The following are samples are should not be used without the advice of the user's legal counsel.

Sample Computer and Information Usage Agreement (Employee, Volunteer, Student) and Sample Computer and Information Usage Agreement (Physician)

The sample computer and information usage agreements (for employees and for physicians) are applicable for employees and physicians who have access to the health care entity's computer system.

Sample Access and Confidentiality Agreement (Employee, Volunteer, Student) and Sample Access and Confidentiality Agreement (Physician)

The sample access and confidentiality agreements (for employees and for physicians) are applicable for those individuals who have access to the health care entity's confidential information.

Sample Vendor Confidentiality Statement for Access to Information Systems

The sample vendor confidentiality statement for access to information systems provides a request for access to a health care provider's information system for the purpose of providing technical support.

Sample Vendor Data Security and Confidentiality Agreement

The sample vendor data security and confidentiality agreement requires the vendor to acknowledge that they are accessing confidential information that is the property of the health care entity.

It is important to note that all of the documents following are *samples* and should not be used without the advice of the user's legal counsel.

SAMPLE

COMPUTER AND INFORMATION USAGE AGREEMENT

(Employee/Volunteer/Student)

Security and confidentiality is a matter of concern for all persons who have access to (HEALTHCARE ENTITY) information systems. Each person accessing (HEALTHCARE ENTITY) data and resources holds a position of trust relative to this information and must recognize the responsibilities entrusted in preserving the security-and confidentiality of this information. Therefore, all persons who are authorized to access data and resources, both through enterprise information systems and through individual department local area networks and databases, must read and comply with (HEALTHCARE ENTITY) policy.

Use of a computer network that is shared by many users imposes many obligations. In particular, data, software and computer capacity have value and must be treated accordingly.

The following specific principles of computer and network systems are applicable to all of (HEALTHCARE ENTITY) students, faculty, staff and employees regardless of their classification as a Health Information Trustee, Health Information Custodian or Health Information User (please refer to attached for definitions, responsibilities and authorities of these classifications). I will:

- Respect the privacy and rules governing the use of any information accessible through the computer system or network and only utilize information necessary for performance of my job.
- Respect the ownership of proprietary software. For example, do not make unauthorized copies of such software for your own use, even when the software is not physically protected against copying.
- Respect the finite capability of the systems, and limit your own use so as not to interfere unreasonably with the activity of other users.
- Respect the procedures established to manage the use of the system.
- Prevent unauthorized use of any information in files maintained, stored or processed by (HEALTHCARE ENTITY).
- Not seek personal benefit or permit others to benefit personally by any confidential information or use of equipment available through my work assignment.
- Not operate any non-licensed software on any computer provided by (HEALTHCARE ENTITY).

Employee Usage Agreement Sample

Page 2 of 5

- Not exhibit or divulge the contents of any record or report except to fulfill a work assignment and in accordance with (HEALTHCARE ENTITY) policy.
- Not knowingly include or cause to be included in any record or report, a false, inaccurate, or misleading entry.
- Not remove any record (or copy) or report from the office where it is kept except in the performance of my duties.
- Report any violation of this code.
- Understand that the information accessed through all (HEALTHCARE ENTITY) information systems contains sensitive and confidential patient/member care, business, financial and hospital employee information that should only be disclosed to those authorized to receive it.
- Not release my authentication code or device to anyone else, or allow anyone else to access or alter information under my identity.
- Not utilize anyone else's authentication code or device in order to access any (HEALTHCARE ENTITY) system.
- Respect the confidentiality of any reports printed from any information system containing patient/member information and handle, store and dispose of these reports appropriately.
- Not divulge any information that identifies a patient/member.
- Understand that all access to the system will be monitored.
- Understand that my obligations under this Agreement will continue after termination of my employment. I understand that my privileges hereunder are subject to periodic review, revision, and if appropriate, renewal.

Employee Usage Agreement Sample

Page 3 of 5

Those who cannot accept these standards of behavior may be denied access to the relevant computer systems and networks. Violators also may be subject to penalties, including disciplinary action, under policies of (HEALTHCARE ENTITY) and under laws of the State of (STATE NAME) or the United States of America to the extent applicable.

By signing this, I agree that I have read, understand and will comply with the Agreement.

_____ _____ _____
Signature Date

_____
Printed Name

_____ _____
Area/Department Phone Number

For discussion purposes only. Not for use without advice of legal counsel.

Employee Usage Agreement Sample - Attachment
Page 4 of 5
DEFINITIONS

Health Information Trustee - An organizational unit (department, college, company, etc.) authorized to create and maintain information and data. The Health Information Trustee, by definition, must have sufficient authority to restrict access to the data within their control.

Health Information Custodian - A Health Information Custodian handles or processes data for the Health Information Trustee. Health Information Custodians could be, but are not limited to, any of the following functional areas: data entry, computer room operators, technical support, courier services, telecommunications, output distribution and systems development and maintenance. In certain cases, a Health Information Trustee may also be a Health Information Custodian.

Health Information User - Anyone who has access to data stored by Information Systems' equipment or facilities in certain cases, the Health Information User may also be the Health Information Trustee and/or Health Information Custodian.

RESPONSIBILITIES AND AUTHORITIES

Health Information Trustee - The Health Information Trustee is ultimately responsible for ensuring the integrity, reliability, accuracy and security of information and data over which they have authority. The Health Information Trustee is responsible for providing the following minimum safeguards:

1. Coordinating with systems development and maintenance personnel to ensure that access security controls are implemented to reasonably protect information created and maintained within their area of responsibility.

2. Implementing such physical security measures as are appropriate (over terminals, PC's data files, etc.) to reasonably ensure the protection of information from unauthorized access;

3. Authorizing to release or coordinate the release of information to internal and/or external sources.

4. Authorizing Information Systems development personnel to create and modify application computer programs and systems.

Health Information Custodian - A Health Information Custodian is responsible for providing the following minimum safeguards to ensure the integrity, reliability, accuracy and security of data over which they have custodial responsibility;

1. Ensuring that processing areas for which custodian is responsible are secured from unauthorized physical access;

2. Performing backup recovery of data following the Health Information Trustee's established file retention;

3. Implementing acceptable administrative controls and ensures an effective segregation of incompatible duties;

4. Implementing procedures to ensure that information is released only to authorized individuals;

Employee Usage Agreement Sample - Attachment

Page 5 of 5

5. Ensuring that systems development and maintenance personnel implement internal processing and controls which reasonably ensure the accuracy and completeness of data;

6. Ensuring adequate protection of proprietary software operating with the Health Information Custodian's systems;

7. Must have expressed consent of the application owner to access, modify, or delete applications related to data.

Health Information User - A Health Information User is responsible for understanding and complying with the following:

1. Assignment of authentication code or devices is intended for individual use only. Authentication code or devices are confidential and should not be posted, shared or distributed to anyone other that the intended user;

2. Implementing security measures as are appropriate for terminals, PC's data files, etc. and reasonably ensure the protection of information from unauthorized access;

3. Compliance with appropriate computer access and data authorization requirements.

For discussion purposes only. Not for use without advice of legal counsel.

SAMPLE

COMPUTER AND INFORMATION USAGE AGREEMENT

(Physician)

Security and confidentiality is a matter of concern for all persons who have access to (HEALTHCARE ENTITY) information systems. Each person accessing (HEALTHCARE ENTITY) data and resources holds a position of trust relative to this information and must recognize the responsibilities entrusted in preserving the security and confidentiality of this information. Therefore, all persons who are authorized to access data and resources, both through enterprise information systems and through individual department local area networks and databases, must read and comply with (HEALTHCARE ENTITY) policy.

Use of a computer network that is shared by many users imposes many obligations. In particular, data, software and computer capacity have value and must be treated accordingly.

The following specific principles of computer and network systems are applicable to all of (HEALTHCARE ENTITY) students, faculty, staff and employees regardless of their classification as a Health Information Trustee, Health Information Custodian or Health Information User (please refer to attached for definitions, responsibilities and authorities of these classifications). I will:

- Respect the privacy and rules governing the use of any information accessible through the computer system or network and only utilize information necessary for performance of my job.
- Respect the ownership of proprietary software. For example, do not make unauthorized copies of such software for your own use, even when the software is not physically protected against copying.
- Respect the finite capability of the systems, and limit your own use so as not to interfere unreasonably with the activity of other users.
- Respect the procedures established to manage the use of the system.
- Prevent unauthorized use of any information in files maintained, stored or processed by (HEALTHCARE ENTITY).
- Not seek personal benefit or permit others to benefit personally by any confidential information or use of equipment available through my work assignment.
- Not operate any non-licensed software on any computer provided by (HEALTHCARE ENTITY).

Physician Usage Agreement Sample

Page 2 of 5

- Not exhibit or divulge the contents of any record or report except to fulfill a work assignment and in accordance with (HEALTHCARE ENTITY) policy.
- Not knowingly include or cause to be included in any record or report a false, inaccurate, or misleading entry.
- Not remove any record (or copy) or report from the office where it is kept except in the performance of my duties.
- Report any violation of this code.
- Understand that the information accessed through all (HEALTHCARE ENTITY) information systems contains sensitive and confidential patient/member care, business, financial and hospital employee information that should only be disclosed to those authorized to receive it.
- Not release my authentication code or device to anyone else, or allow anyone else to access or alter information under my identity.
- Not utilize anyone else's authentication code or device in order to access any (HEALTHCARE ENTITY) system.
- Respect the confidentiality of any reports printed from any information system containing patient/member information and handle, store and dispose of these reports appropriately.
- Not divulge any information that identifies a patient/member.
- Understand that all access to the system will be monitored.
- Understand that my obligations under this Agreement will continue after termination of my employment. I understand that my privileges hereunder are subject to periodic review, revision, and if appropriate, renewal.

Physician Usage Agreement Sample

Page 3 of 5

Those who cannot accept these standards of behavior may be denied access to the relevant computer systems and networks. Violators also may be subject to penalties, including disciplinary action, under policies of (HEALTHCARE ENTITY) and under laws of the State of (STATE NAME) or the United States of America to the extent applicable.

By signing this, I agree that I have read, understand and will comply with the Agreement.

_____ _____
Signature Date

_____
Printed Name

_____ _____
Area/Department Phone Number

For discussion purposes only. Not for use without advice of legal counsel.

Physician Usage Agreement Sample - Attachment
Page 4 of 5
DEFINITIONS

Health Information Trustee -- An organizational unit (department, college, company, etc.) authorized to create and maintain information and data. The Health Information Trustee, by definition, must have sufficient authority to restrict access to the data within their control.

Health Information Custodian -- A Health Information Custodian handles or processes data for the Health Information Trustee. Health Information Custodians could be, but are not limited to, any of the following functional areas: data entry, computer room operators, technical support, courier services, telecommunications, output distribution and systems development and maintenance. In certain cases, a Health Information Trustee may also be a Health Information Custodian.

Health Information User -- Anyone who has access to data stored by Information Systems' equipment or facilities. In certain cases, the Health Information User may also be the Health Information Trustee and/or Health Information Custodian.

RESPONSIBILITIES AND AUTHORITIES

Health Information Trustee -- The Health Information Trustee is ultimately responsible for ensuring the integrity, reliability, accuracy and security of information and data over which they have authority. The Health Information Trustee is responsible for providing the following minimum safeguards:

1. Coordinating with systems development and maintenance personnel to ensure that access security controls are implemented to reasonably protect information created and maintained within their area of responsibility.

2. Implementing such physical security measures as are appropriate (over terminals, PC's data files, etc.) to reasonably ensure the protection of information from unauthorized access; I

3. Authorizing to release or coordinate the release of information to internal and/or external sources;

4. Authorizing Information Systems development personnel to create and modify application computer programs and systems.

Health Information Custodian -- A Health Information Custodian is responsible for providing the following minimum safeguards to ensure the integrity, reliability, accuracy and security of data over which they have custodial responsibility;

1. ensuring that processing areas for which custodian is responsible are secured from unauthorized physical access;

2. Performing backup recovery of data following the Health Information Trustee's established file retention;

3. Implementing acceptable administrative controls and ensures an effective segregation of incompatible duties;

4. Implementing procedures to ensure that information is released only to authorized individuals;

Physician Usage Agreement Sample - Attachment

Page 5 of 5

5. Ensuring that systems development and maintenance personnel implement internal processing and controls which reasonably ensure the accuracy and completeness of data;

6. Ensuring adequate protection of proprietary software operating with the Health Information Custodian's systems;

7. Must have expressed consent of the application owner to access, modify, or delete applications related to data.

Health Information User -- A Health Information User is responsible for understanding and complying with the following:

1. Assignment of authentication code or devices is intended for individual use only. Authentication code or devices are confidential and should not be posted, shared or distributed to anyone other that the intended user;

2. Implementing security measures as are appropriate for terminals, PC's data files, etc. and reasonably ensure the protection of information from unauthorized access;

3. Compliance with appropriate computer access and data authorization requirements.

For discussion purposes only. Not for use without advice of legal counsel.

SAMPLE

ACCESS AND CONFIDENTIALITY AGREEMENT

(Employee/Volunteer/Student)

As an employee/volunteer/student with privileges at (HEALTHCARE ENTITY), you may have access to what this agreement refers to as "confidential information." The purpose of this agreement is to help you understand your duty regarding confidential information.

Confidential information includes patient/member information, employee/volunteer/ student information, financial information, other information relating to (HEALTHCARE ENTITY) and information proprietary to other companies or persons. You may learn of or have access to some or all of this confidential information through a computer system or through your employment activities.

Confidential information is valuable and sensitive and is protected by law and by strict (HEALTHCARE ENTITY) policies. The intent of these laws and policies is to assure that confidential information will remain confidential - that is, that it will be used only as necessary to accomplish the organization's mission.

As an employee/volunteer/student, you are required to conduct yourself in strict conformance to applicable laws and (HEALTHCARE ENTITY) policies governing confidential information. Your principal obligations in this area are explained below. You are required to read and to abide by these duties. The violation of any of these duties will subject you to discipline, which might include, but is not limited to, termination of employment and to legal liability.

As an employee/volunteer/student, you understand that you will have access to confidential information that may include, but is not limited to, information relating to:

- Patients/members (such as records, conversations, admittance information, patient/member financial information, etc),
- Employees/volunteer/students (such as salaries, employment records, disciplinary actions, etc.),
- (HEALTHCARE ENTITY) information (such as financial and statistical records, strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary computer programs, source code, proprietary technology, etc.) and
- Third party information (such as computer programs, client and vendor proprietary information source code, proprietary technology, etc.).

Employee Confidentiality Statement Sample

Page 2 of 3

Accordingly, as a condition of and in consideration of your access to confidential information, you promise that:

1. You will use confidential information only as needed to perform your legitimate duties as an employee/volunteer/student affiliated with (HEALTHCARE ENTITY). This means, among other things, that:

    A. You will only access confidential information for which you have a need to know; and

    B. You will not in any way divulge, copy, release, sell, loan, review, alter or destroy any confidential information except as properly authorized within the scope of my professional activities affiliated with (HEALTHCARE ENTITY); and

    C. You will not misuse confidential information or carelessly care for confidential information.

2. You will safeguard and will not disclose my access code or any other authorization I have that allows me to access confidential information.

3. You accept responsibility for all activities undertaken using my access code and other authorization.

4. You will report activities by any individual or entity that I suspect may compromise the confidentiality of confidential information, Reports made in good faith about suspect activities will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities.

5. You understand that my obligations under this Agreement will continue after termination of my employment. You understand that your privileges hereunder are subject to periodic review, revision and if appropriate, renewal.

6. You understand that you have no right or ownership interest in any confidential information referred to in this Agreement. (HEALTHCARE ENTITY) may at any time revoke my access code, other authorization, or access to confidential information. At all times during your employment, you will safeguard and retain the confidentiality of all confidential information.

Employee Confidentiality Statement Sample

Page 3 of 3

7. You will be responsible for your misuse or wrongful disclosure of confidential information and for your failure to safeguard your access code or other authorization access to confidential information. You understand that your failure to comply with this Agreement may also result in your loss of employment at (HEALTHCARE ENTITY).

_____ _____
Employee/Volunteer/Student Signature Date

_____
Printed Name

For discussion purposes only. Not for use without advice of legal counsel.

SAMPLE

ACCESS AND CONFIDENTIALITY AGREEMENT

(Physician)

As a physician with privileges at (HEALTHCARE ENTITY) (hereafter referred to as "Physician"), you may have access to what this agreement refers to as "confidential information." The purpose of this agreement is to help you understand your duty regarding confidential information.

Confidential information includes patient/member information, employee information, financial information, other information relating to (HEALTHCARE ENTITY) and information proprietary to other companies or persons. You may learn of or have access to some or all of this confidential information through a computer system or through your professional care to patient/members.

Confidential information is valuable and sensitive and is protected by law and by strict (HEALTHCARE ENTITY) policies. The intent of these laws and policies is to assure that confidential information will remain confidential - that is, that it will be used only as necessary to accomplish the organization's mission.

As a physician, you have access to confidential information. You are required to conduct yourself in strict conformance to applicable laws and (HEALTHCARE ENTITY) policies governing confidential information. Your principal obligations in this area are explained below. You are required to read and to abide by these duties. The violation of any of these duties will subject you to discipline, which might include, but is not limited to , loss of privileges to access confidential information, loss of privileges at (HEALTHCARE ENTITY), and to legal liability.

As a physician, you must understand that you will have access to confidential information that may include, but is not limited to, information relating to:

- Patient/members (such as records, conversations, admittance information, patient/member financial information, etc),
- Employees (such as salaries, employment records, disciplinary actions, etc.),
- (HEALTHCARE ENTITY) information (such as financial and statistical records, strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary computer programs, source code, proprietary technology, etc.) and

Physician Confidentiality Agreement Sample

Page 2 of 3

- Third party information (such as computer programs, client and vendor proprietary information source code, proprietary technology, etc.).

Accordingly, as a condition of and in consideration of your access to confidential information, you promise that:

1. You will use confidential information only as needed to perform your legitimate duties as a physician of patient/members affiliated with (HEALTHCARE ENTITY). This means, among other things, that:

   A. You will only access confidential information for which you have a need to know; and

   B. You will not in any way divulge, copy, release, sell, loan, review, alter or destroy any confidential information except as properly authorized within the scope of your professional activities as a physician of patient/members affiliated with (HEALTHCARE ENTITY); and

   C. You will not misuse confidential information or carelessly care for confidential information.

2. You will safeguard and will not disclose your access code or any other authorization you have that allows you to access confidential information. You accept responsibility for all activities undertaken using your access code and other authorization.

3. You will report activities by any individual or entity that you suspect may compromise the confidentiality of confidential information, Reports made in good faith about suspect activities will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities.

4. You understand that your obligations under this Agreement will continue after termination of your privileges as a physician, as defined in this agreement. You understand that your privileges hereunder are subject to periodic review, revision and if appropriate, renewal.

5. You understand that you have no right or ownership interest in any confidential information referred to in this Agreement. (HEALTHCARE ENTITY) may at any time revoke your access code, other authorization, or access to confidential information. At all times during your privileges as a physician, you will safeguard and retain the confidentiality of all confidential information.

Physician Confidentiality Agreement Sample

Page 3 of 3

6. You will be responsible for your misuse or wrongful disclosure of confidential information and for your failure to safeguard your access code or other authorization access to confidential information. You understand that your failure to comply with this Agreement may also result in loss of privileges to access confidential information, loss of privileges and to legal liability.

_____ _____
Physician Signature Date

_____
Printed Name

For discussion purposes only. Not for use without advice of legal counsel.

SAMPLE

Vendor Confidentiality Statement

for Access to Information Systems

(HEALTHCARE ENTITY)

As an employee of _____, I request
(Name of Company)

access to the following applications on (HEALTHCARE ENTITY) systems _____

_____.

I request this access in order to provide technical support for the application(s) above which is a product of our company.

I understand that the information which I will access through the (HEALTHCARE ENTITY) Information Systems is sensitive and confidential. Confidential information includes patient/member information, employee/volunteer/student information, financial information, other information relating to (HEALTHCARE ENTITY) and information proprietary to other companies or persons. I may learn of or have access to some or all of this confidential information through a computer system or through my employment activities.

Confidential information is valuable and sensitive and is protected by law and by strict (HEALTHCARE ENTITY) policies. The intent of these laws and policies is to assure that confidential information will remain confidential - that is, that it will be used only as necessary to accomplish the organization's mission.

As an employee of _____ , I am required to conduct myself in a strict conformance to applicable laws and (HEALTHCARE ENTITY) policies governing confidential information. My principal duties in this area are explained below. I am required to read and to abide by these duties. The violation of any of these duties will subject me to discipline, which might include, but is not limited to, termination of employment and to legal liability.

I understand that I will have access to confidential information which may include, but is not limited to, information relating to:

- Patient/members (such as records, conversations, admittance information, patient/member financial information, etc),

Vendor Confidentiality Statement Sample

Page 2 of 3

- Employees/volunteer/students (such as salaries, employment records, disciplinary actions, etc.),
- (HEALTHCARE ENTITY) information (such as financial and statistical records, strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary, computer programs, source code, proprietary technology, etc.) and
- Third party information (such as computer programs, client and vendor proprietary information, source code, proprietary technology, etc.).

Accordingly, as a condition of and in consideration of my access to confidential information, I promise that:

1. I will use confidential information only as needed by me to perform my legitimate duties as an employee affiliated with

   _____.

This means, among other things, that:

   A. I will only access confidential information for which I have a need to know; and

   B. I will not in any way divulge, copy, release, sell, loan, review, alter or destroy any Confidential information except as properly authorized within the scope of my professional activities and

   C. I will not misuse confidential information or carelessly handle for confidential information.

2. I will safeguard and will not disclose my access code or any other authorization I have that allows me to access confidential information. I accept responsibility for all activities undertaken using my access code and other authorization.

3. I will report activities by any individual or entity that I suspect may compromise the confidentiality of confidential information, Reports made in good faith about suspect activities will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities.

Vendor Confidentiality Statement Sample

Page 3 of 3

4. I understand that my obligations under this Agreement will continue after termination of my employment. I understand that my privileges hereunder are subject to periodic review, revision and if appropriate, renewal.

5. I understand that I have no right or ownership interest in any confidential information referred to in this Agreement. (HEALTHCARE ENTITY) may at any time revoke my access code, other authorization, or access to confidential information. At all times during my employment, I will safeguard the confidentiality of all confidential information.

6. I will be responsible for my misuse or wrongful disclosure of confidential information and for my failure to safeguard my access code or other authorization access to confidential information. I understand that my failure to comply with this Agreement may result in immediate termination of my access to the information system and legal action against me and the company I represent.

_____ _____

Signature of Vendor Staff Member Date

Name and Address of Company Authorized Agent for Company

_____ _____

Signature

_____ _____

Printed Name

_____

_____

Phone Number_____

(Healthcare Entity) Information Systems Contact

_____

Department Contact

_____

<u>For discussion purposes only. Not for use without advice of legal counsel.</u>

SAMPLE

VENDOR DATA SECURITY AND CONFIDENTIALITY AGREEMENT

(HEALTHCARE ENTITY) herein referred to as The Enterprise, has certain information contained within The Enterprise's computer databases or information system. This information includes, but is not limited to, The Enterprise's patients and employee demographics, patient information, patient/member medical insurance and third party payor's of patient/member medical bills, patient/member information and hospital financial information.

The undersigned individual, corporation, partnership or organization (herein referred to as Prospective User) desires access to such information either in an electronic or hard-copy format. This access is requested in connection with the provision of patient/member care services, with medical research, system development agreements with The Enterprise or maintenance of The Enterprise's Information System.

The Enterprise is willing to permit Prospective User access to such information, subject to the following conditions:

1. Prospective User hereby acknowledges that all information accessed through The Enterprise's Information System is confidential and the property of The Enterprise.

2. Prospective User agrees to access only those specific elements of information in The Enterprise's Information System for which the Prospective User has obtained prior permission from The Enterprise to access. In order to obtain such permission, the Prospective User agrees to complete and submit for approval the reasons Prospective User requires access to the system, the specific items of data required to be accessed by Prospective User, and whether or not Prospective User requires the ability to input, edit, download or otherwise collect data in The Enterprise's Information System.

3. Prospective User agrees to access and use information obtained from The Enterprise's Information System only for the purpose(s) for which Prospective User is granted permission to access such information by The Enterprise. The Prospective User agrees not to share any information with anyone who is not authorized by The Enterprise to have access to that information, or disclose any information obtained from The Enterprise's Information System to any third party, other than employees or agents of the Prospective User, without the prior written permission of The Enterprise.

4. Prospective User agrees to require all of its employees and/or agents who will have access to information contained within The Enterprise's Information System to sign the "Vendor Confidentiality Statement for Access to Hospital Information Systems" prior to access by such employees or agents of the information. Prospective User agrees to retain the original statement for each of its employees or agents who have access to the information throughout the term of this Agreement or for a period of one (1) year following termination of the agency or employment with Prospective User, whichever comes later. Prospective User agrees to forward

Vendor Confidentiality Agreement Sample

Page 2 of 3

copies of all confidentiality statements to The Enterprise within three (3) days after written request by The Enterprise.

5. Both parties agree that any breach of the confidentiality obligations of this Agreement will result in irreparable damage for which there is no adequate remedy at law. Therefore, it is agreed that The Enterprise shall be entitled to equitable relief, including an injunction enjoining any such, breach by any court or competent jurisdiction. Such injunction shall be without prejudice to any other right or remedy to which The Enterprise may be entitled, including damages. Prospective User hereby agrees to defend, indemnify, and hold The Enterprise, its officers, agents, and employees harmless from any and all claims, suits, demands, awards and judgements for personal or bodily injury resulting from any disclosure of information by Prospective User or by Prospective User's agents or employees to any third party in violation of the terms of this Agreement. The terms of the paragraph shall survive termination of this Agreement.

6. This Agreement may be terminated by either party and access to The Enterprise's Information System discontinued upon five (5) days prior written notice of one party to the other. Prospective User agrees that The Enterprise may immediately terminate this Agreement and deny Prospective User access to The Enterprise's Information System without notice whenever The Enterprise, in its sole opinion, has determined that Prospective User, its agents, or employees has violated any of the provisions of this Agreement. In the event of such termination, Prospective User agrees that The Enterprise shall not be liable to Prospective User for any damages resulting from Prospective User's inability to access information within The Enterprise's Information System.

7. The obligation to maintain the confidentiality of the information survives the termination of this Agreement. Upon termination of this Agreement, all information accessed shall either be returned to The Enterprise or destroyed.

8. Prospective User agrees that The Enterprise does not guarantee to Prospective User the availability or accuracy of any data contained in The Enterprise's information systems.

9. If either party becomes legally compelled by law, process or order of any court or governmental agency to disclose any confidential information, that party shall notify the other so that it may seek a protective order to take other appropriate action.

This access is requested for the sole purpose of _____

_____.

Vendor Confidentiality Agreement Sample

Page 3 of 3

ACCEPTED BY AUTHORIZED AGENT FOR COMPANY:

_____ _____
Signature Printed Name

_____
Date

_____

NAME AND ADDRESS OF COMPANY

_____

_____

_____

PHONE NUMBER_____

For discussion purposes only. Not for use without advice of legal counsel.

CPRI Members

3M Health Information Systems
Adventist Health Systems/Sunbelt
ALLTEL Information Services Inc. - Healthcare Div.
American Academy of Family Physicians
American Academy of Pediatrics
American Association for Medical Transcription
American Board of Family Practice
American College of Physicians
American Health Information Management Association
American Hospital Association
American Medical Association
American Medical Informatics Association
American Organization of Nurse Executives
Andersen Consulting, LLP
Association of Operating Room Nurses, Inc.
Center for Healthcare Information Management
Centers for Disease Control and Prevention
Chi Systems
College of American Pathologists
College of Healthcare Information Management Executives
Columbia/HCA Healthcare Corp.
Department of Veterans Affairs
Dynamic Healthcare Technologies
Eli Lilly and Company
Ernst & Young, LLP
Harvard Community Health Plan, Inc,
HBO & Company
Health Care Process Improvements Inc.
Health Level Seven
HEALTHPOINT
HealthVISION Corporation
Hewlett-Packard
IBM Healthcare Solutions
IDX Systems Corporation
Institute for Clinical Systems Integration
Joint Commission on Accreditation of Healthcare Organizations
Kaiser Permanente
Management Systems Associates, Inc.
Matria Healthcare, Inc.
Mayo Foundation
Medic Alert Foundation United States
Medical Connections, Inc.
Medical Records Institute
MedicaLogic
Medicus Systems Corp.
National Association of Chain Drug Stores
National Council For Prescription Drug Programs
NC Health Care Info. and Comm. Alliance, Inc.
Neon Healthcare Software
Northwestern Memorial Hospital
Oceania, Inc.
PHAMIS, Inc.
Prudential Insurance Companies of America
Sisters of Mercy Health System
Systems Plus, Inc.
The Permanente Medical Group
Unitron Medical Communications, Inc.
University HealthSystem Consortium
University of Virginia Health Sciences Center

CPRI is a non-profit membership organization committed to advancing improvements in health care quality, cost and access through routine use of information technology. CPRI serves as a neutral forum for bringing the diverse interests of all health care stakeholders together to develop common solutions.

CPRI functions primarily through the voluntary work of its work groups. All individuals are invited to participate in one of the following:

- Work Group on Codes & Structures
- Work Group on Confidentiality, Privacy, and Security
- Work Group on CPR Description
- Work Group on CPR Systems Evaluation
- Work Group on Professional & Public Education

Toolkit Section 4.8.2

Case Study: Securing User Agreements at Kaiser Permanente

To protect the health care organization and reinforce the importance of health care confidentiality, appropriate computer usage, and establish accountability for an individual's computer entries, a health care organization should obtain and periodically renew a signed agreement with each and every physician, employee, student, and volunteer at the beginning of the association. A practical approach is to obtain this agreement at the beginning of the association for employees, students, and volunteers and as a part of their annual evaluation. For physicians this can be done at the time of application for clinical privileges and when they are evaluated for renewal every two years in accordance with JCAHO and NCQA requirements. Kaiser Permanente has drafted a proposal to replace the current approach of using separate agreements for these items with this single approach.

Draft Electronic Signature Policy Document
Kaiser Permanente

Purpose

The purpose of this policy is to ensure that entries made in information systems meet legal and ethical requirements. Examples of health care professional entered information include the entry or updating of significant health problems, visit diagnoses and procedures, allergies, preventive health prompts, discharge summaries, consultation reports, orders, laboratory results review and receipt, and visit notes. Our patient's health care record has officially been designated to comprise both the paper chart and patient specific information in our online systems.

Background

All human entries in clinical information systems databases must be accurate and attributable to an individual. This is accomplished in electronic systems by the use of an "electronic signature." Electronic signatures have the same legal meaning and significance as a hand written signature. In the patient record, signatures are used to identify the person who made an entry, to indicate that a review of an entry has been made, and to designate approval of an entry.

When one logs on to the computer system, the use of the individual's user identification code and secret password is meant to inform the computer system who is using it and keeps track of each action taken. When one enters information, the last step before the computer accepts the information is a request to press a specific key and or enter a code to confirm the entry. This is the electronic equivalent of signing on paper. The computer keeps a record of the action taken, the user identification code, the time, and the date. This provides an audit trail for each action taken. In the same way individuals are accountable for the paper documents they sign, they are also accountable for the entries they make in information systems.

The JCAHO requires "that the hospital has a system in place to assure that only authorized individuals make entries into medical records: identify the date and author of every entry in the medical record: and enable the author to authenticate an entry to verify it is complete, accurate, and final." and "establish policies and mechanisms to assure that only an author can authenticate his or her own entry. Indication of authentication can include written signatures or initials, rubber-stamps. or computer 'signatures' (or sequence of keys)."

Medicare Conditions of Participation require existence of a "system of author identification" that "ensures the integrity of authentication and protects the security of all record entries." Entries must be dated, and the authors of each entry must be identified and must authenticate their entries. Authentication may include "signatures, written initials, or computer entry."

California Code of Regulations -Title 22 section 70751 (g) requires a signed statement from each physician that the electronic signature key (user-ID and password) will only be known and used by that individual physician.

Policy:

Each individual who enters information into information systems is responsible for the accuracy, appropriateness, and completeness of the entries made through the use of their user identification code.

The sharing of one's user identification code or password is prohibited as this would prevent attributing actions taken in information systems to a single individual.

Each individual entering information in information systems will sign an a document agreeing:

1. To make complete and accurate entries
2. Not to enter information through the use of his or her own or another individual's user identification code
3. Not to share his or her user identification code or password

Department managers and chiefs are responsible for instructing their staff on the appropriate use of the information systems. Any violation of this policy shall constitute grounds for disciplinary action, up to and including termination.

Draft Confidentiality, Computer Usage, and Accountability Agreement
Kaiser Permanente

Information systems contain confidential information pertaining to members, patients, health care professionals and the organization. This information is a major asset to our organization and is required by law to be protected. The use of a computer network that is shared by many individuals imposes many obligations. A task of our Confidentiality and Security Program is to inform individuals who use computer resources of their responsibilities and to secure their agreement to abide by the associated policies and procedures.

I, _____ (name):

1. will respect the privacy and rules governing the use of any information accessible through the computer system or network and only utilize information necessary for performance of my job,
2. understand that the information accessed through all our information systems contains sensitive and confidential patient, member, business, financial and employee information which should only be disclosed to those authorized to receive it,
3. will not exhibit or divulge the contents of any record or report except to fulfill a work assignment,
4. understand that I may access health information on myself, but must have specific permission to access information on my spouse, teenage children, friends, neighbors, and other physicians or employees,
5. will not release my user identification code or password to anyone, or allow anyone to access or alter information under my identity,
6. understand that my user identification code and password are the equivalent of my signature and that I am accountable for all entries and actions recorded under them,
7. understand that I am responsible for logging out of information systems and will not leave unattended a display device to which I have logged on,
8. understand that all access to information systems will be monitored,
9. will not attempt to access information by using a user identification code or password other than my own,
10. will not remove any records, reports or copies from their storage location except in the performance of my duties,
11. report any violation of confidentiality or computer usage policies,
12. respect the ownership of proprietary software (For example, I will not operate unlicensed software on Company computers or make unauthorized copies of such software for my own use.),
13. respect the finite capability of the systems, and limit my use so as not to interfere unreasonably with the activity of others,
14. abide by the procedures established to manage the use of the system,
15. will only make incidental personal use of these resources,
16. will not use these resources to engage in illegal activities, or harass anyone,
17. prevent unauthorized use of information maintained, stored or processed by the company,

18. will not seek personal benefit of or permit others to benefit personally by any confidential information or use of equipment available through my work assignment,
19. understand that my obligation under this agreement will continue after my termination of employment and that my privileges are subject to periodic review, revision and renewal,
20. understand that violators of this agreement will be denied access to information systems, subject to disciplinary action, including termination and may be subject to penalties under State and Federal laws and regulations.

By signing this, I agree that I have read, understand, and will comply with this agreement.

Signature: _____ Date: _____

Printed Name: _____ Department: _____

Toolkit Section 4.9

Implementing Information Security Practices

In *For the Record: Protecting Electronic Health Information* (1996), The National Research Council Computer Science and Telecommunications Board encourages all health care organizations to implement technical measures for managing data security of the following types:

1. **Strong authentication.** Organizations should adopt authentication systems incorporating single-session or encrypted authentication protocols and token-based authentication systems requiring some type of card, button, or badge in addition to a user password.
2. **Enterprise wide authentication.** Organizations should move toward enterprise-wide authentication systems. These systems concentrate security for many systems in a single authentication transaction in conjunction with other technical and management practices, which ensures good password protection.
3. **Access validation.** Organizations should utilize software tools to ensure that users only have access to information for which they have a right to access.
4. **Expanded audit trails.** All health care organizations should be able to maintain logs of all internal accesses to clinical information.
5. **Electronic authentication of records.** Health care organizations should adopt an electronic signature system; that is, systems with the capability to identify the individual who enters or alters each element of information in the electronic record. Organizations must be aware of any state legal requirements related to electronic authentication.

The CPRI Security Features included below offer guidance in responding to the NRC's recommendations.

Security Features

For

Computer-based Patient Record Systems

Prepared by
CPRI Work Group on
Confidentiality, Privacy & Security

September 1996

Computer-based Patient Record Institute
Creating information solutions for health care

Security Features

For

Computer-based Patient Record Systems

Prepared by
CPRI Work Group on
Confidentiality, Privacy & Security

September 1996

Computer-based Patient Record Institute
Creating information solutions for health care

Computer-based Patient Record Institute
Creating information solutions for health care

Security Features for Computer-based Patient Record Systems
© Copyright 1996, by the Computer-based Patient Record Institute. All rights reserved.

No part of this publication may be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without permission in writing from the publisher.

Printed in the United States of America

This book was prepared camera-ready.

SECURITY FEATURES FOR COMPUTER-BASED PATIENT RECORD SYSTEMS

Overview

The Computer-based Patient Record Institute (CPRI) is a nonprofit organization of stakeholders in health care committed to facilitating development and implementation of computer-based patient records. Computer-based patient records with properly designed and monitored security systems have the potential for improving health care quality, cost, and access while affording greater protection of confidentiality for private health information. CPRI's Work Group on Confidentiality, Privacy, and Security was established as one of the four original work groups to encourage the creation of policies and mechanisms to protect patient and caregiver privacy and ensure information security. It is developing a series of security guidelines and other related documents for organizations implementing computer-based patient record systems.

The following guidelines have been published:

- *Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Record Systems* (February 1995)

- *Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Record Systems* (June 1995)

- *Guidelines for Managing Information Security Programs at Organizations Using Computer-based Patient Record Systems* (January 1996)

Additional guidelines in this series will address:

- Authorization and control of access to computer-based patient records

- Security audit functions and processes

Other associated documents completed by this work group include:

- *Sample Confidentiality Statements and Agreements for Organizations Using Computer-based Patient Record Systems* (June 1996)

Purpose

The purpose of this document is to provide guidance to dove opers of computer-based patient record systmns for design of security features, purchasers of such systems for Specification of security features, and auditors and consultants of such systems for evaluation of security features. This document is not considered or intended to be viewed as an exhaustive list of all security requirements a co nputer-based patient record system should provide, but rather as a document to assist an organization in develop; ng its own set of requirements.

The document contains three distinct sections:

Introduction to Security Features provides an overview to the reader outlining die scope and context of the document.

Description of Security Features provides a narrative discussion of the key areas related to security features which should be considered when developing, selecting, or evaluating a computer-*based patient record system.*

List of Security Features displays security features in a format which may be amenable for use in development, selection or evaluation of the security features of a computer-based patient record system.

In addition to references used in this document, a list of additional resources relative to applicable standards developed in other industries or for other health care purposes is also provided.

Acknowledgments

This document was prepared by members of the Work Group on Confidentiality, Privacy, and Security, Kathleen Frawley and Dale W. Miller, co-chairpersons, and Cynthia Miller, project team leader.

In addition to the 58 member organizations of CPRI and the over 300 participants in its Work Group on Confidentiality, Privacy, and Security who contributed significantly to the development of this work, CPRI extends appreciation to two of its member organizations who provided copies to their members for review and input: the Center for Healthcare Information Management (CHIM) includes nearly 100 member organizations representing vendors of health information technology and the College of Healthcare Information Management Executives (CHIME) includes approximately 525 chief information officers in health care provider organizations.

Table of Contents

Overview iii

Purpose iii

Acknowledgments iv

Introduction to Security Features 1

Description of Security Features 3

- Security 3
- Authentication 3
- Authorization 4
- Integrity 5
- Audit Trails 5
- Disaster Prevention/Recovery 6
- Data Storage and Transmission 6

List of Security Features 7

References 15

Additional Resources 17

SECURITY FEATURES FOR COMPUTER-BASED PATIENT RECORD SYSTEMS

Introduction to Security Features

Today's health care industry is striving to achieve the development and deployment of computer-based patient records for improvements in health care quality, cost, and access, Towards this objective, vendors are developing and health care organizations are selecting and implementing computer applications and comprehensive systems which will support these efforts. These systems are being evaluated based on a number of essential criteria; one of which is their ability to support the security requirements necessary to ensure the integrity and confidentiality of health information to protect the privacy and certain legal 6tercsts of patients, providers, and health care organizations,

A computer based patient record is defined by the Institute of Medicine as "an electronic patient record that resides in a system designed to support users through availability of complete and accurate data, practitioner reminders and alerts, clinical decision support systems, links to bodies of medical knowledge, and other aids." The Institute of Medicine also defined the computer-based patient record system as "the set of components that form the mechanism by which patient records are created, used, stored, and retrieved ... [including] people, data, rules and procedures, processing and storage devices, and communication and support facilities." (Dick and Steen, 1991).

A computer-based patient record is electronic maintained information about an individual's lifetime health status and health care. It replaces the paper medical record as the primary record of care, meeting all clinical, legal, and administrative requirements. It is more than the content of toda3e$ paper medical record. Information technology can merge text with images and sound, It facilitates access, upon patient authorization, for legitimate users, to health data stored in multiple, dispersed locations. (CPRI, May 1996). Such access to data contributes to continuity of healthcare. Longitudinal health data, reminders and alerts, linkages with knowledge sources for decision support, and enhanced outcomes research support quality improvements, wellness promotion, and clinical research and education. Complete and accurate data for all health care encounter, reduction in redundant data collection, and elimination of repetitive testing contribute to productivity gains, reduced rest, and improved management of the health care delivery system. Integration of health data with administrative and legal data supports the business operations of the health care provider and secondary uses such as insurance authorization, claims adjudication, and reimbursement; public health reporting; and continuing education. Enhanced communication among caregivers and documentation of an individual's health status also support consumer health education and continuity of care.

Computer-based patient record systems can provide greater protection of confidentiality and data integrity than paper medical when security systems are properly designed and monitored because access is more controlled, data itself may be protected directly through encryption, audit trails provide a record of all access, and entries are unalterable. CPRI has developed a number of guidelines to assist in the development of security policies governing creation, authentication, and retention of health information; description of the authority and responsibility for a security manager; creation of procedures and sample agreements for access, release, disclosure, and amendment to health information; and guidelines for developing security educational programs. CPRI has developed this document to assist in formulating specific security design requirements. (CPRI's effort in this area is to provide a tool, rather than an exhaustive document to be used in its entirety, for:

- developers to design security features,
- purchasers to specify security features, and
- auditors and consultants to evaluate security features.

Any provider or other entity which acts as the custodian of health information must engage specific security features to physically @ locations for data system components, identify authorized users, control and ensure authorized

local and remote user access to internal and external sources of data, control input and amendment of data by users, control outbound data transmission, ensure data integrity, ensure information and process completeness, manage database backup and recovery, and ensure data system availability and reliability. System performance should not deter implementation of security features.

Description of Security Features

Security *is the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats*. (National Research Council, 1991).

In today's dynamic health care environment, disparate mforrnatio4 systems arc coming together to form computer-based patient record systems intent on supporting the ongoing maintenance of a longitudinal record for quality patient care. Computer-based patient record systems must include a variety of security features to protect the confidentiality and integrity of health information to preserve the privacy and property rights of patients, providers (individual caregivers and enterprises), and others who interact with the computer-based patient record.

All health plans, clearinghouses, and providers must ensure the confidentiality of patient and provider-identifiable health information through appropriate security in all aspects of the information system - from the lowest layer of data transport (e.g., cables, switches, routers, transmitters), through the network layer, information layer (of databases, file servers, and electronic libraries), and software applications layer, to the management layer of operations and administrative structures and processes that establish and monitor security policies. The instant availability of verifiably correct and complete patient information is critical to ensure the well-being of the patient and to protect die health care enterprise from costly claims. The need to assure that no patient's life is endangered due to information-system error or failure to conform to security policies are critical concerns m health care. Health care enterprises also have an obligation to protect the intellectual property associated with providers and the operation of the enterprise. (Reference *Glossary of Terms Related to Information Security,* CPRI, July 1996, for comprehensive definitions and relationships among privacy, confidentiality, and security.)

The essential features of a secure system and network may be categorized as: *authentication, authorization, integrity, audit trails, disaster prevention/recovery, and secure data storage and transmission.*

Authentication

Authentication *refers to providing assurance regarding the identity of a subject or object For example, ens uring that a particular user is who the user claims to be (authentication of user) and corroboration that the source of data is received as is claimed (authentication of data origin).* (ASTM El 762)

A method for secure authentication is essential in a computer-based patient record system, as life-altering decisions are made based upon information maintained in the system. Individual users are held accountable for the health information they enter, amend, validate, and view within a system. Therefore, each user must be uniquely identified to the system. Specific policies within the organization should specify the disciplinary actions and penalties for sharing any unique identifier with other individuals. (Reference G*uidelines for Establishing Information Security Policies at Organizations Using Computer-Based Patient Records,* CPRI, February 1995, for further information on policy development.)

Authentication can be accomplished through biometric identifiers (e.g., fingerprint, retinal scan, voiceprint); use of a smart card, token, or other physical thing one possesses: a password; or a combination thereof. One of the most prevalent means of user-identity authentication used in health care system is the entry of passwords. However, if p are stored on the system they must be encrypted. Consideration should also be given to the pros and cons of user assignment vs. random assignment of password components. All passwords should be scheduled to expire at routine intervals.

Passwords are commonly implemented as a set of user identification codes and passwords. A user identification code is used to identify a user to the system and to other users. The user identification code provides the relationship the user and what information the user may access. A password is a string of characters that in conjunction with other information, such as user identification code, uniquely confirms the user's identity to the system, (Marotta, 1986) A password may be chosen by the user or assigned by the system. When security devices are used, they are encoded with the user identification code (or an encrypted or indirect reference to it) but not the password. Every effort should be made to establish a user identification code and password system for the computer-based patient record that eliminates multiple logons for the user.

Once a user has been authenticated, ensuring that the current user is still the authenticated user must be addressed. M g the opportunity for an unauthenticated user to utilize another's access can be supported through the use of automatic logoff after a stated period of inactivity or when the authenticated user accesses the system from another terminal. The logon and logoff processes should be quick and efficient to help ensure that users comply with the requirement that they logoff following completion of their terminal activity.

Authorization

Authorization *is the granting of rights, which includes granting of access based on access rights.* (ISO 7498-2)

Authorization provides that an authenticated user has access to the functions, information, and privileges which the user is requesting the system to provide. Authorization to access a system includes both authorization to gain physical (or connectivity) access and authorization to gain access to resources contained within the system. It also provides evidence of action on data. Authorization is accomplished through access controls, confidentiality services, and non-repudiation (or attribution) services.

Access control services protect against unauthorized access to any system resource, including the computer system, network, software application programs, sad data files. Access control services assure that people, computer systems, and programs can use only those resources they are authorized to use and only for the purposes for which they are authorized. Access controls also protect against unauthorized use, disclosure, modification, and destruction of resources. Various forms of access controls (e.g,, identity-", label-based, and role-based) have been developed in other industries and should be evaluated for use in health care.

Confidentiality services protect against die disclosure of information to entities not authorized to have that information. (Baker and Cooper, 1995). Locally, access controls placed on data files can protect them from being read by unauthorized users or groups of users. Such access controls can protect die data, and the attributes associated with data files (existence, size, and variations). Confidentiality services can also provide for removal of data from storage media so they may not be read after memory or files have been (appropriately) "deleted," Confidentiality services must also be instituted within a network environment. The most common form of confidentiality service over a network is encryption.

Non-repudiation services assure that information that purports to be from (or purports not to be from) and actions that purport to have been performed by (or purports not have been performed by) a user or system are as claimed. (Baker and Cooper, 1995) In other words, non-repudiation services provide evidence to prevent a person from unilaterally modifying or terminating obligations arising out of a transaction effected by computer-based means. Repudiation is a threat in which an individual falsely denies having token an action. A non-repudiation service does not eliminate repudiation, but ensures the availability of evidence to support resolution of any disagreement. The most used mechanisms for providing evidence that an individual did (or did not do) a particular act are encryption (digital signatures) and audit trails.

Integrity

Integrit*y is the property that information is changed only in a specified and authorized manner. Data integrity, program integrity, system integrity, and network integrity are all relevant to consideration of computer and system security.* (National Research Council, I 991)

Data integrity refers to the accuracy, consistency, and completeness of data. Corruption of health information system compromise the quality of data and may lead to challenging the correctness of the information provided by the system. Such data errors may lead to erroneous actions by caregivers who base diagnosis and treatment decisions on data provided through the system. Data integrity measures ensure that data have not been altered or destroyed in an unauthorized manner. A data integrity control policy has at least four essential components: security measures, procedural controls, assigned responsibility, and audit trails (Dick and Steen, 199 1). To ensure the integrity of information, unauthorized deliberate or accidental modification or entry of data must be prevented. Moreover, the source, date and time, and content of any alterations must be known. Therefore, additions and alterations must be traceable to the source. Further, information regarding such alterations must be attainable by the user of the information. All time sources should require secure synchro4ization to avoid erroneous times and dates.

Program integrity refers to the quality of software design and protection against modification. Software "bugs" and software design complexity can contribute to corruption or loss of information. Effective software development tools must be used to design application systems. Maintaining separate hardware domains for the operating system and application programs is essential for protecting critical code and data structures from external interference.

System integrity is the capability of an so system to perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation. Hardware and software features should be used to periodically validate the correct operation of the hardware elements of the system. In addition, sound back-up and recovery are very important to enable a system to recover quickly and securely in the event of a system failure.

Network integrity extends system integrity to interconnected local and wide area networks.

Audit Trails

*An **audit trail** is the result of monitoring each operation on information.* (National Research Council, 1991)

An audit trail is a chronological record of activities occurring in the system, created immediately concurrent with user . Audit trails can be examined to detect and investigate breaches m security, determine compliance with established policy and operational procedures, and enable the reconstruction of a sequence of events affecting the information.

Audit trail records contain identification of the user, data source (for automated devices), person about whom the health information is recorded, provider facility, and other participant users if applicable. Audit trail records also contain the date/time and location of the activity, and the nature of the activity (i.e., function performed and information accessed). (Dickinson, 1996)

Audit trails track access to view content; to create content (including that to update, modify, append, or import from other systems), and to copy to external media or export to other systems. Audit trails also track the progress of each operation from the point of initiation through event steps, to terminal state (e.g., complete, resolved, canceled).

Disaster Prevention/Recovery

Disaster recovery *is the process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.* (CPRI, July 1996)

To ensure the safety and prevent the potential loss of data, the computer-based patient record system needs to support the organization's detailed disaster recovery plan. This inc4udes measures to protect health information from damage, minimize disruption, ensure stability, and provide for orderly recovery in the event of a disaster, such as flood, fire, etc.

The system needs to support redundancy of "em components such as processors, network links, and databases. The system must support making backup copies of information without impacting system functions, and support recreating information from back ups.

Data Storage and Transmission

Data storage *refers to the physical location and maintenance of data.* (CPRI, September 1996) *Transmission of data is the exchange of data between person and program, or program and program, when the sender and receiver are remote from each other.* (Longley, 1987)

Physical location considerations include physical security for processors, storage media, cables, terminals or workstations, etc. Physical attributes of the storage media refer to permanence and durability. Ongoing system maintenance, precautions against sabotage, and updating obsolete systems are also considerations of data storage relating to the trustworthiness of computer records for purposes of producing health information that is admissible as evidence in court (Waller, 1991). Retention is also an aspect of data storage that is often governed by legal and regulatory requirements, as well is provider policy @h may be established based on requirements for use in patient care, research, and educational purposes. Retention refers to preservation of information in some form for a given period of time (Abdelhak, l996).

Data transmission is critical to the implementation of a computer-based patient record system. Today's health care environment requires the use of disparate source for capturing health-related information. This information is also shared these source systems to provide information to internal users as well as external requesters, payers, etc. Data may be accessed via remote Workstations, the Internet, and complex networks supporting one or more organizations, and potentially within a national information infrastructure.

Systems to support such data transmission must provide critical security functionality to ensure that the integrity and confidentiality of the data are maintained. The security features integral to computer-based patient record systems must be designed to provide for the security of the network included in the system and to manage the security of interfaces to external networks.

Encryption should be considered for protecting information when it is not possible to maintain control of the physical storage media or the transmission network. When property implemented, encryption offers the potential to provide cost-effective protection of health care information from both unauthorized disclosure and from unauthorized changes during transit. Additionally, the direct connection of systems to the Internet require the implementation of a “firewall” to serve as a control point and filtering mechanism. The organization's plan should also address remote access and the technologies that are incorporated to ensure security.

List of Security Features

Following is a fist of features designed to assist in the development of security requirements which may be adopted for any computer-based patient record system. All features may not be applicable for all applications; and the list is not necessarily exhaustive. The list 4nplies no prioritization. A thorough review of all state statutes and regulations should be done prior to adopting any security features for any product or application.

Section I. Authentication Features

Description	Provided	Comments
1. System provides for the use of both a user identification code and password to verify authorization to access the system.		
2. System supports the use of additional user authentication devices such as tokens, smart cards, badge readers, signature verification, one-time password generators, biometric identifies, dial-back modems, etc. in addition to the user identification code and password.		
3. System permits the use of alphanumeric user identification codes.		
4. Identification codes are used only to represent one person.		
5. System permits user identification codes of sufficient length to permit the organization tot assign a unique user identification code to each user.		
6. System permits passwords of sufficient length to permit unique passwords for every user.		
7. System permits the use of passwords containing combinations of alphabetic, numeric, and special characters.		
8. System permits the specification of password editing rules.		
9. System permits the security administrator to specify a minimum password length that will be enforced by the system.		
10. System permits the security administrator to reset passwords to a unique value.		
11. System permits specifying a minimum password length on a per user basis.		
12. System permits users to choose their own passwords without assistance or involvement of a security administrator.		
13. System forces user to select a password at initial sign-on and when the password has been reset.		
14. System provides password management function to allow password change to be announced a variable number of days before it becomes mandatory.		
15. System permits users to change their passwords at will.		
16. System prohibits the reuse of user identification codes.		

Section I. Authentication Features

Description	Provided	Comments
17. System prohibits the reuse of passwords per user.		
18. System provides for comparing user suggested passwords with dictionary entries to prohibit weak passwords prior to accepting the password change.		
19. System permits the security administrator to specify a password expiration interval.		
20. System permits specifying a password expiration interval on a per user or per class of user basis.		
21. System automatically prompts users to enter a new password upon password expiration.		
22. System permits security administrator to specify that a users password has expired.		
23. System permits security administrator to specify a date or time limit for expiration of a users access privileges.		
24. System provides messages to user upon denial of access due to an invalid user identification code or password.		
25. System supports automatic disabling of a user identification code after a predetermined, system administrator-defined, number of consecutive invalid access attempts..		
26. System provides the ability to inform user of the last time the system was accessed with that user identification code.		
27. System supports the encryption of the password file or the password information.		
28. System administration function s are separate from system operation, management, and maintenance functions.		
29. System prevents system support and maintenance personnel from accessing patient's data.		
30. System supports s hierarchy of security administration.		
31. System is designed t permit highest level security administrators to delegate specific security administration functions to departmental security administrators.		
32. System provides for multiple security administrators to be assigned the highest level of authority.		
33. System permits security administrator to disable a user identification code without deleting it from the system.		
34. System supports the real time disabling of a user identification code.		
35. System permits the security administrator to force immediate sign off of a user.		

Section I. Authentication Features

Description	Provided	Comments
36. System allows security administrator to define a period after which an unused user identification code is automatically disabled and notice is provided to the security administrator.		
37. System provides a system administrators functions for monitoring devices, sign ons by function/sub-function.		
38. System provides security features associated with dial-up diagnosis (of system trouble) capability.		
39. System supports the security administrator's ability to define and control vendor access.		
40. System provides reports of current inventory of users, IDs, and access authorities.		
41. System provides tools for batch and on –line management of IDs.		
42. System provides for security control of all batch jobs, started tasks, and data access by each end user, application and subtask on an platform.		
43. System provides uniform security controls and password management functionality on multiple and varied hardware and operating systems.		
44. System accommodates single sign on identification and password across all platforms.		
45. System supports transaction authentication.		
46. System supports authentication of network connections by systems, programs, and intelligent agents.		
47. System provides for dynamic reconfiguration based on administrator requirements (e.g., immediately or deferred).		
48. System provides capabilities for controlling an isolating network components.		
49. System provides means to control and detect changes to the network configuration.		
50. System can accommodate the user identification code and password being passed to it by an external security brokering agent including, single .log on.		
51. System provides reporting and maintenance tools for the security administrator.		

Section II. Authorization Features

Description	Provided	Comments
1. System allows defining access to specific data elements, files, functions, menus, commands, and networks based on user's patient care responsibilities or job function, including but not limited to: By user: a. System Manager b. Technical (programmer) c. Operator d. Department Manager e. Supervisor f. End-user – departmental personnel g. End-user – other hospital personnel (nursing, etc.) h. End-user – enterprise wide		
2. System supports defining groups of users to be granted access to specific data elements, files, functions, menus, and commands or collections of these.		
3. System permits the security administrator to grant specific users the authority to permit other users to access specific data items, menus, or functions.		
4. System supports the encryption of sensitive data and keky management tools to support the encryption methods.		
5. System has a time-out feature that automatically signs a user off if a terminal has been left unattended for an organization-define time period.		
6. System supports the designated length of the time-out feature by system module, terminal location and user, or a combination.		
7. System time-out parameters can be modified without changing a hard-coded program.		
8. System allows user to restrict printing and display of confidential data elements.		
9. Systems can determine who is accessing a patient's record at any point in time through on-line inquiry.		
10. System prevents access to functions without logging in through the security system.		
11. System prevents inquiry to certain data elements based on the value of that field.		

Section II. Authorization Features

Description	Provided	Comments
12. System prevents user from seeing menu items, screen formats, report forms if user's security profile prevents them from access in the data elements associated with these system components.		

Section III. Integrity Features

Description	Provided	Comments
1. System provides control over stored data to ensure data is complete and internally consistent.		
2. System provides user-definable screen and report prompts that will indicate missing or critical information.		
3. System provides data management features that eliminate the redundant maintenance of duplicate patient data.		
4. System provides the ability to store all rejected transactions along with a reason for the rejection.		
5. System supports anti-virus software.		
6. System is protected from unauthorized access via Internet through the use of firewalls, cryptography , and authentication devices.		
7. System provides mechanism for controlling simultaneous updates to the database.		

Section IV. Audit Trail Features

Description	Provided	Comments
1. System supports alarm features to provide immediate notification of predefined events, including the events recorded in the audit logs.		
2. Audit trails can be produced to identify: a. all users who have used a selected function b. all activity of a given user c. all areas accessed via communications links d. all users who have signed on the system with date, time, and location or mode of sign on (port, terminal dial-up, LAN) e. users who have singed off system with date/time of sign off f. all detected attempts at unauthorized access including user identification code and invalid password, with date, time and location. g. all modifications to security settings and parameters all changes to access authorities, including creating, disabling and deleting user identification codes h. all changes to access authorities, including creating, disabling and deleting user identification codes i. access via the remote diagnostic capabilities j. use of debugging tools which may modify data, the operating system or application programs j. all commands to enable and disable logging of activities		
3. System prevents deletion, overwriting, or unauthorized modification of audit trails.		
4. System provides the ability system logs and reports all		

	violations of system security procedures.		
5.	System provides management reports of security access.		
6.	System provides the ability to display organization defined security messages.		
7.	System allows sign on identification to tag on-line transaction audit records for reporting capabilities.		
8.	System supports separate files or transactions to allow training without corrupting the operational database.		
9.	System log facilities trace all production changes in organization's environment,.		
10.	Application –level changes (e.g., destination table, routing tables) can be easily moved into production with not need to disable production environment. Such changes can be readily backed out.		
11.	System supports the ability to use third-party audit packages.		
12.	System provides audit reports of file changes, journal entries, exceptions, validation changes, error reports, etc.		

Section V. Disaster Prevention / Recovery Features

Description	Provided	Comments
1. System provides a backup process that can be performed in a dynamic mode so that the system can be operational 24 hours per day.		
2. File backup procedures are provided.		
3. System provides a data archiving process based on system administrator criteria (e.g. time, data type, discharge, disposition).		
4. System supports disaster recovery procedures.		
5. In the event of hardware/software failure, system can recover to the point of failure.		
6. System supports disk mirroring or shadowing for security downtime processing, error recovery, etc.		
7. System provides sufficient back-up and recovery feature to assure no data loss after system failure..		

Section VI. Data Storage and Transmission Features

Description	Provided	Comments
1. System supports ability to control import and export of data.		
2. System provides interface to allow archival of data.		
3. System security maintained when integrating and communicating with systems outside the vendor's solution..		
4. System provides ability to encrypt data..		
5. Secure dial-in access, unique user IDs and passwords, limited access times, and limited connection duration are incorporated for remote access.		

References

Abdelhak M (Ed.), 1996 *Health Information: Management of a Strategic Resource.* Philadelphia: W.B. Saunders Company.

ASTM E1762. *Guide for Electronic Authentication of health Care Information.* Committee E-31 on Computerized Systems, Subcommittee E31.20 on Authentication. West Conshohocken, PA: ASTM, Oct. 10, 1995.

Baker DB, Cooper T, 1995. *Information System Security Issues for Health Care.* Draft. Science Applications International Corporation and Kaiser Permanenente.

CPRI, May 1996. *Computer-based Patient Record Description of Content* Work Group on CPR Description, Schaumburg, IL: Computer-based Patient "rd Institute.

CPRI, September 1996. *Computer-based Patient Record System Description of Functionality.* Work Group on CPR Description, Schaumburg, IL: Computer-based Patient Record Institute.

CPP L July 1996. *Glossary of Terms Related to Information Security for Computer-based Patient Record Systems.* Work Group an Confidentiality, Privacy & Security, Schaumburg, IL: Computer-based Patient Record Institute.

CPRI, February 1995. *Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Records.* Work Group on Confidentiality, Privacy & Security, Schaumburg, IL: Computer-based Patient Record Institute.

Dick RS, Steen EB (Eds.), 1991. *7he Computer-based Patient Record., An Fssential Technologyfor Health Care.* Washington, DC: National Academy Press.

Dickinson, GL, 1996. "Comments on System/Application Functional Requirements Related to Security of Computer-based Patient Records." Commentary.

ISO 7498-2. *Information Processing Systems - Open Systems Interconnection - Basic Reference Model Part 2: Security Architecture.* International Standards Organization, 1989.

Longley, D. *Data & Computer Security: Dictionary of Standards, Concepts, and Terms.* UK: MacMillan.

Marotta, RE (Ed). The *Digital Dictionary,* Bedford, MA: Digital Equipment Corporation.

National Research Council, 199 *1. Computers at Risk.- Safe Computing in the Information Age.* System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications. g, DC: National Academy Press.

Waller, A, 1991. "Legal Aspects of Computer-based Patient Records and Record Systems," Appendix B, *7he Computer-based Patient Record.- An Essential Technology for Health Care.* Dick RS & Steen EB (Eds.), Washington, DC: National Academy Press.

Additional Resources

The following organizations have also been involved in developing security requirements for computers in general and for health information systems in particular. *CPPJ does not guarantee that this list is a comprehensive survey of all organizations having done work in this area. Suggestions for inclusion are welcome,*

Organization	**Work Effort**	Telephone Contact
Information Technology Industry Council	ASC X3.92 Data Encryption Algorithm (DEA) ASC X3 106 Modes of Operation of the DEA	202-737-8888
American Bankers Association	ASC X9F Data & Information Security Standards	800-338-0626
Data Interchange Standards Association (DISA)	ASC X12N Electronic Data Interchange, Insurance Subcommittee EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport)	703-548-7005
Department of Defense	Trusted Computer System Evaluation Criteria ("Orange Book")	Government Printing Offices
American College of Radiology and National Electrical Manufacturers Association	DICOM standard for digital imaging and communications with PACS	202-457-8400
American Society for Testing and Materials (ASTM)	E31 Healthcare Informatics Committee E1384 Standard Guide for Description of Content and Structure of the Computer-based Patient Record E1714 Guide for Properties of a Universal Healthcare Identifier E1762 Guide for Electronic Authentication of Health Care Information E1769 Guide for Properties of Electronic Health Records and Record System	610-832-9585
Computer-based Patient Record Institute	Security Guidelines for Organizations with computer-based patient records	301-657-5918
Health Care Financing Administration	Provider identification standards	410-966-5318
Health Industry Business Communications Council (HIBCC)	Standards for site of care and supplier labeling identifies	602-381-1091
Health Level Seven (HL7)	Application protocol for electronic data exchange in health care environments	313-677-7777
Institute of Electrical & Electronic Engineers (IEEE)	IEEE/MEDIX standards for medical data interchange	908-562-3814
National Council for Prescription Drug Programs	Standards for pharmaceutical billing transactions	602-957-9105

CPRI Members

3M Hlth Info Sys
Adventist Hlth Sys/Sunbeft
ALLTEL Info Svcs - Hlthcare Div
Amer Acad of Family Physicians
Amer Acad of Pediatrics
Amer Assn for Med Transcription
Amer Board of Family Practice
Amer College of Physicians
Amer Hlth Info Mgmt Assn
Amer Hospital Assn
Amer Med Informatics Assn
Amer Medical Assn
Amer Org of Nurse Executives
Andersen Consulting, LLP
Arkive Information Systems
Assn of Operating Rm Nurses
Chi Systems
Coll of Amer Pathologists
Coll of Hlth care Info Mgmt Execs
Columbia/HCA Hlth care
Dept of Veterans Affairs
Dynamic Hlthcare Tech
Eli Lilly and Company
Ernst & Young, LLP
Harvard Comm Hlth Plan
HBO & Company
Hlth Industry Mnfrs Assn
Hlth Level Seven
HEALTHPOINT
HealthVISION Corp
Hewlett-Packard
IBM Healthcare Solutions
IDX Systems corp
Inst for Clin Sys Integ
JCAHO
Kaiser Permanente
Management Systems Assoc
Mayo Foundation
Medic Alert Fnd US
Medical Connections
Medical Records Inst
MedicaLogic
Medicus Systems
Natl Assn of Chain Drug Stores
Natl Cncl for Pres Drug Progs;
NC Hlth Care Info & Comm AlInce
NEON Hlth care Softmre
Northwestern Memorial Hosp
Oceania
PHAMIS
Prudential Insurance Co
Sisters of Mercy Hlth Sys
Systems Plus
The Permanente Med Group
Unitron Med Comm
Univ Hlth System Consortium
Univ of VA Hlth Sci Ctr

CPRI is a nonprofit membership organization committed to advancing improvements in health care quality, cost, and access through routine use of information technology. CPRl serves as a neutral forum for bringing the diverse interests of all health care stakeholders together to develop common solutions.

CPRI functions primarily through the voluntary work of its work groups. All individuals are invited to participate in one of the following:

- Work Group on Codes & Structures
- Work Group on Confidentiality, Privacy & Security
- Work Group on CPR Description
- Work Group on CPR Systems Evaluation

Toolkit Section 4.9.2

Special Issues in Electronic Transmission of Confidential Data

In addition to general elements of a technical data security infrastructure, health care providers should be aware of the risks and approaches to managing the risks of electronic transmissions of confidential patient and business information between organizations. Powerful tools such as facsimiles, e-mail and the Internet pose challenges that must be addressed. Discussions of important recent developments on these issues follow, including AHIMA recommendations for appropriate approaches to using facsimile (Fax) transmissions, HCFA's new rules for using the Internet, and PCASSO project for providing secure patient use of the Internet. The Health Care Finance Administration has taken an active interest in provider's use of the Internet.

Toolkit Section 4.9.2.1

Facsimile (Fax) Transmissions

Facsimile (Fax) transmission of documents has been widely used for many years in health care. In a paper environment, faxing provides a fast and economical means of communication among multiple providers. Fax technology accommodates text, graphics, and images, is relatively cheap, and is easy to install and use. It does, however, have some serious liabilities. Printout quality has improved over the years but many machines still do not provide adequate print quality. The major liabilities are misdirection and poor monitoring practices for receiving transmissions. While technology brings many advantages, a major challenge is incorporating it into the business workflow effectively and utilizing it appropriately.

Faxing is fast and efficient from the viewpoint of the sender. Modern machines can store many transmissions in a memory queue so that work proceeds at an efficient pace. Copies do not have to be made because originals can be fed into the machine. That saves time for the sender. Misdirection may occur by misdialing the fax number, miscopying a fax number, or obtaining a wrong fax number, among other ways. Misdirection is a serious problem because confidential patient information is delivered into unauthorized hands.

> *Former IDN CIO routinely receives misdirected faxes at his home from a local physician's office. He has called the office on multiple occasions as well as faxed the office back regarding their misdirected transmissions. The physician's office continues to fax him patient information.*

Faxing can be very inefficient on the receiving end. Fax machines are routinely shared by many people and typically installed in a centralized, high traffic area. High volume fax machines need constant tending, as paper will overflow. As transmissions print out open face, confidentiality is difficult to maintain. Proper procedures require calling the intended recipient to stand by for the delivery so confidential information does not sit on the machine, available to unauthorized personnel. In real practice, this is the exception rather than the rule.

> *New Director of a Health Information Management Department walked into the overcrowded Release of Information area to familiarize herself with procedures. The fax machine sat on top of a file cabinet and was busy pumping out the receipt of a very large transmission of a patient record. The fax receiving tray was filled to overflowing and portions of the fax were falling from the top of the file cabinet neatly into the wastebasket serendipitously placed on the floor beneath.*

Auto-faxing and automated document distribution systems use fax technology as part of their distribution services. When using this technology, procedures should be in place to provide test faxes for every new fax number entered into the system. This requires not only a feature to provide testing capability, but also human verification by both sender and receiver that the transmissions are occurring accurately.

AHIMA recommends transmission of health records by fax only in urgent health care situations or when third party payors require immediate information for certification of ongoing care for a hospitalized patient. AHIMA has published an excellent resource that addresses practical and legal issues of faxing. A summary follows of *Faxing Safeguards: Guidelines for Transmitting Patient Health Information by* Mary Brandt, MBA, RRA, CHE, AHIMA 1997.

Background

"Each provider should develop policies and procedures for transmitting health information via facsimile that protect patient privacy and comply with legal, regulatory and accreditation requirements."

Regulatory and Accreditation Requirements

Many states restrict the transmission of certain types of health information, such as information relating to AIDS, HIV, or behavioral health services.

Medicare conditions of participation for hospitals do not specifically allow or prohibit facsimile transmission.

The Bureau of Policy Development of HCFA permits the transmission of physicians' orders by facsimile. If the original was signed, they do not need to be resigned.

Legal rules of evidence either based on the Uniform Rules of Evidence or Uniform Photographic Copies of Business and Public Records Act have been used by many states to address admissibility of facsimile.

AHIMA Recommendations

AHIMA recommends facsimile transmission of heath information only when the original record or mail-delivered copies will not meet the needs of immediate patient care. "The sensitive information contained in health records should be transmitted via facsimile only when: 1) urgently needed for patient care, or 2) required by third-party payer for ongoing certification of payment for a hospitalized patient."

The information should be limited to what is necessary to meet the requester's needs. Routine disclosure of information should be made though regular mail or courier.

Autofaxing, which allows automatic facsimile transmission of reports, should be set up carefully to ensure what is needed for patient care and that correct facsimile numbers are contained in the system.

Authorizations

Authorizations for disclosure may be transmitted by facsimile.

Confidentiality Notice

A cover letter should accompany each transmission and include:

- Date/time of transmission
- Sending facility's name, address, telephone, and facsimile numbers
- Authorized receivers' name
- Number of pages transmitted
- Confidentiality notice, including instructions on redisclosure and destruction

Misdirected Transmission

There should be a procedure to investigate the situation when a facsimile transmission fails to reach the recipient. The internal logging system of the facsimile machine should be checked to obtain the number to which the transmission was sent. If the number was incorrect a facsimile should be sent to that number explaining that the information was misdirected and asks for the documents to be returned by mail to the sending facility and your risk manager should be notified.

Receipt of facsimile documents containing health information

A procedure should be in place to:

- Ensure accountability for monitoring the facsimile machine
- Remove documents promptly
- Check for completeness and legibility
- Notify senders of problems
- Follow the instructions on the cover page
- Arrange for secure delivery of the documents

Facsimile documents may generally be included in the patient's health record. Some states may prohibit this.

Facsimile Policy and Procedure

1. Limit use to urgent situations
2. Ensure appropriate location of facsimile machines
3. Assign accountability for managing each facsimile machine
4. Define appropriate safeguards to ensure transmissions are sent to the appropriate individual
5. Define procedure for inclusion of facsimile documents into a patients health record
6. Define procedures for cases of misdirected transmissions and receipts

Authorization for Disclosure of Health Information

1. I hereby authorize _____[name of provider]_____ to disclose the following information from the health records of:

   Patient Name: _____ Date of Birth
   _____

   Address: _____ Telephone
   _____

   _____ Patient Number
   _____

   covering the period(s) of health care

   From (date) _____ to (date)_____

   From (date) _____to (date)_____

2. Information to be disclosed:
   - ☐ complete health record(s)
   - ☐ progress notes
   - ☐ discharge summary
   - ☐ laboratory tests
   - ☐ history & physical examination
   - ☐ X-ray reports
   - ☐ consultation reports
   - ☐ photographs,videotapes, digital or other images
   - ☐ other (please specify) _____

   I understand that this will include information relating to (check if applicable):
   - ☐ acquired immunodeficiency syndrome (AIDS) or infection with human immunodeficiency virus (HIV)
   - ☐ behavioral health services/psychiatric care
   - ☐ treatment for alcohol and/or drug abuse.

3. This information is to be disclosed to _____ for the purpose of _____.

4. I understand this authorization may be revoked in writing at any time, except to the extent that action has been taken in reliance on this authorization. Unless otherwise revoked, this authorization will expire on the following date, event, or condition:
   _____.

5. The facility, its employees, officers, and physicians are hereby released from any legal responsibility or liability for disclosure of the above information to the extent indicated and authorized herein.

Signed: _____
(Patient) (Date)

_____
or (Legal Representative) (Relationship to Patient) (Date)

_____
(Signature of Witness) (Relationship to Patient) (Date)

Note: This sample form was developed by the American Health Information Management Association for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

FACSIMILE COVER LETTER

[sending facility name]
[address]
[city, state, zip code]
[telephone number]
[facsimile number]

DATE: _____ TIME:_____ NO. OF PAGES: _____

TO: _____(name of authorized receiver)_____

_____(name of authorized receiver's facility)_____

TELEPHONE: _____FAX: _____
(of receiver) (of receiver)

FROM: _____(name of sender)_____

TELEPHONE: _____FAX: _____
(of sender) (of sender)

COMMENTS:

*****CONFIDENTIALITY NOTICE*****

The documents accompanying this telecopy transmission contain confidential information belonging to the sender that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party and is required to destroy the information after its stated need has been fulfilled, unless otherwise required by state law.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this telecopy in error, please notify the sender immediately to arrange for return of these documents.

Note: This sample form was developed by the American Health Information Management Association for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Letter for Misdirected Fax

FACSIMILE COVER LETTER

[sending facility name]
[address]
[city, state, zip code]
[telephone number]
[facsimile number]

DATE: _____ TIME: _____ NO. OF PAGES: _____

TO: Recipient at 999/999-9999

FROM: _____
(name of sender)

TELEPHONE:_____ FAX: _____
(of sender) (of sender)

COMMENTS:

We believe that information on one of our patients was transmitted to you in error. This is confidential information, belonging to *[name of sender]* that is legally privileged. Please return these documents to us immediately by mail. Thank you.

*****CONFIDENTIALITY NOTICE*****

The documents accompanying this telecopy transmission contain confidential information belonging to the sender that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party and is required to destroy the information after its stated need has been fulfilled, unless otherwise required by state law.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this telecopy in error, please notify the sender immediately to arrange for return of these documents.

Note: This sample form was developed by the American Health Information Management Association for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Toolkit Section 4.9.2.2

E-mail

Electronic-mail or e-mail is a fast growing technology in health care. As health care organizations implement electronic systems, they frequently choose e-mail as the introductory vehicle as it provides instant value to most new users. E-mail is comparatively easy to learn, even for the most technically challenged, and can provide a sense of immediate benefit. Patients are also putting pressure on providers to expand their capabilities to e-mail. Some health care organizations even publish e-mail procedures for patients on their Web sites. [See. Stanford Medical Group at www.med.standford.edu/shs/smg/e-mail.html.] Industry standards for e-mail require client software that is compliant with S/MIME, (Security/Multipurpose Internet Mail Extensions), a protocol that adds digital signatures and encryption to Internet MIME. There are no additional hardware requirements.

Benefits

E-mail potentially offers many benefits to health care providers.

1. E-mail improves ease of communication across a multiprovider setting. By allowing the sender and receiver to process communications at their convenience, 24 hours a day, seven days a week, e-mail eliminates the frustration of "telephone tag" and operates much faster than regular mail.
2. E-mail provides the ability to reach many different people quickly through broadcast messages using distribution lists. This not only saves enormous amounts of time in communicating with others far and near, it also ensures consistency of message and inclusion of appropriate parties in recurring correspondence.
   a. E-mail leaves a well-defined trail. It provides a clean record of who received what information. Messages are date and time stamped as they pass through various routers and servers to reach their intended and sometimes unintended destination(s). E-mail can be easily forwarded. It also carries the potential to reduce error by eliminating an interim messenger taking notes or verbally passing information.
3. E-mail facilitates the use of templates for quick distribution of patient information. The template may take the form of a list of educational Web sites or specific follow-up instructions for common patient scenarios.
4. Improvements over FAX include
   a. E-mail allows the receiver to read, print, or edit messages in electronic format.
   b. Automatic document distribution systems can forward clinical information not only to a fax server but also to an e-mail client to provide quick access to documents.

Potential Risks

Security of e-mail is difficult and potential pitfalls must be thought through. Until sure of the security of their e-mail system, health care providers should not put anything on e-mail that they would not want published to the world. Policy should clearly define who can and cannot participate on the e-mail system.

Risks of e-mail include the following:

1. Sometimes consultants and persons outside an organization are given access to and use of an internal e-mail system. This can be treacherous when global distribution lists are used to disseminate information. Information meant to stay within the organization can go to outsiders.
2. Use the Reply feature cautiously. Many experts recommend that its use be very limited because it poses risks to message control. Although the Reply feature offers a quick and easy way to respond without having to retype the address of the original sender, it also provides the original message. If the original message contained sensitive information, it would be unwise to proliferate the message in the e-mail system. As sender and receiver send messages back and forth, the string of message expands along with the exchange. Messages early in the string are carried along with new messages forwarded to new people or a distribution list of people. This can cause loss of control over the earlier messages as the discussion shifts and new persons are drawn into the reply string.
3. Selecting the wrong name will cause mail to be misdirected. E-mail addresses must be precise in spelling and punctuation. E-mail systems provide address books to facilitate addressing correspondence. Mail that is sent to an incorrect address or an address that is no longer in service is automatically bounced back to the sender as well as the mail administrator of the sender's service

provider. Messages are again proliferating in the system. Web TV is growing in popularity, and people can receive their messages via their television. If the sender has a shared e-mail account at home, this may allow access to family and/or friends.

4. Because companies have legal right of access to employee's incoming and outgoing e-mail, patients using an employer's e-mail system may therefore surrender privacy of any personal correspondence. Also, system administrators may get copies of bounced messages and backups hold old messages. Patients must be made aware of the potential privacy issues in corresponding by e-mail. Some organizations include a notice in each e-mail correspondence as an automatic message to remind patients of the critical issues in e-mail correspondence. For a sample of one such notice refer to the Kaiser Permanente procedures in this manual.
5. E-mail can be a major mode of entry for viruses into systems. With over 40,000 known viruses, it is imperative that anti-virus software be maintained to protect systems from invasion. In addition to software protection, policies and procedures should enforce good habits for keeping this problem to a minimum. Software is also available to screen incoming messages for objectionable material or from unauthorized sites.
6. E-mail can permit unauthorized access to employees who have left an organization. Good security practices require that access privileges to e-mail systems by individual employees be changed promptly when employees leave the system. E-mail systems must be backed up at regular and frequent intervals to restore data in times of system failures. Back-up files become a double-edged sword in that confidential e-mail is maintained in another file. Proper security procedures for storing and destruction of backup files must be implemented. Every point of e-mail proliferation must be identified and proper security procedures put in place to ensure adequate confidentiality of correspondence and destruction when retention requirements are met.

Policies and Procedures

It is imperative to have policies and procedures for e-mail usage in place. An excellent resource document is a White Paper published in the Journal of the American Medical Informatics Association by the AMIA Task Force on Guidelines for the Use of Clinic-Patient Electronic Mail (http://www.amia.org/pubs/pospaper/positio2.htm). This document discusses the use of e-mail and provides general guidelines for clinical communications as well as Medicolegal and Administrative Guidelines.

Policies and Procedures should address at a minimum:

- Verification requirements for sending and receiving addresses
- Procedures for handling misdirected mail (both sent and received)
- Patient education on good e-mail practices and limitations on security
- When e-mail is appropriate and when it is not (e.g., do not use for urgent matters)
- What types of information may be transmitted through e-mail, (e.g., appointment confirmation, yes; HIV test results, no)
- Procedures for security of multi-user accounts (Web TV, multiple household users).
- Documentation in medical record of e-mail correspondence
- Virus protection program with regular update of virus programs
- Proper retention and destruction procedures to ensure all vulnerable areas are covered

References

1. Annals of Internal Medicine, Electronic Patient-Physician Communication: Problems and Promise. 15 September 1998. 129:495-500. [www.acponline.org/journals/annals/15sep98/eleccomm.htm]
2. Journal of the American Medical Informatics Association, Kane B, and Sands, D; Guidelines for the Clinical Use of Electronic Mail with Patients. 1998;5:104-111.
3. The Internet for Nurses and Allied Health Professionals, Margaret Edwards, 1997, Springer, New York.
4. Computerizing Large Integrated Health Networks, Robert M. Kolodner, Editor, 1997, Springer-Verlag, New York.
5. Handbook of Medical Informatics, J.H. van Bemmel and M.A. Musen, Editors. 1997, Springer-Verlag.

Toolkit Section 4.9.2.3

HCFA and the Internet

On November 24, 1998, the Health Care Financing Administration (HCFA), published a new policy and guidelines "for the security and appropriate use of the Internet to transmit HCFA Privacy Act-protected and other sensitive HCFA information." Realizing that its longstanding policy was based on outdated technology and in conflict with new HIPAA legislation, HCFA reversed its position on the use of the Internet. The new policy applies to Medicare, Medicaid, and Federal Child Insurance programs. However, most experts agree that its scope will expand to include all patients with the new HIPAA security regulations. The policy is reprinted below and may also be obtained from the HCFA web site at http://www.hcfa.gov/security/isecplcy.htm HCFA's frequently asked questions on this topic may be found at http://www.hcfa.gov/security/fq011399.htm. Health care organizations should review the new requirements as part of maintaining their awareness of all the new changes in federal medical privacy legislation and regulation. The encryption requirement includes dial-up communications and will significantly affect organizations whose legacy systems do not support the encryption requirement. E-mail communications concerning protected patients (Medicare, Medicaid, and FCI) must only occur using secure e-mail protocols, such as S/MIME. According to HCFA, developing adequate data security is a cost of doing business. Discussions of software encryption and firewalls follow below to aid in interpreting the HCFA policy.

Background to HCFA Policy

SOFTWARE-BASED ENCRYPTION

The HCFA Internet Policy calls for minimum software standards. It requires a minimum Secure Sockets Layer level of Version 3.0. Standard commercial implementations of Public Key Infrastructure (PKI), or some variation thereof implemented in the SSL are acceptable.

Secure Sockets Layer (SSL) is an open architecture, nonproprietary, Internet security handshake protocol developed by Netscape. SSL provides data security and integrity through data encryption, server authentication, message integrity, and optional client authentication between a TCP/IP connection and an application protocol. It is application independent accommodating layering of HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), and Telnet protocols. Netscape has proposed SSL to the W3 Consortium working group on security for adoption as the security standard for web browsers and Internet servers.

Public Key Infrastructure (PKI) is being designed to solve the key management process problems that deal with creation, distribution, authentication and storage of keys . Through the use of PKI, health care information can be sent over networks including the Internet assuring its confidentiality (without concern that it has been disclosed), its integrity (data remained unchanged during transmission), its authentication (maintain confidence in the identity of the sender), and its nonrepudiation (the sender cannot dispute having sent the message).

Secure/ Multipurpose Internet Mail Extensions (S/MIME) is a protocol that adds digital signatures and encryption to Internet MIME messages, a standard format for extended Internet e-mail.

For a detailed discussion of SSL, PKI, S/MIME and encryption in general, contact the following Web sites:

Netscape: http://home.netscape.com

Go to http://home.netscape.com/products/security/ssl/index.html for a detailed discussion of SSL The Web site provides an indepth tutorial on how SSL works, frequently asked questions (FAQs), as well as download capability of the protocol.

RSA Data Security: http://www.rsa.com

RSA developed the public-key cryptosystem incorporated by Netscape into the SSL protocol. Up-to-date and authoritative, the RSA Web site is an excellent resource on cryptography. For the basics on SSL, go to: http://www.rsasecurity.com/standards/ssl/. It is time well spent to browse through their FAQ section

“Frequently Asked Questions About Today’s Cryptography” at: http://www.rsa.com/rsalabs/faq/. FAQ 5.1.2 “What is SSL” gives a clear and succinct description of the technology.

FIREWALLS

HCFA policy also calls for hardware to protect networks from unauthorized use and attack, including firewalls. According to the National Institute of Standards and Technology (NIST), "the purpose of a firewall system is to control access to or from a protected network (i.e., a site). It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated." Firewalls may consist of hardware or software, or a combination of the two. Firewalls may vary in the amount or level of penetration into a site they allow or disallow.

For a comprehensive discussion of firewalls, refer to the document "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls" found at the NIST Web site: http://csrc.ncsl.nist.gov/nistpubs/800-10/main.html. This is an excellent document on the Internet and Internet security. Discussion includes such topics as the firewall concept, why firewalls, issues and problems with firewalls, firewall components, firewall examples, firewall policy, procuring a firewall, administration issues with firewalls, and extensive references and other firewall sources. The document is a public document and can be downloaded from the NIST site.

The International Computer Security Association (ICSA) publishes a Firewall Buyer's Guide. The guide provides practical information on developing and purchasing a firewall. The guide is $49.95 plus $3.00 shipping and includes a print and CD version. To view and order the guide, go to http://www.icsa.net.

HCFA's New Policy on Internet Communications
Effective November 24, 1998

Internet Communications Security and Appropriate Use Policy and Guidelines for HCFA Privacy Act-protected and other Sensitive HCFA Information is a bulletin that formalizes the policy and guidelines for the security and appropriate use of the Internet to transmit HCFA Privacy Act-protected and other sensitive HCFA information. This bulletin is effective as of the date of issuance and remains in effect until superseded or canceled.

The Internet is the fastest growing telecommunications medium in our history. This growth and the easy access it affords have significantly enhanced the opportunity to use advanced information technology for both the public and private sectors. It provides unprecedented opportunities for interaction and data sharing among health care providers, HCFA contractors, HCFA components, State agencies acting as HCFA agents, Medicare and Medicaid beneficiaries, and researchers. However, the advantages provided by the Internet come with a significantly greater element of risk to the confidentiality and integrity of information. The very nature of the Internet communication mechanisms means that security risks cannot be totally eliminated. Up to now, because of these security risks and the need to research security requirements vis-a-vis the Internet, HCFA has prohibited the use of the Internet for the transmission of all HCFA Privacy Act-protected and other sensitive HCFA information by its components and Medicare/Medicaid partners, as well as other entities authorized to use this data.

The Privacy Act of 1974 mandates that federal information systems must protect the confidentiality of individually identifiable data. Section 5 U.S.C. 552a (e) (10) of the Act is very clear; federal systems must: "...establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." One of HCFA's primary responsibilities is to ensure the security of the Privacy Act-protected and other sensitive information it collects, produces, and disseminates in the course of conducting its operations. HCFA views this responsibility as a covenant with its beneficiaries, personnel, and health care providers. This responsibility is also assumed by HCFA's contractors, State agencies acting as HCFA agents, other government organizations, as well as any entity that has been authorized access to HCFA information resources as a party to a Data Release Agreement with HCFA.

However, HCFA is also aware that there is a growing demand for use of the Internet for inexpensive transmission of Privacy Act-protected and other sensitive information. HCFA has a responsibility to accommodate this desire as long as it can be assured that proper steps are being taken to maintain an acceptable level of security for the information involved.

This issuance is intended to establish the basic security requirements that must be addressed for use of the Internet to transmit HCFA Privacy Act-protected and/or other sensitive HCFA information.

The term "HCFA Privacy Act-protected Data and other sensitive HCFA information" is used throughout this document. This phrase refers to data which, if disclosed, could result in harm to the agency or individual persons. Examples include:

- All individually identifiable data held in systems of records. Also included are automated systems of records subject to the Privacy Act, which contain information that meets the qualifications for Exemption 6 of the Freedom of Information Act; i.e., for which unauthorized disclosure would constitute a "clearly unwarranted invasion of personal privacy" likely to lead to specific detrimental consequences for the individual in terms of financial, employment, medical, psychological, or social standing.
- Payment information that is used to authorize or make cash payments to individuals or organizations. These data are usually stored in production application files and systems, and include benefits information, such as that found at the Social Security Administration (SSA), and payroll information. Such information also includes databases that the user has the authority and capability to use and/or alter. These records must be adequately protected because modification of such records could cause improper payment.
- Proprietary information that has value in and of itself and which must be protected from unauthorized disclosure.

- Computerized correspondence and documents that are considered highly sensitive and/or critical to an organization and which must be protected from unauthorized alteration and/or premature disclosure.

Policy

This Guide establishes the fundamental rules and systems security requirements for the use of the Internet to transmit HCFA Privacy Act-protected and other sensitive HCFA information collected, maintained, and disseminated by HCFA, its contractors, and agents.

It is permissible to use the Internet for transmission of HCFA Privacy Act-protected and/or other sensitive HCFA information, as long as an acceptable method of encryption is utilized to provide for confidentiality and integrity of this data, and that authentication or identification procedures are employed to ensure that both the sender and recipient of the data are known to each other and are authorized to receive and decrypt such information. Detailed guidance is provided below.

Scope

This policy covers all systems or processes that use the Internet, or interface with the Internet, to transmit HCFA Privacy Act-protected and/or other sensitive HCFA information, including Virtual Private Network (VPN) and tunneling implementations over the Internet. Non-Internet Medicare/Medicaid data communications processes (e.g., use of private or value-added networks) are not changed or affected by the Internet Policy.

This policy covers Internet data transmission only. It does not cover local data-at-rest or local host or network protections. Sensitive data-at-rest must still be protected by all necessary measures, in conformity with the guidelines/rules that govern the entity's possession of the data. Entities must use due diligence in exercising this responsibility.

Local site networks must also be protected against attack and penetration from the Internet with the use of firewalls and other protections. Such protective measures are outside the scope of this document, but are essential to providing adequate local security for data and the local networks and ADP systems that support it.

Acceptable Methods

HCFA Privacy Act-protected and/or other sensitive HCFA information sent over the Internet must be accessed only by authorized parties. Technologies that allow users to prove they are who they say they are (authentication or identification) and the organized scrambling of data (encryption) to avoid inappropriate disclosure or modification must be used to insure that data travels safely over the Internet and is only disclosed to authorized parties. Encryption must be at a sufficient level of security to protect against the cipher being readily broken and the data compromised. The length of the key and the quality of the encryption framework and algorithm must be increased over time as new weaknesses are discovered and processing power increases.

User authentication or identification must be coupled with the encryption and data transmission processes to be certain that confidential data are delivered only to authorized parties. There are a number of effective means for authentication or identification that are sufficiently trustworthy to be used, including both in-band authentication and out-of-band identification methods. Passwords may be sent over the Internet only when encrypted.

We note that the Health Insurance Portability and Accountability Act of 1966 (HIPAA) calls for stringent security protection for electronic health information both while maintained and while in transmission. The proposed Security Standard called for by HIPAA was published in the Federal Register on August 12, 1998. The public had until October 13, 1998, to comment on the proposed regulation. Based on public comments, a final regulation is planned for late 1999. Policy guidance contained in this bulletin is consistent with the proposed HIPAA security requirements.

ENCRYPTION MODELS AND APPROACHES

Figure 1 depicts three generalized configurations of connectivity to the Internet. The generic model is not intended to be a literal mirror of the actual Internet interface configuration, but is intended to show that the encryption process takes place prior to information being presented to the Internet for transmission, and the decryption process after reception from the Internet. A large organization would be very likely to have the Internet Server/Gateway on their premises while a small organization would likely have only the Internet Client, e.g., a browser, on premises with the Internet Server at an Internet Service

Provider (ISP). The Small User and Large User examples offer a more detailed depiction of the functional relationships involved.

The Encryption/Decryption process depicted graphically represents a number of different approaches. This process could involve encryption of files prior to transmittal, or it could be implemented through hardware or software functionality. The diagram does not intend to dictate how the process is to be accomplished, only that it must take place prior to introduction to the Internet. The "Boundary" on the diagrams represents the point at which security control passes from the local user. It lies on the user side of the Internet Server and may be at a local site or at an Internet Service Provider depending upon the configuration.

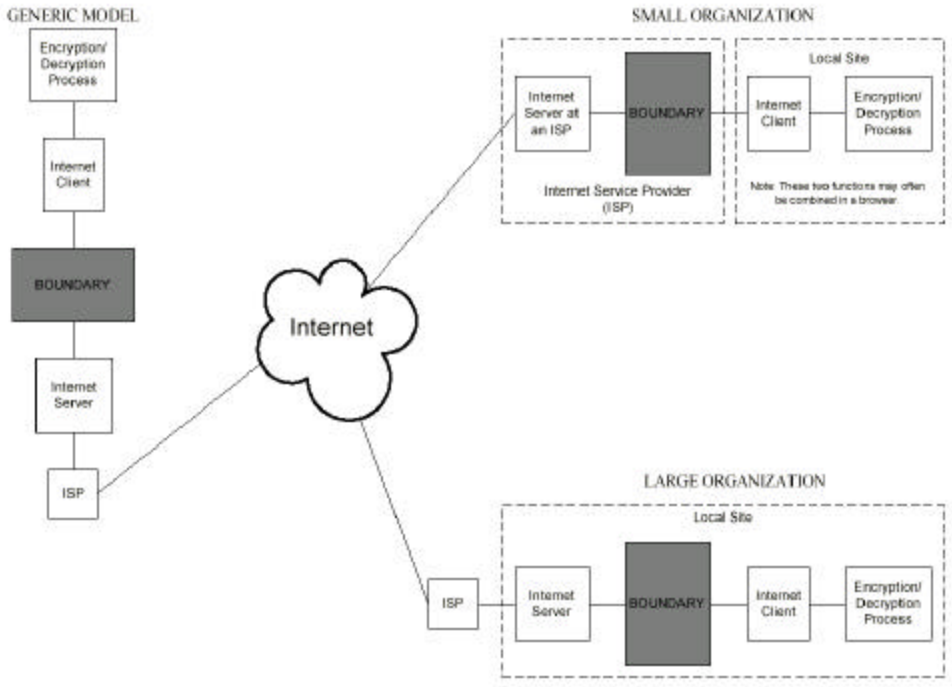


FIGURE 1:

The method(s) employed by all users of HCFA Privacy Act-protected and/or other sensitive HCFA information must come under one of the approaches to encryption and at least one of the authentication or identification approaches. The use of multiple authentication or identification approaches is also permissible. These approaches are as generic as possible and as open to specific implementations as possible, to provide maximum user flexibility within the allowable limits of security and manageability.

Note the distinction that is made between the processes of "authentication" and "identification". In this Internet Policy, the terms "authentication" and "identification" are used in the following manner. Authentication refers to generally automated and formalized methods of establishing the authorized nature of a communications partner over the Internet communications data channel itself, generally called an "in-band process." Identification refers to less formal methods of establishing the authorized nature of a communications partner, which are usually manual, involve human interaction, and do not use the Internet data channel itself, but another "out-of-band" path such as the telephone or U.S. mail. They should not be interpreted as terms of art from any other source.

The listed approaches provide encryption and authentication/identification techniques that are acceptable for use in safeguarding HCFA Privacy Act-protected and/or other sensitive HCFA information when it is transmitted over the Internet.

In summary, a complete Internet communications implementation must include adequate encryption, employment of authentication or identification of communications partners, and a management scheme to incorporate effective password/key management systems.

ACCEPTABLE ENCRYPTION APPROACHES

As of November 1998, a level of encryption protection equivalent to that provided by an algorithm such as Triple 56 bit DES (defined as 112 bit equivalent) for symmetric encryption, 1024 bit algorithms for asymmetric systems, and 160 bits for the emerging Elliptical Curve systems is recognized by HCFA as minimally acceptable. HCFA reserves the right to increase these minimum levels when deemed necessary by advances in techniques and capabilities associated with the processes used by attackers to break encryption (for example, a brute-force exhaustive search).

Hardware-based Encryption

Hardware encryptors, such symmetric password "private" key devices (such as link encryptors), while likely to be reserved for the largest traffic volumes to a very limited number of Internet sites, are acceptable.

Software-based Encryption

Secure Sockets Layer (SSL) (sometimes referred to as Transport Layer Security [TLS]) implementations - At a minimum SSL level of Version 3.0, standard commercial implementations of PKI, or some variation thereof, implemented in the Secure Sockets Layer are acceptable.

S-MIME - Standard commercial implementations of encryption in the e-mail layer are acceptable.

In-stream - Encryption implementations in the transport layer such as pre-agreed passwords, are acceptable.

Offline - Encryption/decryption of files at the user sites before entering the data communications process is acceptable. These encrypted files would then be attached to or enveloped (tunneled) within an unencrypted header and/or transmission.

ACCEPTABLE AUTHENTICATION APPROACHES

Authentication is accomplished over the Internet, and is referred to as an "in-band" process. Formal Certificate Authority-based use of digital certificates is acceptable. Locally managed digital certificates are acceptable, providing all parties to the communication are covered by the certificates. Self-authentication, as in internal control of symmetric "private" keys, is acceptable. Tokens or "smart cards" are acceptable for authentication. In-band tokens involve overall network control of the token database for all parties.

ACCEPTABLE IDENTIFICATION APPROACHES

Identification is the process of identification that takes place outside of the Internet connection and is referred to as an "out-of-band" process. Telephonic identification of users and/or password exchange is acceptable. Exchange of passwords and identities by U.S. Certified Mail is acceptable. Exchange of passwords and identities by bonded messenger is acceptable. Direct personal contact exchange of passwords and identities between users is acceptable. Tokens or "smart cards" are acceptable for identification. Out-of-band tokens involve local control of the token databases with the local authenticated server vouching for specific local users.

REQUIREMENTS AND AUDITS

Each organization that uses the Internet to transmit HCFA Privacy Act-protected and/or other sensitive HCFA information will be expected to meet the stated requirements set forth in this document.

All organizations subject to OMB Circular A-130 are required to have a Security Plan. All such organizations must modify their Security Plan to detail the methodologies and protective measures if they decide to use the Internet for transmittal of HCFA Privacy Act-protected and/or other sensitive HCFA information, and to adequately test implemented measures.

HCFA reserves the right to audit any organization's implementation of, and/or adherence to the requirements, as stated in this policy. This includes the right to require that any organization utilizing the Internet for transmission of HCFA Privacy Act-protected and/or other sensitive information submit documentation to demonstrate that they meet these requirements.

ACKNOWLEDGMENT OF INTENT

Organizations desiring to use the Internet for transmittal of HCFA Privacy Act-protected and/or other sensitive HCFA information must notify HCFA of this intent. An e-mail addre**s** is provided below to be used for this acknowledgment. An acknowledgment must include the following information:
Name of Organization
Address of Organization
Type/Nature of Information being transmitted
Name of Contact (e.g., CIO or accountable official)
Contact's telephone number and e-mail address

For submission of acknowledgment of intent, send e-mail to: internetsecurity@hcfa.gov. Internal HCFA elements must proceed through the usual HCFA system and project development process.

For questions or comments, write to:

Office of Information Services, HCFA
Security and Standards Group
Division of HCFA Enterprise Standards -Internet
7500 Security Boulevard
Baltimore, MD 21244

Toolkit Section 4.9.3

Case Study: PCASSO (Patient Centered Access to Secure Systems Online)

By Dixie B. Baker, Ph.D.
Principal Investigator

PCASSO (Patient Centered Access to Secure Systems Online) is a research project funded by the National Library of Medicine (NLM) of the National Institutes of Health (NIH) through its Health Applications for the National Information Infrastructure (NII) initiative. In short, PCASSO's primary purpose is to enable consumers to securely access their health information – including sensitive clinical data – over the Internet.

Science Applications International Corporation (SAIC) has partnered with the University of California, San Diego (UCSD) School of Medicine and Healthcare Network, on this research, development, deployment and evaluation project designed to enable not just health care providers and medical researchers, but also patients, to safely and securely access patient health information over the Internet. The PCASSO model system uses familiar World Wide Web technologies (e.g., Web browser, Secure Sockets Layer protocol, Java Applet) to support the search and retrieval of information, including patient demographics, medications, laboratory tests, and transcription reports. State-of-the-art security technologies are used to protect the confidentiality and integrity of patient information.

Phase I of the project (1996 through 1997) had three objectives: (1) to develop a model, architecture and functional prototype that supported the goal of shared access by providers and patients via the Internet; (2) rigorously to evaluate the security characteristics of the PCASSO model in a laboratory simulation environment, and; (3) to Develop a detailed deployment plan for rolling out PCASSO and for evaluating its safety and efficacy in a real-world regional health care setting.

Phase II (1998 through 1999) includes the integration and evaluation of the PCASSO model with the clinical information systems of the UCSD Medical Centers and Healthcare Network. This countywide system of five hospitals and 45 affiliated community sites includes over 250 primary care providers and over 1300 specialists. UCSD has over 19,000 annual in-patient admissions and over 590,000 outpatient visits. As with most integrated health care systems, the computing environment includes multiple legacy systems connectable via a CAI interface engine. The Phase II roll-out involves the UCSD Biomedical Library in a manner that establishes an important new role for medical librarians in the emerging NII, assisting patients and providers to use state-of-the-art information technology.

PCASSO Architecture

The PCASSO architecture is depicted in Figure 1. PCASSO consists of secure web services, trusted application surrogate services, and secure administration services.

Secure Web Services
The secure web services include:

- The *Public Key infrastructure* (PKI) that generates, certifies and manages public encryption keys and key certificates;
- The *PCASSO Server* that authenticates users, initiates a user process, and serves as the intermediary between that process and the client;
- The *Secure Operating System*, which in PCASSO model is Data General B2 DG/UX;
- The *Client Intrusion Detector*, "SpiCE

Trusted Application Surrogate Services
The trusted application surrogate services include:

- The *Data Importer and Loader* that receives HL7 messages from the UCSD interface engine, parses them, attaches sensitivity labels to them, and loads data into the PCASSO Clinical Data Repository (CDR).
- The *Clinical Data Repository (CDR)*, a Trusted Oracle 7 database that stores the labeled clinical information, as well as operational information used by the PCASSO server, and;
- The *Browser Client with Application Rules*, a Java applet that is downloaded from the server and through which the user interacts with the PCASSO server. The client is the interface through which the user logs in, selects a role, downloads data and logs off.

Secure Administration Services
The secure administration services include:

- *Role-based Account Management*, which enables the PCASSO Administrator to manage user accounts, including assigning user roles to individual users;
- *Audit Services*, which enables the PCASSO Administrator to set audit parameters and to review audit logs, and;
- *Notification Services*, which sends e-mail to patients when a change in their record is detected.

Papers providing details regarding the PCASSO architecture can be found at the project web site: **http://medicine.ucsd.edu/pcasso**

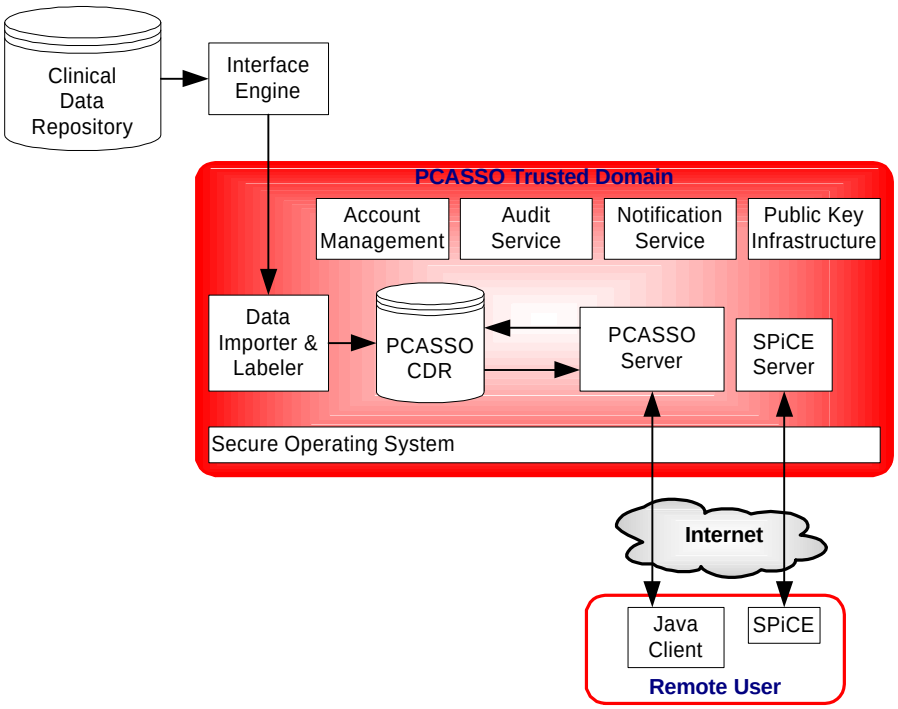


Figure 1. PCASSO Architecture

Project Status

The PCASSO Project is now in the final year of Phase II. The model system has been developed (per the architecture described above) and has just been installed at UCSD. The PCASSO server sits on the Internet and is accessible through any Internet Service provider (ISP). About a dozen providers have PCASSO accounts and are actively using and evaluating the system for safety and usability. Additional providers are being added daily. Current plans include making the system available to patients in the coming months.

The CHIME-Trust Healthcare Public Key Infrastructure and Trusted Third Party Services A Case-Study

Toolkit Section 4.9.4

Lori Reed-Fourquet, MS, John T. Lynch, MPH, Michael K. Martin, DVM, MPH , Michael Cascio, Wing-Yan Leung, MS, Philip P. Ruenhorst MHA

CHIME Inc.
Wallingford Connecticut

INTRODUCTION

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the 1998 Internet policy of the Healthcare Finance Administration (HCFA) emphasize the importance of protecting electronic health information during acquisition, transmission, use and storage and focus special attention on systems for encryption, authentication, digital signature, and access control. Proposed HIPAA data security rules require such technology when deploying electronic signatures even though use of electronic signatures remains optional. HCFA's Internet Policy mandates strong-grade encryption, the use of authentication or identification of communication partners, and a management scheme to incorporate effective password and key management systems. Trusted Third Party Services such as the CHIME-Trust system help satisfy regulatory requirements as well as enable secure, confidential communication over untrusted lines among unaffiliated enterprises. CHIME-Trust also demonstrates adaptations of public key and directory technology necessary to accommodate the range of professional certifications and related access privileges characteristic of healthcare. Such a common infrastructure specific to the needs of the healthcare domain has been recommended by the efforts of G7/Enable[i], and has been successfully tested through the efforts of the EuroMed and other European projects[ii].

In Connecticut, as throughout most of this country patient care, frequently occurs across several unaffiliated enterprises. As a healthcare service organization, CHIME has established CHIME-Trust, a trusted third party service based on Public-Private Key technology (PKI) and Lightweight Directory Application Protocol (LDAP) services. Providing a common root for LDAP and Certification services within a healthcare domain secures communication chain-of-trust and identity searches, thereby establishing a cost-effective infrastructure for inter-institution communication of confidential patient information. CHIME-Trust creates a common root among participants thus enabling HIPAA compliant communications of patient care data over health information networks and over the Internet. CHIME-Trust also functions as a foundation for interoperability of security services among unaffiliated healthcare providers, between providers and payers, and potentially between providers and patients.

Although several commercial entities provide Certificate Authority Services, they often do not meet the needs of healthcare they do not certify an individual's professional

credentials. Healthcare applications must be able to ascertain an individual's role, specialty, and the status of professional credentials as well as their identity. Furthermore, the certificate policies of the Healthcare Domain Certificate Authorities must be consistent with the extensive validation processes that are currently conducted to establish trust and permissions allowing clinicians to practice medicine. Such policies must be consistent throughout the chain-of-trust relationships. In establishing a Trusted Third Party service for the Healthcare domain, CHIME provides the means to establish this level of assurance. Furthermore, CHIME will continue to negotiate extended chain-of-trust relationships consistent with this policy such that interoperability and consistency may be achieved.

Many healthcare facilities consider operating their own Certificate Authority. While this option is sufficient for a self-contained operation, it is not scaleable for the level of interoperability required by healthcare. Healthcare transactions regularly involve unaffiliated entities. Under such a scenario, each organization must negotiate trust for the unaffiliated certificates. This negotiated trust must then be configured into each software product relying upon the certificates along with the appropriate access control. Most Certificate and Directory aware software does not currently support multiple 'certificate mapping' and therefore require complex integration efforts for each Certificate Authority/Directory recognized. Establishing the same level of trust for diverse attestation processes dilutes the trust model. Without a common Certificate Authority, such an effort would be both unmanageable and unreliable. Participating in a common Certificate Authority Model simplifies these relationships and configuration efforts.

Consider, for example, a prescription that is written by a physician certified through an Institutional Certificate Authority. Should this prescription need to be filled in another state, particularly if it is through a pharmacy with which the Institutional Certificate Authority has had no previous relationship, there is no inherent mechanism for the pharmacy to check the validity and reliability of the signature. In the absence of predefined trust configuration, this transaction would require a manual intervention. On the other hand, if the prescription were signed through a well defined chain-of-trust, such validity and reliability would be inherent within the configuration, and no manual intervention would be required. This applies to any electronic transaction conducted between healthcare entities that have not pre-established relationships and trust.

CHIME-Trust: A Trusted Third Party Network for Healthcare

CHIME-Trust is a Public Key Infrastructure for the Healthcare Domain. It is specifically designed to protect confidential health information throughout the life cycle of patient care and the healthcare system. We opened participation in the project to all healthcare providers, provider institutions, their trading partners, and their customers. In order to understand CHIME-Trust, it is best to describe first the background of CHIME-Net. In 1993, multiple efforts existed within the state of Connecticut to establish connectivity for isolated communications among providers, and between providers and payers. Specifically, this connectivity was intended to enable applications such as EDI for the eligibility and claims management process. Other applications included electronic mail and on-line access to a shared database of patient discharges. With this as a basis, we examined the potential benefits of establishing a health information network for the

provider and payer community. A number of potential benefits to provider connectivity were identified including the ability to:

- Share Clinical Information
- Transfer Patient Records
- Obtain Historical Patient Records
- Reduce High Volume Paper Correspondence
- Provide a Central Data Repository for Research
- Transfer Lab Test and Image Data
- Enable an Emergency Response System
- Electronically Transfer Files
- Exchange Electronic Mail
- Provide an Infrastructure for multimedia data transmission for Patient Care/Consultation

Based upon this benefits analysis, the providers began a statewide health information network in 1994, funded, in part, by the National Library of Medicine Information Systems Grant (1 G08 LM06347-01). This network was designed to connect each provider to a central router at CHIME, and to connect CHIME to the Internet. This network now includes 51 institutional connections including acute care hospitals, rehabilitation facilities, home healthcare providers, and long-term care facilities. The network is further extended through community-based connectivity efforts to include physicians, pharmacies and clinics. Trading partners have also joined the network providing for a communication foundation between providers and payers. Given that much of the benefit to this connectivity was to be attained by sharing and communicating confidential health information, it was important to complement the network infrastructure with a security infrastructure.

In effort to attain this goal, a sister affiliate, CHREF, engaged in a 3-year joint venture funded by NIST-ATP 70NANB5H1195, to assess alternatives for Community Security Information Sharing. Through research into industry goals and security technologies we identified and tested Trusted Third Party services, including Certificate Authorities, Registration Authorities, and Healthcare Community Directories as a robust infrastructure that would allow for large-scale deployment of secure health information services. Throughout this project, we similarly evaluated numerous biometric and token-based architectures for user authentication. Among these, we found that smart cards were the most viable solution for user authentication based upon the reliability of the technology and user acceptance. We do, however, expect this approach to be enhanced through the use of biometrics as the biometric technology matures.

Project Goals

HIPAA poses a fundamental requirement for accountability and logging of information at the individual user level. This poses major challenges because healthcare providers are mobile, typically affiliated with multiple institutions and operate in time-critical environments. Without an extendible infrastructure, the care provider could be faced with numerous identities, accounts, and technologies across multiple environments, a complexity that potentially reduces efficient access. A security infrastructure, therefore, should enable a user to deploy a single professional certificate across all healthcare applications, institutions, and across multiple security technologies. For example, an authorized user should be able to use the same certificate to access patient care systems

and the Virtual Private Network of another provider institution. This digital identity should function within the provider systems and communicate billing information with trading partners. These goals have spurred several integration and interoperability activities such as working with vendors of security technologies to assure the healthcare professional identity stored on a smart card may be used with electronic mail, Virtual Private Network technologies, extranet technologies, EDI tools, digital signature tools and Web-based systems. Efforts also aim to assure interoperability with multiple payers, transcription and coding services, trading partners and other certificate authorities.

CHIME-Trust has faced several challenges. Although standards exist for using smart card-based certificates and key stores, many of the security technologies have not yet implemented this interface. However, the mobile nature of the healthcare provider and extreme sensitivity of the data dictate a level of strong authentication achieved through the use of token-based technologies. Other certificate-based technologies have used custom certificate extensions as required components for the security services. Because such custom extension requirements are not widely published, accommodating them poses complications to the certificate authority in managing certificate policy and configuring certificate authority software. Certificate authorities and certificate authority software typically utilize directory services for storage and retrieval of certificate-based information. However, the community healthcare directory must be populated with more comprehensive information and attributes that are more volatile than the certificate would warrant. The directory must also be structured so as to allow for proper management, reliability of service, and access control. Unfortunately, some certificate authority software places configuration restrictions upon the directory architecture which are, at times, in conflict with the requirements of the healthcare directory infrastructure.

In addition to these complexities, interoperability of multiple certificate authorities pose additional challenges. Trust in the infrastructure depends on knowledge that the CA takes appropriate measures to bind an individual's healthcare credentials to the individual's identity. This is encompassed within the certificate policy. If a given infrastructure employs multiple approaches or policies, it lessens trust. It is therefore important to adopt the same, or at least comparable validation criteria as a healthcare information security standard. While these efforts are in progress, they do not yet exist, resulting in the propagation of numerous, difficult to reconcile practices. Moreover, no tools exist to map or cross-certification equivalent or recognized policies. Implementing such trust at the application-level constitutes another alternative for interoperability across multiple certificate authorities and directories. Although many tools use certificates and directories for authentication and access control, these tools have not been designed to recognize either multiple certificates or certificate authorities in a single directory, or multiple directories and certificate authorities. Most vendors are willing to accept such input into their development cycles, but the timetables for new software features are prohibitive.

Project Architecture

In 1999, CHIME designed a scaleable security infrastructure through the establishment of a Healthcare Public Key Infrastructure. This is a Trusted Third Party Service that incorporates a distributed registration process with a robust, distributed healthcare directory including enrollment of users into standards-based roles. This infrastructure enables encryption, digital signature, non-repudiation, identification,

authentication, and role-based access control. Because the infrastructure is specifically intended to service inter-institutional secure communications, it is necessarily standards-based and operates in a multi-vendor environment. We have tested the interoperability of this solution against multiple security products and across multiple trading partners. The architecture of the statewide Healthcare Domain Trusted Third Party includes three primary components. These include The Certificate Authority (CA), the Registration Authority (RA), and the LDAP Directory server. All three of these components are extendible.

Within the state of Connecticut, CHIME serves as the root CA for the healthcare providers and institutions within the state. This model supports the possibility that a larger community network may wish to maintain its own subordinate CA that would be implemented as a branch of the tree. CHIME issues certificates to both healthcare professionals and organizations. This supports the requirement that health information systems must be able to identify access to patient records by individual. It also supports the requirement that information may be sent to an organization for processing by one of many possible providers. Multiple certificate assurance levels are defined based upon the level of protection supported by the recipient. The highest level of certificate is intended to have a level of certainty sufficient to practice medicine. The lower level certificates will serve to authenticate users to less sensitive health applications and to exchange communications, but may not be used for the delivery of medical orders. Certificates for signing and for authentication may be issued directly through CHIME or through one of the subordinates within the hierarchy. The Trusted Third Party architecture described also allows for this statewide CA to become a direct subordinate to a higher authority. This may be a national entity or other such entity that would obviate the need for a higher level root.

In order to assure the credentials of the providers, RAs will be set up both at CHIME and at major healthcare centers and organizations. The RAs will be closely linked with the Human Resources area of member hospital and healthcare organizations. Within most hospitals, these processes are distributed between the human resource area for permanent staff and medical staffing offices for independent practitioners. Several processes already exist to insure licensing credentials for all practitioners in the organization, including validation of current licensing status with state and federal licensing boards. The RAs will exploit this process thereby insuring that proper controls and checks exist while minimizing the impact and cost to security implementation.

The healthcare domain also requires the ability to support entity certificates. This requires validation with the State Department of Health and with Drug Control to insure that the organization is licensed for the appropriate category of medical practice, not only validation against business incorporation records. It is also important to verify that the organization is in good standing with the General Services Administration and the Office of the Inspector General.

Another important component of the Trusted Third Party infrastructure is the LDAP directory server. Certificates are associated with users registered in the directory. Users are also assigned to roles as defined through ASTM security standards. The directory configuration allows users to hold multiple roles at one or many institutions as typically occurs in healthcare. Integration of the Certificate Authority with the LDAP Directory Server supports the type of Enrollment and Registration infrastructure that will

be required by a CHIN to appropriately identify users and assign privileges within the system. These two components serve as a foundation for the registration of user roles as a foundation for the Role-Based Access Control model. The CA, the RA, and the LDAP directory constitute Trusted Third Party services as a key infrastructure to support secure HIN applications and services. Because the LDAP is a strongly emerging standard, the user registry may be distributed and replicated among the member locations, as LDAP becomes more prevalent. We designed the directory architecture to accommodate this anticipated growth.

Trusted Third Party Services

CHIME provides a number of services as a Trusted Third Party. Many of these are core Certificate Authority services. These services include management of Certificate Revocation Lists, Certificate Distribution, Certificate Revocation, and time stamping. Some of these processes will be unique to the healthcare professional certification environment and as such will be services not typically offered through standard Certification Authorities. These services include a Credential Verification Process, Certificate Authority Policy Definition, Identification and Authentication, Directory Services, and Role management services. Other services offered through this program are intended to assist the Trusted Third Party member community in implementation and integration of the Trusted Third Party infrastructure. These services include Education, Integration, and Representation on standards development committees and Negotiation for chain-of-trust partnerships. A formal certification process intended to validate professional credentials will map such credentials to directory attribute structures and roles based upon ASTM E31.20 Healthcare Information Security Standards. A Hierarchy of Chain-of-trust and LDAP architecture will be utilized to allow for such processes and services to be distributed to those participants interested in servicing their own community. In addition to providing each site with detailed documentation, central services have been implemented to assist the technical personnel at participating sites in deploying any relevant hardware or software.

Enrollment with the Trusted Third Party Services entails several steps. The user first contacts a certified registrar in order to initiate the credential verification process. This would typically take place as an integral part of the staffing process. This registrar examines the identification and credential documentation of the user, insures directory registration of the user, and attests to the relative attribute and credential information. The user's public and private key is then generated, and the registrar issues the certificate request to the CA. The Certificate Authority then issues the appropriate certificate to the user to be distributed on smart card by the Registrar, synchronizing the public key information with the user's directory entry.

Revocation would normally be initiated through the RA that originated the certificate. However, because the healthcare domain certificate is bound to professional credentials, the certificate revocation or suspension may be initiated through licensing organizations such as Drug Control or the Department of Health. The CA insures appropriate communications along with revocation when initiated through a party other than the originating RA.

Protection Scheme

This architecture can be used directly for S/MIME capable electronic mail packages and LDAP/Certificate aware access control interfaces. These products may be configured to use the LDAP directory service to look up the Public Key for healthcare professionals. These certificates may also be utilized for the protection of Web-based applications through the use of ticketing agents, and natively through some web services. These products use the Public Key Infrastructure of the Trusted Third Party to obtain authentication certificates and to determine user roles through LDAP services. The Web services can then be appropriately configured to allow or disallow access based upon role-based access control. Strong authentication may be enforced based upon certificate level.

Organizing CHIME-Trust

Management

CHIME, an affiliate of the Connecticut Hospital Association, manages CHIME-Trust. Organizations may choose among several options for participation that allow for multiple levels of autonomy. Small organizations and individual providers may choose to enroll through the central Registration Authority (RA) or through one of the distributed RAs. Small facilities and organizations may choose to participate as a 'light-weight' RA. This model allows for the user registration process to be conducted at the local registration site, but the actual certificate issuance is handled through a fully functional RA. The 'Full' RA holds a contract either directly with the CA, or with a coordinating RA. The 'Full' RA handles the enrollment/revocation process, handling both the directory management for the local users, and the certificate issuance, including smart card production. The architecture also allows for a coordinating RA. This RA serves as a regional leader, and manages the contractual relationships and certification process for local registration authorities within its region. The architecture similarly allows for a Subordinate CA. Although costs and potential integration issues typically preclude this option, the architecture accommodates organizations committed to operating a certificate authority for the healthcare domain. The last type of participation is as a relying party. The relying party may establish trust in the infrastructure without necessarily subscribing to certification services. This concept is applicable to trading partners that may wish to honor the Healthcare PKI infrastructure for enabling secure access and communications with necessary individuals or systems. Any of the above participation types may utilize directory replication to insure redundancy and broad communications information for the directory community. All participation is based upon contractual relationships with the possible exception of the relying party. This latter relationship may exist with or without a contractual relationship at the discretion of the relying party.

Funding

CHIME-Trust has a number of funding sources. Early Research for CHIME-Trust was funded through a NIST-ATP sponsored Joint Venture (70NANB5H1195), through which supporting technologies were assessed, integrated and tested. Components related to electronic commerce for Pharmacy applications has been supported through a NIST ATP sponsored Joint Venture (70NANB7H3035). Assistance for implementation and deployment activities has been requested from and granted by the National Library of Medicine (1G08LM06897-01). Ongoing operational costs are secured through fees per identity and for Directory replication.

Routine Operational Issues

We addressed several, important organizational issues in the process of configuring the CHIME-Trust Infrastructure. While Certificate Authority products are becoming widely available, the software alone does not provide sufficient assurance that all processes have been appropriately conducted prior to issuance. Inappropriate management of the Certificate Authority can compromise the integrity of the infrastructure. In order to secure the Certificate Authority, we implemented significant physical safeguards in collaboration with building management personnel. Similarly, we made changes in our personnel practices to accommodate management of the Certificate Authority. For example, the practices of separation of duties and employing multiple roles to execute certain sensitive functions have imposed levels of training, background checking, and key/password/code protection not typically found in healthcare. These changes involved education, process management, policy definition, and capital expenditure. Legal council was involved for changes to personnel policies for CHIME-Trust staff as well as for contract development.

Local registration authorities raise additional organizational issues. Although we tried to minimize burdens on provider-based local registration authorities, instituting the certification process requires changing promotion and exit processes. The certification process is intended to mimic the rigorous credential validation process required of healthcare providers for practicing at healthcare institutions. Healthcare users, however, include both medical staff (licensed healthcare practitioners) and non-licensed employees. Two different areas within the institution typically handle these functions. Instituting a registration authority in this environment entails either adding new job responsibilities to existing jobs, or implementing new job functions. The registrar is responsible for managing changes to certificate and directory status for job changes that may result in role changes, and for revocation, as appropriate, for employees that leave the organization. This involves personnel documentation and communications that may not be part of the existing process.

Registering users poses important operational challenges. This process must be rigorous in order properly to attest to the identity and credentials of the individual being registered and must include face-to-face verification. We initially established only one registration authority to give us the opportunity to refine our policies and procedures before decentralizing the process. We had to address certain technical limitations of our supporting products by adapting our business process. For example, we found that the Directory entry must be made prior to certificate issuance while paying particular attention to the accuracy of the fields used to map the certificate to the directory. Distribution of the Registration Authorities will similarly require some restructuring of job function and responsibilities at the Local Registration Authority sites. We found that allowing registrants to schedule on-site registration particularly helped successful deployment of the technology.

Educating potential users at all levels has greatly helped successful deployment of CHIME-Trust. We conduct educational programs for executives, technical personnel, and decision-makers, regularly inform them of pending changes and recruit representatives for advisory groups. The Health Services Librarians developed 'Train-the-trainers' program and end-user training programs.

Obstacles

A number of operational challenges exist. Because this technology is relatively young, few vendors incorporate it into products for the healthcare market. When coupled with the other requirements of HIPAA, significant operational re-engineering will be required. We are working with the healthcare providers to identify and assess opportunities for shared solutions and to provide assistance in change management.

Lessons Learned

Implementing CHIME-Trust has required paying special attention to change management among all participants in the chain-of trust, not only in the organization providing the service. Changes must occur in operations, personnel management, physical security, and technology. Successfully establishing an infrastructure that crosses the boundaries of multiple enterprises depends on use of standards and open systems, including participation in the development of these standards when necessary. Because maximizing the interoperability of the PKI requires a critical mass of participants, any organization interested in providing such a service should sponsor broad community-based events to minimize the learning curve.

Bibliography

[PKI] Public Key Infrastructure Study, Final Report, National Institute of Standards and Technology, Gaithersburg, MD, April 1994

Freir A, Karlton P, Kocher P. "The SSL Protocol Ver 3.0". Netscape Communications Corporation at http://home.netscape.com/eng/ssl3

CCITT Blue Book, Recommendation X.509 and ISO 9594-8. "Information Processing Systems – Open Systems Interconnection – The Directory Authentication Framework, CCITT, Geneva, March 1988.

Reed-Fourquet LL., *et.al.* 194. "A Frame-Relay Approach for a State-Wide Health Information Network." Proceedings, Eighteenth Annual Symposium on Computer Applications in Medical Care 416-420.

Reed-Fourquet LL., *et.al.* 1995. "CHIME-Net, The Connecticut Health Information Network: A Pilot Study." Proceedings, Nineteenth Annual Symposium on Computer Applications in Medical Care .

1999 Annual Book of ASTM Standards, Healthcare Informatics; Computerized Systems and Material Information. 1998 Volume 14.01.

G7/Enable Sub-Project 5 Final Report: http://www. ehto.be/sp5/finrep/index.html

Katsikas SK, Spinellis DD, Iliadis J, Blobel B. "Using Trusted Third Parties for Secure Telemedical Applications Over the WWW: The EUROMED-ETS Approach."1998. International Journal of Medical Informatics 49(1998).

Lynch JT, Reed-Fourquet L, Martin MK, Leung WY, Ruenhorst PA, "A Healthcare Public Key Infrastructure, The Connecticut Experience." HIMSS 2000.

Reed-Fourquet. "Secure Sharing of Patient Information over the CHIME-Net Statewide Health Information Network." Toward an Electronic Patient Record '97. Presentation

G7/Enable Sub-Project 5 Final Report: http://www. ehto.be/sp5/finrep/index.html

Reed-Fourquet *et.al* 1999."Enabling Secure Information Sharing for Inter-Enterprise Patient Care" Toward an Electronic Patient Record '99.

INFOSEC/THIS Project, *Requirements on Electronic Signature Services*, Ver. 2.0, Spri, Sweden, December 1995.

INFOSEC/THIS Project, *Trusted Third Party Services*, Ver. 2.0, Spri, Sweden, December 1995.

Healthcare Telematics/ TrustHealth Project, *Functional Specification of TTP Services*, Spri, Sweden, August 1996.

INFOSEC/HEALTHSIGN Project, Requirements, benefit and validation analysis for an ES/TTP Pilot in Healthcare, HSC, United Kingdom, April 1994.

Polemi D, "Review of Existing Results of TTPs for Health Care Systems," EUROMED-ETS, Deliverable 1, INFOSEC Project 20820, CEC, DGXIII B-6, March 1997.

Polemi D, "TTPs in EUROMED: The Proposed Solution," EUROMED-ETS, Deliverable 2, INFOSEC Project 20820, CEC, DGXIII B-6, February 1998.

Polemi D, "Pilot and Validation of Security Measures in Euromed," EUROMED-ETS, Deliverable 3, INFOSEC Project 20820, CEC, DGXIII B-6, September 1997.

Polemi D, "Trusted Third Party Services for Health Care In Europe," EUROMED-ETS, Deliverable 4, INFOSEC Project 20820, CEC, DGXIII B-6, February 1998.

---

[i] G7/Enable Sub-Project 5 Final Report: http://www. ehto.be/sp5/finrep/index.html

[ii] The European community has done extensive research in the area of health information security. Many of these efforts involve the concept of trusted third party systems. These efforts involve both conceptual models and prototype systems and infrastructures similar to those described in this document. This research and development was first published in 1994 (Trusted Health Information Systems THIS) as a 3-year study for healthcare information security requirements. This was followed by an architectural study completed in 1998 (TrustHealth I), that identified supporting services that would be required for the implementation of Trusted Third Parties in Healthcare. This effort continues in a current effort that will include some demonstration projects (TrustHealth II).

Business Continuity Planning and Disaster Recovery Planning
Toolkit Section

The proposed rules for data security and electronic signature, published by the Department of Health and Human Services call for a contingency plan in the section on administrative procedures to guard data integrity, confidentiality, and availability.

The requirement states: "We would require a contingency plan to be in effect for responding to system emergencies. The organization would be required to perform periodic backups of data, have available critical facilities for continuing operations in the event of an emergency, and have disaster recovery procedures in place. To satisfy the requirement, the plan would include the following:

- ?? Applications and data criticality analysis**,**
- ?? A data backup plan,
- ?? A disaster recovery plan,
- ?? An emergency mode operation plan, and
- ?? Testing and revision procedures."

Several web sites offer information on business continuity and disaster recovery planning. The Disaster Recovery Institute International was founded in 1988 to provide a base of common knowledge in contingency planning that serves as the industry's best practices standard "The Professional Practices for Business Continuity Planners".
It covers:

1. Project Initiation and Management
2. Risk Evaluation and Control
3. Business Impact Analysis
4. Developing Business Continuity Strategies
5. Emergency Response and Operations
6. Developing and Implementing Business Continuity Plans
7. Awareness and Training Programs
8. Maintaining and Exercising Business Continuity Plans
9. Public Relations and Crisis Coordination
10. Coordination with Public Authorities

It is available as at http://www.dr.org. DRII also administers the industry's only global certification program for qualified business continuity/disaster recovery planners and provides training courses.

Other web sites with useful information include:
The Disaster Recovery Journal (http://www.drj.com)
The Contingency Planning & Management Magazine
(http://www.contingencyplanning.com).

Toolkit Section 5.0

Chapter Five

ENHANCING PATIENT UNDERSTANDING

Toolkit Section 5.1

Introduction

As the DHHS recommendations on confidentiality make clear, health care providers face new obligations in informing patients about how they manage health information. The DHHS recommendations signal some broad social changes, however, whose significance transcends the narrow legal and regulatory context of their development. Reforms in health care finance (specifically the emergence of managed care) are refocusing some aspects of health care from the doctor-patient relationship to the organization-patient relationship, thus making health care organizations accountable to patients in new ways. In addition to being accountable for health care processes and outcomes, organizations are becoming accountable to patients for their business practices, particularly for what they do with information about their individual cases. These changes as well as DHHS proposals will increasingly require health care organizations to obtain new types of consent, provide access to information historically reserved for institutional use only, educate patients about their business practices, and extend new services to their patients using electronic media. Model examples for how some health care organizations are trying to meet these new obligations follow.

Toolkit Section 5.2

Complying with Consent, Inspection, and Disclosure Requirements

The American Health Information and Management Association (AHIMA) offers guidelines and sample documents for managing consent, inspection and disclosure of patient medical records in "Release and Disclosure: Guidelines Regarding Maintenance and Disclosure of Health Information." It includes discussion of important questions about disclosing patient records including General Principles, Classification of Information (Non-confidential, Confidential definitions), Authority to Grant Authorization, Minimum Requirements for Acceptable Authorization, Revocation of Authorization, Requirements for Disclosure to Specific Individuals/Entities, and Methods of Disclosure. It also addresses special situations (AIDS, Adoption, Alcohol/Drug Abuse, Photography) and Redisclosure of Health Information.

AHIMA guidelines for authorizing patient inspection and emendation of their records are summarized below:

- Most states allow a patient, or the patient's legal representative, to examine and obtain copies of the patient's hospitals records, although some states grant patients the right to review their hospital records only after discharge. Less clear are the rights of access to health records maintained by physicians and other individual health care providers.

- After the patient's discharge, health information may be disclosed to the patient or the patient's legal representative upon written request and presentation of proper identification. In the case of behavioral health records, the patient's physician should be contracted prior to disclosure.

- If the patient or the patient's legal representative requests access to health information, the recommended procedure is as follows:

    1. The request should be documented in writing.
    2. The request should be discussed with the patient's attending physician who should be encouraged to review the record with the patient or the patient's legal representative.
    3. A physician who believes that disclosure of information would be harmful to the patient's physical or mental well being should document this opinion in the record, and the information should not be disclosed.
    4. If the physician does not wish to meet with the patient and/or the patient's legal representative and does not believe disclosure would be harmful to the patient, the information should be disclosed, unless otherwise prohibited by state law.
    5. Patients should be permitted to review their records without charge.
    6. To ensure the integrity of the record, the provider's health information management professional or designee should directly supervise such a review.
    7. Questions regarding treatment, prognosis, or other clinical matters should be referred to the attending physician.
    8. Patients who request copies may be charged a reasonable fee to cover the cost of accessing and copying the record.

- If information in the record is disputed, the following procedure should be followed:

    1. The patient or the patient's legal representative should discuss the issue with the health care practitioner who made the entry in question. If the health care practitioner agrees the entry contains an error, he or she should make the correcting entry in the patient's record.

2. When correcting paper records, a single line should be drawn through the entry containing the error, the correct data should be recorded, and the individual making the correction should sign and date it. The original entry should never be obliterated.
3. For errors corrected in a computer-based record, the system should preserve both the original entry and the amendment, as well as the identity of the person making the amendment and the date and time it was made.

- If the health care practitioner does not agree that a correction is warranted, he or she should discuss the matter with the patient or the patient's legal representative. The patient or the patient's legal representative may make a separate statement in writing or on a computer disputing the information and offering an amendment. Such a statement should be filed with the record or made a part of it and included with any future disclosures.

The following examples from AHIMA illustrate documents necessary to comply with the rules. The sample forms were developed by the American Health Information Management Association for discussion purposes only. They should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

1. Employee/Student/Volunteer Nondisclosure Agreement
2. Employee/Student/Volunteer Nondisclosure Acknowledgement
3. Contractor/Vendor Nondisclosure Agreement
4. Authorization for Disclosure of Health Information
5. Revocation of Authorization for Disclosure of Health Information
6. Request for Correction/Amendment of Health Information
7. Facsimile Cover Letter
8. Record of Verbal Disclosure of Health Information
9. Electronic Data Interchange Nondisclosure Agreement
10. Statement Accompanying Disclosures

The attached sample documents including sample forms are taken from "Release and Disclosure, Guidelines Regarding Maintenance and Disclosure of Health Information," published by AHIMA.

Exhibit 1

Employee/Student/Volunteer Nondisclosure Acknowledgement

I have been asked by *[name of health care facility]* to reaffirm my commitment made at the time of my employment/assignment to protect the confidentiality of health information. I understand that *[name of health care facility]* reminds its employees and volunteers of their confidentiality obligations on a periodic basis to help ensure compliance, due to the significance of this issue. By my signature below, I acknowledge that I made the commitment set forth below at the time of my employment/assignment, I confirm my past compliance with it, and I reaffirm my continued obligation to it.

[Name of health care facility] has a legal and ethical responsibility to safeguard the privacy of all patients and protect the confidentiality of their health information. In the course of my employment/assignment at *[name of health care facility]*, I may come into possession of confidential patient information, even though I may not be directly involved in providing patient services.

I understand that such information must be maintained in the strictest confidence. As a condition of my employment/assignment, I hereby agree that, unless directed by my supervisor, I will not at any time during or after my employment/assignment with *[name of health care facility]* disclose any patient information to any person whatsoever or permit any person whatsoever to examine or make copies of any patient reports or other documents prepared by me, coming into my possession, or under my control, or use patient information, other than as necessary in the course of my employment/assignment.

When patient information must be discussed with other health care practitioners in the course of my work, I will use discretion to ensure that such conversations cannot be overheard by others who are not involved in the patient's care.

I understand that violation of this agreement may result in corrective action, up to and including discharge.

_____
Signature of Employee/Student/Volunteer

_____
Date

Note: This sample form was developed by the American Health Information Management Association for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Exhibit 2

Contractor/Vendor Nondisclosure Agreement

[Name of health care facility] has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their health information. In the course of its business relationship with *[name of health care facility]*, *[name of vendor/contractor]* and/or its employees and/or agents may come into possession of confidential patient information, even though it may not be directly involved in providing patient services.

In consideration of, and as a condition to, its business relationship with *[name of health care facility], [name of vendor/contractor]* and its employees and/or agents will hold the following information ("confidential information") in strictest confidence:

(1) any information supplied by *[health care facility]* or its affiliates;

(2) any information which is the direct or indirect result of *[name of vendor/contractor]*'s services provided for *[name of health care facility]*; and

(3) any information about *[name of health care facility]*'s or its affiliates' business operations, products, services, or patients.

No confidential information shall be disclosed except to employees of *[name of vendor/contractor]* who need to know it to fulfill *[name of vendor/contractor]*'s obligations to *[name of health care facility]* or to authorized representatives of *[name of health care facility]*. At any time, upon request of *[name of health care facility], [name of vendor/contractor]* will return promptly all embodiments of confidential information in a form acceptable to *[name of health care facility]* without retaining any copies thereof. Furthermore, *[name of vendor/contractor]* will not sell, share, discuss, assign, transfer, or otherwise disclose any confidential information outlined above with any other individuals or business entities and will not use the confidential information for any purpose other than providing the mutually agreed upon services.

It is understood that "confidential information" does not include information which:

(a) generally becomes available to the public other than as a result of disclosure by *[name of vendor/contractor]* or

(b) was available to *[name of vendor/contractor]* on a non-confidential basis prior to its disclosure by *[name of health care facility].*

At all times during the term of *[name of vendor/contractor]*'s agreement with *[name of health care facility]* and thereafter, *[name of vendor/contractor]* and its employees and agents shall protect the confidential information from unauthorized use or disclosure and otherwise abide by the terms of this agreement.

_____ _____

Signature of Vendor/Contractor Date

Note: This sample form was developed by the American Health Information Management Association for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Exhibit 3

Authorization for Disclosure of Health Information

1. I hereby authorize [name of provider]_____ to disclose the following information from the health records of:

   Patient name _____ Date of birth
   _____

   Address _____ Telephone
   _____

   _____ Patient number
   _____

   covering the period(s) of health care

   From (date) _____ to (date)_____

   From (date) _____to (date)_____

2. Information to be disclosed:
   - ☐ complete health record(s)
   - ☐ discharge summary
   - ☐ history & physical examination
   - ☐ progress notes
   - ☐ consultation reports
   - ☐ laboratory tests
   - ☐ X-ray reports
   - ☐ photographs, videotapes, digital or other images
   - ☐ other (please specify) _____

   I understand that this will include information relating to (check if applicable):
   - ☐ acquired immunodeficiency syndrome (AIDS) human immunodeficiency virus (HIV) infection
   - ☐ behavioral health service/psychiatric care
   - ☐ treatment for alcohol and/or drug abuse

3. This information is to be disclosed to _____

for the purpose of _____.

4. I understand this authorization may be revoked in writing at any time, except to the extent that action has been taken in reliance on this authorization. Unless otherwise revoked, this authorization will expire on the following date, event, or condition:
   _____.

5. The facility, its employees, officers, and physicians are hereby released from any legal responsibility or liability for disclosure of the above information to the extent indicated and authorized herein.

Signed: _____
(patient) (date)

_____
or (legal representative) (relationship to patient) (date)

_____
(signature of witness) (date)

Note: This sample form was developed by the American Health Information Management Association for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Exhibit 4

Revocation of Authorization for Disclosure of Health Information

(1) I hereby revoke authorization to _____[name of provider]_____to disclose information from the health records of:

Patient name _____ Date of birth _____

Address_____ Telephone _____

Patient number_____

covering the period(s) of health care:

From (date) _____ to (date)_____

From (date) _____ to (date)_____

From (date) _____ to (date)_____

From (date) _____ to (date)_____

(2) I understand that disclosures made in good faith may have already occurred in reliance upon my previously issued authorization and that this revocation cannot apply retroactively to such disclosures. I also understand that the disclosure of health information may be required by law in some instances, such as for the reporting of communicable diseases.

(3) The facility, its employees, officers, and physicians are hereby released from any legal responsibility or liability for disclosure of the information I authorized previously.

Signed:_____ _____
Signature of Patient or Legal Representative Date

_____ _____
Signature of Witness Date

Note: This sample form was developed by the American Health Information Management Association for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Exhibit 5

Request for Correction/Amendment of Health Information

Patient name _____ Date of birth _____

Patient number _____ Telephone_____

Date of entry to be amended _____

Type of entry to be amended _____

Please explain how the entry is incorrect or incomplete. What should the entry state in order to be more accurate or complete?

Would you like this amendment sent to anyone to whom we may have disclosed information in the past? If so, please specify the name and address of the organization or individual.

_____ _____

Signature of Patient or Legal Representative Date

Comments of Health care Practitioner:

_____ _____

Signature of Health care Practitioner Date

Note: This sample form was developed by the American Health Information Management Association for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Exhibit 6

Facsimile Cover Letter

[sending facility name]
[address]
[city, state, zip code]
[telephone number]
[facsimile number]

DATE: _____ TIME: _____ NUMBER OF PAGES: _____

TO: _____
(name of authorized receiver)

_____
(name of authorized receiver's facility)

TELEPHONE: _____FAX: _____
(or receiver) (of receiver)

FROM: _____
(name of sender)

TELEPHONE: _____FAX: _____
(of sender) (of sender)

Comments:

*****CONFIDENTIALITY NOTICE*****

The documents accompanying this telecopy transmission contain confidential information belonging to the sender that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party and is required to destroy the information after its stated need has been fulfilled, unless otherwise required by state law.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this telecopy in error, please notify the sender immediately to arrange for return of these documents.

Note: This sample form was developed by the American Health Information Management Association for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Exhibit 7

Record of Verbal Disclosure of Health Information

Patient name _____ Date of birth _____

Patient number _____

Date of disclosure _____ Time of disclosure _____

Information disclosed to:

Name _____

Address _____

_____

Telephone Number _____

Reason for disclosure _____

Specific information disclosed:

_____ _____

Signature of Individual Making Disclosure Date

Note: This sample form was developed by the American Health Information Management Association for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Exhibit 8

Electronic Data Interchange Nondisclosure Agreement

This agreement applies to all data transmitted electronically between *[name of health care facility]* and *[name of other party]* in connection with its *[business relationship]*. In consideration of, and as a condition to, *[business relationship]*, *[name of other party]* agrees to: (1) ensure that all such data is secure and to prevent unauthorized access to its facilities and system in which such data is maintained and through which such data is transmitted; and (2) ensure that such data is maintained in strict confidence and not disclosed to any unauthorized person/entity.

In addition, *[name of other party]*, agrees (1) to use this information only for the purpose of providing services to *[name of health care facility]* for *[purposes of the business relationship]*; and (2) to disclose this information only to those of its employees or agents who need to access the information to provide services to *[name of health care facility]* for *[purposes of the business relationship]* and who have signed a confidentiality statement providing substantially the same protection for the data as this agreement.

If a party to this agreement uses an intermediary third party to transmit, log, or process data, that party shall, prior to the disclosure of data, obtain an agreement from that third party providing substantially the same protection for the data as this agreement and shall be responsible for any acts, failures, or omissions by that third party in its provision of services. For purposes of this agreement, the third party shall be deemed to be an agent of that party.

Further, *[name of other party]* agrees to indemnify and hold harmless *[name of health care facility]* from all damages, losses, costs, liabilities, and expenses resulting from any and all breaches of this agreement by *[name of other party]*, its employees, or agents.

The obligations of *[name of other party]* under this agreement, including, without limitation, its responsibility for maintaining the security and confidentiality of the data, shall survive termination of the *[business relationship]*. Upon termination of the *[business relationship]* or upon request of *[name of health care facility]*, all information shall be returned to *[name of health care facility]* in a form acceptable to *[name of health care facility],* and no copies thereof may be retained by *[name of other party]*.

_____ _____
Signature of Health care Facility Date

_____ _____
Signature of Receiving Party Date

Note: This sample form was developed by the American Health Information Management Association for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Exhibit 9

Statement Accompanying Disclosures

As the recipient of this information, you are prohibited from using this information for any purpose other than the stated purpose. You may disclose this information to another party ONLY:

- with written authorization from the patient or his or her legal representative;
- as required by state law; or
- if urgently needed for the patient's continued care.

You must destroy this information after its stated need has been fulfilled.

If this disclosure contains information relating to alcohol or drug abuse education, training, treatment, rehabilitation, or research, the following shall apply:

This information has been disclosed to you from records whose confidentiality is protected by federal law. Federal regulations (Title 42 CFR Part 2) prohibit you from making any further disclosure of it without the specific written consent of the person to whom it pertains, or as otherwise permitted by such regulations. A general authorization for the release of medical or other information is NOT sufficient for this purpose.

Note: This sample form was developed by the American Health Information Management Association for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Toolkit Section 5.3

Helpbot: Complying with Patient Information Requirements

Researchers from George Washington University (Arwa Al-aama, Lance Hoffman, Ph.D, and Anya Kim) and Georgetown University Medical Center (Jeff Collmann, Ph.D and Marion Meissner) have developed a World Wide Web instructional tool known as HelpBot to inform patients about how they safeguard the security of patient information in Project Phoenix, a telemedicine in hemodialysis project funded by the National Library of Medicine. HelpBot enables patients and family members to explore Project Phoenix's approach to data security as deeply as individually required simply by clicking through various levels of the tool. Four basic levels exist, including a homepage that introduces the whole project, a level that explains the telemedicine network, a level that explains the risks to data security found during our risk assessment of the telemedicine network, and a level explaining our risk management plan. A user can navigate through the tool in an infinite number of ways, depending on their need to know and personal approach to learning. For example, if a patient wants to go straight from the beginning to the end, he can proceed horizontally from the introduction to the risk management plan. If a family member wants to vertically explore a particular component of the system, the telemedicine unit for example, she can click on the telemedicine unit, then click on the risks in the telemedicine unit, and finally click on how the risks are being handled. At any point, a user can change the search pattern, return to the beginning, or exit. In relevant sections, a user can activate hot links to other sites (for example, the firewall guide of the International Computer Security Association) while staying within the HelpBot frame. Patients thus obtain as detailed an explanation of the project's approach to data security as they desire by determining for themselves the level of detail actually searched. The design of HelpBot incorporates principles of human-computer interface theory and computer-based education to make it easy for anyone to use with little or no support. Because HelpBot resides on the World Wide Web, anyone with Internet access may use it. HelpBot thus represents one way a healthcare organization can explain its health information security program in a form readily understandable and accessible to patients. To view the current version and/or to find instructions for developing your own version of HelpBot, please see http://www.healthdatasecurity.georgetown.edu.

Toolkit Section 6.0

Chapter Six

INSTITUTIONALIZING RESPONSIBILITY

Toolkit Section 6.1

Introduction

The well known maxim "Confidentiality is everybody's business" states the basic truth. Transforming this truism into practice requires institutional work and personal commitment. This toolkit provides models and methods for assisting health care providers to manage patient records as a broad institutional process, including the technical protection of the information system. In addition to these concrete methods, however, health care providers should institutionalize a sense of responsibility for maintaining patient confidentiality at all levels, including individual staff, program managers, and organizational administrators. Health care providers should develop methods for binding these levels of responsibility together such as in the illustration of the "Trustee/Custodian Agreements" from Kaiser Permanente explained below.

Individual Responsibilities

In the course of doing their daily work, individual staff will acquire medical, familial, financial, and other types of private information about patients. They should divulge such information only to authorized persons and for authorized purposes as required. They should never discuss such information outside the context of patient care, quality assurance, authorized research activities, or as required by law or administrative edict. They should attend all in-service training on data security and patient confidentiality. They should read and comprehend the organization's policies, procedures, and practices for data security and patient confidentiality. They are individually responsible for seeking answers to questions and/or issues they do not understand in these processes including bringing ambiguous, incomplete, or erroneous policies, procedures, and practices to the attention of the organization's administrators. Success in discharging these duties merit positive notice in annual evaluations. Failure to discharge one's individual obligations in maintaining patient confidentiality may lead to disciplinary action including possible dismissal.

Program Responsibilities

A health care organization's program directors, including physicians, investigators, and unit managers, are responsible for creating and promoting a climate for maintaining the confidentiality of patient information. Conditions favorable to such a climate include acting as role models in practicing good patient confidentiality practices; developing effective staff in-service training programs on patient confidentiality; aggressively investigating and disciplining potential breaches of patient confidentiality; rewarding exemplary practices in maintaining patient confidentiality; developing and revising policies, procedures, and practices for patient confidentiality as needed; and communicating a sense of good confidentiality practices to patients. Success in creating and promoting a satisfactory climate for patient confidentiality merits positive notice in annual evaluation. Failure to promote a satisfactory climate for patient confidentiality may lead to disciplinary action including reassignment or removal from the project team. Organizational Responsibilities

The organization's central administration bears responsibility for supporting physicians, administrators, and staff in their efforts to maintain patient confidentiality. Such support includes agreeing to cooperate in developing jointly acceptable policies, procedures, and practices for maintaining patient confidentiality; assuring project management promotes a climate of patient confidentiality; affirming project management's authority to investigate and discipline potential breaches of patient confidentiality; and including performance in maintaining patient confidentiality as a component of the staff's annual evaluation. Institutional officials should continuously reaffirm the importance of good patient confidentiality practices to the life of the health care organization.

Toolkit Section 6.2

Case Study: Kaiser Permanente's Trustee/Custodian Agreement

Kaiser Permanente has created two special roles, the information trustee and information custodian. The information trustee and custodian link regular staff and information technology and security specialists. In large organizations, the differentiation of work roles, particularly between clinical and non-clinical staff, threatens to isolate information security functions. By creating the trustee/custodian relationship Kaiser has institutionalized mutual responsibility for secure information control between clinical and information staff, thus integrating not segregating it from everyday work. Not all health care providers require developing an arrangement as formal as Kaiser's Trustee/Custodian Agreement, yet, most organizations larger than a single physician office differentiate between clinical and information systems staff. Formulating roles institutionalizing a sense of mutual responsibility for information security among staff operationalizes the idea that confidentiality is everybody's business. Instead of relegating information security to the technical specialists and parceling responsibility for managing patients only to clinicians, all staff assume responsibility for the enterprise, its patients, and the confidentiality of patient information.

Data Trusteeship at Kaiser Permanente Northern California

In recent years, more essential business functions have become dependent on information technology; therefore, the way business systems are designed and implemented by Kaiser Permanente Northern California Region (KPNCR) has evolved. To keep up with the rapid changes brought on by technological growth, KPNCR must adapt and fine tune its approach to design and implement systems that provide security and promote higher data quality.

In January 1996, the Trustee Project was initiated in response to various audit recommendations and criteria of the National Committee for Quality Assurance. The project:

- Identifies and/or verifies Trustees for KPNCR's data processing resources (objects), regardless of platform (applications, operation files/databases, reporting/filing databases, transactions)
- Maintains information in a comprehensive, centralized list for KPNCR employees
- Establishes an infrastructure to implement a continuing process to grant access to these resources
- Follows the initiatives already implemented by Kaiser Permanente Southern California

This document provides guidelines on the Trustee's roles and responsibilities in relation to data quality, usage, classification, and protection.

Roles and Responsibilities

The Trustee is an individual manager or agent of the manager accountable for leading, managing, and administering activities related to an application and its data. The Trustee:

- Determines logical controls for KPNCR data assets
- Determines how a business application and its data are used and develops and communicates policies, standards, and procedures that are consistent with Regional policies, standards, and procedures
- Approves access to data by users
- Audits and monitors applications for appropriate access to and use of data
- Initiates corrective action in the event of inappropriate or unauthorized use
- Identifies data belonging to the application and classifies it according to "classification criteria"
- Defines control mechanisms for classified data
- Ensures that access audit reports are being monitored
- Specifies acceptable level of data quality during the development of an application
- Approves requests for changes to production data outside the normal business process
- Designates one or more surrogates to act on his or her behalf if necessary

The Information Confidentiality, Privacy, and Security Group (ICPSG) represents major organizational groups within KPNCR irrespective of the organizational entity. This group is responsible for establishing, maintaining, and monitoring compliance with policies, standards, and procedures, as well

as discussing and resolving issues related to information security. The ICPSG has published Regional policies, standards, and procedures regarding confidentiality and data classifications.

The Data Quality Leadership Team (DQLT) leads the effort to identify, organize, and integrate KPNCR's many systems currently in operation to ultimately improve the quality of data. This group allows KPNCR to make timely and appropriate clinical and business decisions. The DQLT is responsible for:

- Developing data quality policy
- Providing oversight of the implementation of the Data Quality Administration Plan
- Monitoring and evaluating data quality within KPNCR
- Improving the data quality administration process
- Reviewing and approving plans for data quality system issues that conflict with Regional data quality policies
- Establishing process teams after reviewing current data quality efforts and requirements

Data Classification

All corporate data, regardless of medium, is classified according to its value and level of sensitivity. Classification refers to a rank assigned to data based on the real monetary cost to replace the data and the degree to which disclosure or misuse could damage a patient, customer, business partner, or KPNCR. The classification/level of sensitivity determines the access controls to be placed upon the data.

Within general categories of data (e.g., patient medical record), some data may be considered more sensitive or critical than others. Inappropriate disclosure of some information in the patient medical record (e.g., mental health) , whether accidental or intentional, could be especially damaging to the patient. Therefore, this data shall have a higher level of classification. Data is classified as follows:

Public

- Classification Criteria: none
- Examples: publications to customers, press releases
- Access Protocol: available to the general public
- Encryption: not required
- Auditing: none

Internal

- Classification Criteria: disclosure may cause some harm to KPNCR or its customers
- Examples: internal phone directories, organizational memos, announcements, procedures
- Access Protocol: generally available to all staff on a need-to-know basis
- Encryption: required if transmitted via Internet
- Auditing: none

Confidential

- Classification Criteria: disclosure may cause some harm to KPNCR or its customers
- Examples: patient laboratory results, treatments, admissions, visits, appointment data (except for that which is REGISTERED CONFIDENTIAL), customer/vendor files, personnel memos
- Access Protocol: limited to as few persons as possible on a need-to-know basis
- Encryption: required if transmitted via Internet
- Auditing: access should be audited as determined by the Trustee and ICPSG

Registered Confidential

- Classification Criteria: access may cause severe harm to KPNCR or its Customers and employees
- Examples: mental health/substance abuse treatment data; strategic corporate plans/financial information; payroll, benefits, and personnel data

- Access Protocol: limited to as few persons as possible on a need-to-know basis
- Encryption: required if transmitted over the Internet
- Auditing : all access should be audited and alerts should be triggered by criteria specified by the Trustee and/or the ICPSG. Alerts should be reported as close to real time as possible to the individual designated by the Trustee.

Data Issues

Data Issues can be classified as quality issues or security issues. This section focuses on the definition of both types of issues and their characteristics.

Quality Issues

Quality issues refer to data that is consistent with its expected value. The expected values should be defined by the Trustee at the time the application that collects and stores the data is developed. Implicit in this definition is that data are captured and maintained in the source applications and support the business activities of its users. Quality of data is the responsibility of the collecting application.

To ensure quality is high or that the expected value has been captured, data should possess the following characteristics:

- Accessibility: must be available to the client
- Integrity: processing of the data must not change the business meaning of the data
- Availability: current and available to the client when needed
- Accuracy: must represent correct values
- Consistency: consistently valued and can be shared across the business entities

Any inconsistencies that arise related to the characteristics should be addressed as quality issues. Types of quality issues are:

1. Inaccurate data: may be caused by errors in data entry, errors in transformation, or errors in querying the data. An example is the Diagnostic Related Group (DRG) table with fields that have shifted to the right one character causing the DRG 124 to become 12. This would result in the reporting of an entirely different DRG.

2. Incomplete data: may be caused by applications that do not consistently value pertinent fields within their system. An example is the provider field that identifies a member's primary care provider. This field only has value if a primary care provider has been designated. Incomplete data will exist for those members who do not have a primary care provider designated.

3. Inconsistent data: may be caused by applications that have been developed over time that report similar information with different formats. An example is the birth date. On the membership database, this field is six characters, but on the patient demographic database, the field is eight characters.

4. Missing data: results from operational applications that did not collect the required information for whatever reason. An example would be the ordering provider on the radiology application. If an area chooses not to collect these data, the field operationally defaults to the department chief.

5. Non-Captured data: results when data have not been captured for the input source. This issue relates to expectations of users. An assumption may be that members height and weight are captured in the Reg Plus application. This would be an inappropriate assumption given that this is an appointment registration system and is not designed to capture clinical information.

Security Issues

Security issues refer to:

- Data, image, and text security and application systems controls not in accordance with the ICPS policies, standards, and procedures
- Unauthorized attempts to gain access to data
- Unauthorized use of data (those not authorized by Trustee to access data)
- Any breach of information confidentiality

Summary

Although KPNCR owns all data processing resources, Trusteeship identifies the business representative responsible for quality, which affects data integrity, availability, and confidentiality. As KPNCR evolves to maintain its position as a leader in the health care industry, complex data issues need to be tracked, monitored, and resolved. This may seem somewhat idealistic in nature and is very hard to measure, but a measurable result will be achieved with the strong commitment and support of the Trustee.

Example Format and Content for a Trustee-Custodian Agreement

Ownership

Governance:

The [name of Organization] is the active governing body over the direction of the [System/Application].

Sponsor(s):

[Sponsor name(s) and title(s)]

Trustee(s):

[Trustee name(s) and title(s)]

Custodian(s):

[Custodian name(s) and title(s)]

Responsibilities:

The Trustee(s) is an individual or group of senior manager(s) or agent(s) of the manager(s) accountable for leading, managing, and administering activities related to a system/application and its data. A Trustee representing an operational business unit is required for every business application and is responsible for:

- Developing a Trustee/Custodian agreement
- Assigning sensitivity levels to data
- Identifying potential risks to business applications and data
- Identifying individuals who use business applications and data
- Coordinating business units needs
- Developing standard application and data access profiles for job functions
- Reviewing and approving/denying access requests which deviate from profiles
- Auditing and monitoring applications for appropriate access to and use of data
- Advising Human Resources on the seriousness of an infraction when unauthorized use has occurred
- Ensuring that access audit reports are reviewed
- Determining retention periods for data and output (e.g., reports)
- Specifying acceptable levels of data quality during the development of an application
- Approving requests for changes to production data outside the normal business process
- Planning for resumption of business activities after an outage or period of unavailability
- Formally designating one or more surrogates, who may act in the Trustee's behalf.

The Custodian is the individual or organization entrusted with the physical possession or management of the system and data. All systems and data must be assigned to a Custodian. The Custodian may or may not belong to the Information Technology (IT) organization. The Custodian is responsible for:

- Implementing measures to ensure that the media upon which the data is stored are physically secure
- Ensuring that sensitivity levels are technically enforced
- Ensuring the availability of data for processing on a continuing basis
- Implementing technologies that secure data during transmission over private or public networks

- Implementing storage technologies under which processing is optimized
- Implementing storage and retention procedures
- Developing and implementing backup, recovery, and business resumption plans to ensure that the impact of any system failure or disruption is minimized
- Ensuring the availability of backup data

IT is responsible for:

- Ensuring availability of systems and data
- Providing tools and support for controlling access to data
- Administering access controls
- Reporting and analyzing audit log data

Access to Production [System/Application]:

- Individual user IDs are [not] required to access the [System/Application]. Shared user IDs are [not] permitted.
- Prior to any release or transmittal of [System/Application] data, written approval must be obtained from the Trustee.
- Procedures:
  - Requests for access to [System/Application] are made using the [process or form].
  - Requests for new access or changes to access levels are submitted by authorized requestors on behalf of individual users.
  - An individual's access privileges in [System/Application] are determined by identifying the individual's job function with pre-defined model security profiles. If the individual does not meet any pre-defined model, or requires greater privileges than the job function allows, then the request must be approved by one or more of the Trustees (e-mail is acceptable), who assigns an appropriate security profile to the requester.
  - Information Security completes all requests by assigning security profiles as appropriate.
- It is the responsibility of the individual user's supervisor/manager to notify Information Security of employee terminations and employee transfers that cause a change in an individual's access requirements.
- Information Security provides [frequency] reports to the Trustee, listing all persons who have received access to [System/Application].

Access to Data:

- Data used by [System/Application] are of two types:
  - Operational: data used in the continuing, real-time operation of [System/Application]
  - Archival: data contained and managed offline and/or in "data warehouses" and used principally for creation of management reports
- Operational data is subject to the following rules:
  - Individual users in functional business areas may access and update operational data in accordance with their security profiles.
  - IT staff access to operational data is restricted to: IT Application support staff and database administrators currently assigned to support [System/Application], who may browse data to verify that [System/Application] is working correctly.
  - In an emergency situation, the Trustee may authorize a database administrator to modify data. This must be requested and documented in accordance with Change Control procedures.
- Archival data is subject to the following rules:
  - Individual users in functional business areas may access and update operational data in accordance with their security profiles.
  - IT Application support staff and database administrators currently assigned to support [System/Application], may browse data to verify that [System/Application] is working correctly.

Security Incident Reporting:

- Unusual activity (e.g., six or more repetitive unsuccessful log-in attempts, unusual hours of access, etc.) identified by Information Security will be brought to the attention of the Trustee.
- Information Security will review the [System/Application] transaction logs as required per incident reported.
- Formal incident reporting procedures are described in the [name of procedure/manual].

Output Distribution:

- The Trustee is responsible for ensuring the completeness and accuracy of the results of processing.
- IT will provide the Trustee with a master schedule of the output produced by [System/Application]. IT will update and re-issue the schedule as needed.
- Recipients are responsible for reconciling receipt of expected output.
- Missing or misdirected output should be brought to the attention of [IT customer services].
- The Trustee must approve the online or hard-copy distribution of output. A [frequency] report showing [System/Application] output and its distribution/online access will be sent to will be sent to the Trustee for review and approval.

Problem Management:

- The Trustee will be notified by IT as follows in the event normal processing is interrupted:
  - [online not available - time and method for contacting Trustee]
  - [output delayed - time and method for contacting Trustee]
- The [first level title] is the first contact point for problems identified by individuals. If it is determined that the problem is system- or application-wide, the [first level title] will notify [second level title] of the details.
- [Second level title] is the contact point for problems if the [first level title] is unavailable.
- [Second level title] documents and assigns problems to the appropriate IT organization.
- At the direction of the Trustee/Custodian or IT support staff, [second level title] will immediately notify [local operations or individual users] regarding production problems and resolutions.

Change Control:

- As needed, the [organization] meets to prioritize and approve changes.
- Prior to implementation of changes, Trustees/Custodians will be notified.
- All changes must be reasonably tested and debugged, with due care, prior to implementation in production.
- Changes are reviewed [with what frequency, and by whom].

System/Application Recovery and Availability:

- Data for the [System/Application] will be backed up via [technology] and stored [location] on a [frequency] basis.
- [N months/years] of historical data will be retained.
- In the event of failure [System/Application] data will be recoverable to [when (e.g., within 60 minutes of failure, end of previous day, etc.)].
- In the event of a major disaster, the restoration of [System/Application] will fall under the Business Resumption Plan, which currently provides for restoration of systems/applications within [time frame] of initial failure.
- The Trustee, Custodian, and IT will annually, or at the request of the Trustee/Custodian, review and test backup requirements to ensure that the recovery process works successfully and that the backups are accurate.
- Prior to purging archived data, the Trustee must be notified and written approval obtained.

Production Scheduling:

- Batch scheduling requirements for [System/Application] are determined by the Trustee and Custodian and provided to IT production control at implementation.
- Initial scheduling requirements are determined by the Trustee prior to implementation. Changes to [System/Application] processing must originate from, or be approved by, the Trustee/Custodian.

- By-request jobs are scheduled through IT production control.
- The details of scheduling requirements are documented and maintained [in hard copy with IT production control, or in an automated scheduling system].

Interfaces:

- The following systems have online interfaces that transmit data continuously to [System/Application]:
  - [system 1]
  - [system 2]
  - [system n]
- [System/Application] continuously transmits data to:
  - [system 1]
  - [system 2]
  - [system n]
- All changes to, or additions of, interfaces must be performed in accordance to the change control procedures.

User Documentation:

- The Trustee, Custodian, and IT are responsible for developing and maintaining user documentation.
- User documentation comprises [as appropriate to System/Application]:
  - General user of [System/Application]
  - Screen functions
  - Report definitions
  - Data editing criteria
  - Error messages
  - Business continuity/recovery plans
  - Balancing and control processes
  - Processing cycles/deadlines
  - Report definitions
  - Desk procedures

Witnesses:

The guidelines for administration of the Trustee/Custodian agreement with Information Technology have been reviewed and approved by:

_____	_____
Sponsor - [name]	Date Signed
_____	_____
Trustee - [name]	Date Signed
_____	_____
Custodian -[name]	Date Signed
_____	_____
IT (if different from Custodian) - [name]	Date Signed

Note: In the event that there are multiple Sponsors, Trustees, Custodians, or IT representatives, signature lines should be included for all parties.

Toolkit Section 7.0

Chapter Seven

WEB SITES

Because the World Wide Web has become such a rich resource, we have carefully listed Web site addresses throughout the *CPRI Toolkit*. A comprehensive list by chapter appears below in alphabetical order.

Chapter Three

Organization	***Web Address***
American Health Information and Management Association	http://www.ahima.org
Dept Health & Human Services	http://aspe.os.dhhs.gov
Administrative Simplification	http://aspe.os.dhhs.gov/admnsimp/
Data Security Standards	http://erm.aspe.hhs.gov/erm/secnprm
Medical Privacy Model	http://aspe.os.dhhs.gov/admnsimp/pvcrec.htm
Electronic Privacy Information Center (EPIC)	http://www.epic.org
National Conference of State Legislatures	http://www.ncsl.org
National Council for Prescription Drug Program	http://www.ncpdp.org
National Institute of Standards and Technology (NIST) Computer Security Resource Clearinghouse (CSRC)	http://csrc.nist.gov
Washington Publishing Company	http://www.wpc-edi.com
"Thomas"—federal bill tracking	http://thomas.loc.gov
For the Record: Protecting Health Information	http://www.nap.edu/books/0309056977/html/index.html
Crisis Emergency Response Team (CERT)	http// :www.cert.org
Secure Environment for Information Systems in Medicine (SEISMED)	http://www.semper.org/sirene/projects/seismed

Chapter Four

Organization	***Web Address***
American Health Information Management Association (AHIMA)	www.ahima.org
American Medical Informatics Association (AMIA)	www.amia.org
Center for Healthcare Information Management (CHIM)	www.chim.org
College of Healthcare Information Management Executives	http://chime-net.org
Computerized Patient Records Institute (CPRI)	www.cpri.org
Health Care Finance Administration	http://www.hcfa.gov
Healthcare Information Management Systems Society (HIMSS)	www.himss.org
International Computer Security Association (ICSA)	www.icsa.net
Joint Healthcare Information Technology Alliance	www.jhita.org
MIS Training Institute	www.misti.com
Netscape on SSL	http://home.netscape.com/products/security/ssl/index.html
NIST on firewalls	http://csrc.ncsl.nist.gov/nistpubs/800-10/main.html
PCASSO	http://medicine.ucsd.edu/pcasso
RSA Data Security	http://www.rsa.com
SSL Discussion	http://www.rsa.com/ssl/basics/index.html
FAQ Crytography	http://www.rsa.com/rsalabs/faq/
Tunitas Group	http://home.earthlink.net/~tunitas

Chapter Five

Organization	***Web Address***
American Health Information Management Association (AHIMA)	www.ahima.org
HelpBot	
Georgetown University	http://www.healthdatasecurity.georgetown.edu
To Design	http://www.seas.gwu.edu/seas/projects/phoenix/document/howto.html

Chapter Nine

Organization	***Web Address***
Computer-based Patient Record Institute	www.cpri.org
Netscape	http://home.netscape.com/products/security/
PC Web	http://www.pcwebopedia.com
RSA Data Security	www.rsa.com
Tech Encyclopedia	www.techweb.com/encyclopedia/
Whatis?com	www.whatis.com

Toolkit Section 8.0

Chapter Eight

GLOSSARY

Introduction

This glossary was prepared to provide a consistent set of definitions for terms related to the security of computer-based patient records. As many of the terms are integrally related, an introduction has been prepared to provide context to the terms in the glossary, to demonstrate the inter-relationships among certain key terms, and to guide the user in interpreting terms used in the definitions. As in all language that is contextually rich and complex, there may be several terms which technically may carry variations in meanings but which are often used synonymously. Every effort has been made to be sensitive to the politically correct usage of terms.

While there are annotations provided for all terms in the glossary, the actual definitions provided are not necessarily reported verbatim from the references annotated, but rather some have been interpreted for the context of health information. Experts involved in the project performed the editing based on personal experience and usage of the terms. In this way, the definitions of the terms both fit the purpose intended and are readable by both technically knowledgeable as well as lay individuals who may choose to refer to this work.

It is the intention of the CPRI Work Group to continuously add, update, and revise this document as appropriate. Comments and/or suggestions for inclusions, deletions, and revisions of definitions should be submitted to CPRI for consideration.

Acknowledgments

The original document was prepared in 1996 by members of the Work Group on Confidentiality, Privacy, and Security, Kathleen Frawley and Dale W. Miller, co-chairpersons. The leader of the glossary project team was Dianne Vollgraff. These individuals are indebted to the many volunteers who participated in the work group meetings, provided input, and prepared and reviewed the drafts of this document. In January 1999, additional edits and updates were made by the CPRI Confidentiality and Security Tool Kit Task Force, Ted Cooper, MD, Chairperson. The leader of the glossary project was Barbara Demster. Updates included terms contained in new guidelines published subsequent to the glossary as well as new terms considered by the Task Force to be important additions (e.g., Secure Sockets Layer Technology, etc.)

GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN COMPUTER-BASED PATIENT RECORD SYSTEMS

A computer-based patient record (CPR) is electronically maintained information about an individual's lifetime health status and health care. A CPR resides in a computer-based patient record system (CPR system) which provides the functionality to support

data capture, storage, processing, communication, security, and presentation. CPR systems exist in multiple, disperse locations where health care may be provided.

Currently, there are few complete CPR systems. Components of CPR systems are generally independent of other locations' systems. Security mechanisms are important in any environment where confidential health information is maintained but become even more important as electronic systems are used and components of CPRs become connected for exchanging information across locations which may contribute to continuity of care. For example, a patient may have been born in one hospital, transferred to a neonatal intensive care unit of another hospital, returned home with home care and telemedicine consultations, and later moved to a new location and another provider who needs to understand the nature of the patient's chronic condition. A CPR system would contain the functionality to identify the various locations of health information, and, with the patient's consent, permit access to specific information to authorized users. The locations and nature of information contained in the respective CPRs must never be accessible to anyone without patient authorization and legitimate need for the information.

In order for specific health information to be available when needed, there must be both provisions for access and security measures to control that only authorized individuals or entities obtain the information. A primary function of a CPR system is to provide the security that ensures confidentiality of private health information that has been disclosed to a caregiver. Security systems also protect the integrity of that data.

Privacy, confidentiality, and security are integrally related concepts. Privacy refers to the right of individuals to keep information about himself or herself from being disclosed to anyone. However, once information is disclosed, such as for the purpose of obtaining health care, the obligation of the second party not to permit access to the information without proper authorization and authentication is referred to as confidentiality. When private information is maintained in paper or computer files, security is the means to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss.

Terms Used in Context of the Glossary

Many terms are associated with health information (e.g., data, information, and knowledge) and their compilation and use in an electronic environment (e.g., computer-based patient record, and automated record of care). Many terms are also associated with those who both receive health care (e.g., consumer, patient, client, and person) and provide health care (e.g., provider, caregiver, clinician, doctor, nurse, and hospital). While there are differences among these terms, some terms are used synonymously and some terms have more politically correct usage. There are many new concepts associated with CPRs for which terms may not have been agreed upon. This is especially true in discussing data that can be identified with a patient ("personally identified data") and data that have been stripped of information that can provide information about a patient's identity ("misidentified data") but may still identify a patient for linkage purposes.

Data, information, and knowledge form a continuum. Technically, “data” refers to a sequence of symbols to which meaning may be assigned. Data are raw facts. When data are processed to provide greater meaning or usefulness, the processed data are referred to as "information." An individual data element (such as results of a blood test) may not

provide information because it is not associated with other data that makes the data useful (e.g., the results of the blood test combined with other data may yield the interpretation that the patient has hyponatremia). Practically, the term data is often used synonymously with the term information. Though defined separately, data and information will be used as synonyms in defining other terms in this glossary. "Knowledge" generally means the understanding imparted from a sum of information. (The conclusion that the patient has hyponatremia results from knowledge gleaned from textbooks and experts' summary of findings that hyponatremia is associated with a worsening prognosis in patients with small cell lung cancer.)

The term "computer-based patient record" was coined by the Institute of Medicine patient record study committee in their report: The Computer-based Patient Record: An Essential Technology for Health Care (National Academy Press, 1991). Although many providers and vendors had been creating computer systems designed for clinical information prior to the release of this report, and hence various names such as "electronic medical record" or "clinical information system" exist, the full scope of the concept had not previously been emphasized or summarized through a specific name associated with it. Since the report's release, some have proposed a set of names, which may form a continuum along implementation of the full scope of the vision, although there is no consistent recognition of these names. In Europe, the term "electronic health record" is used to describe efforts toward applying advanced computer technology to health information, though the scope of the information and functionality may not be exactly similar to that in the United States. The term computer-based patient record is used in this glossary with a definition consistent with the full vision providing lifetime health information for a person as promulgated by the Institute of Medicine.

Every person has an associated health status at all times, but information about such health status is generally not recorded continuously except for the purpose of providing care. The nature of the computer-based patient record described in this document refers to information about a person's health status and health care as related to specific services designed to diagnose and treat illness and injury as well as maintain health and promote wellness. When a person receives such health care services, he or she may be considered "patients" (of hospitals or doctors), "clients" (of health care programs), "residents" (of long term care facilities),etc. While every effort is made in this glossary to refer to "health care recipient," individual receiving health care, or person, the more familiar term "patient" may also be used to refer to all who may be receiving any health care services.

Health care services are provided collectively by organizations and individually by physicians, nurses, therapists, and others. Sometimes the term "provider" is used in a restricted sense to refer to an organization or individual receiving direct reimbursement for health care services. As this term is generally limited to hospitals, other health care organizations, and physicians, it does not include an entire cadre of others who provide health care services such as nurses and therapists. "Caregiver" is a term that may be more encompassing when referring to people who provide health care services and may have access to confidential health information about an individual. Health care services associated with diagnosing and treating illness and injury, maintaining health, and

promoting wellness may collectively be referred to as "health care" or "clinical" services; the term "medical" is generally considered to be restricted to care provided by physicians.

"Identity" and "identification" are important concepts when considering the many uses of health information. Standard dictionaries define identification as evidence of identity, and define identity as the distinguishing characteristics of an individual. There is a subtle but very important difference between these two concepts. When direct patient care is provided, the caregiver generally knows the identity of the individual and identifying information such as name, address, birth date, etc. These characteristics serve to identify the identity of the individual. (If the individual assumes a disguise, an alias will identify the person without revealing the identity of the person.) In health care research it is often important to know that disparate information belongs to the same individual without needing to know the identity of the individual. A common identifier may be assigned to information to ensure that one set of information can be linked with another set of information, but neither set of information can necessarily be linked to the individual.

Glossary

Access: The provision of an opportunity to approach, inspect, review, make use of data or information. Refers to such actions by the individual receiving health care as well as providers of health care services and any other individual or entity who has appropriate authorization for such actions. [CPRI, 1995b] The ability to enter, view, or modify information. Access includes the ability to copy or print information as well as the ability to cause it to be transmitted via a computer network or facsimile machine. [CPRI, 1995c]

Access control: The prevention of unauthorized use of a resource. [ISO 7498-2] Information-use policy to determine who can have access to what data/information (both within and external to the organization adopting the access control policy); policies and procedures preventing access by those who are not authorized to have it. [Institute of Medicine, 1994]

Access level: A level associated with an individual who may be accessing information (e.g., a clearance level) or with the information which may be accessed (e.g., a classification level). [National Research Council, 1991]

Access mode: A distinct operation recognized by protection mechanisms as a possible operation on data/information. Read and write are possible modes of access to a computer file; execute is an additional mode of access to a program; and create and delete are access modes for directory objects. [MTR-8201; National Research Council, 1991]

Accountability: The concept that individual persons or entities can be held responsible for specified actions, such as obtaining informed consent or breaching confidentiality. [National Research Council, 1991]

Accuracy: Magnitude of errors in data resulting from miscoding or misrepresenting facts, maintaining out-of-date findings, or commingling of data from more than one person. [Institute of Medicine, 1994]

Administrative (health care) data/information: Data/information collected during the course of a health care event unrelated to the status of the individual's health or health care. Includes demographics, provider identification, caregiver identification, date and time of care, and other such data providing the who, what, when, and where of data capture. [CPRI, 1995a]

Alcohol and drug abuse regulations: Federal law restricts disclosure of patient health information without patient authorization from facilities with federally assisted programs and with an identified unit or providers whose primary function is the provision of substance abuse services, alcohol or drug abuse diagnosis, treatment, or referral for treatment. (42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records, Federal Register 52, 21796, June 9, 1987; Drug Abuse and Treatment Act of 1972 & sect; 408, Public Law No. 92-255.) [Kunitz and Associates, Inc., 1995]

Algorithm: A procedure for solving a mathematical problem in a finite number of steps that frequently involves repetition of an operation. In 1972, the National Bureau of Standards (NBS - now the National Institute of Standards and Technology) identified the need for a data encryption standard for use in unclassified applications. (See Data Encryption Standard below.) [National Research Council, 1991]

Architecture: An arrangement of components intended to fulfill some need. [Tuttle, 1994]

Attack: The act of aggressively trying to bypass security controls. The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system and the effectiveness of existing countermeasures. [Fites and Kratz, 1993]

Audit trail: Documentary evidence of monitoring each operation an individual performs on health information. [National Research Council, 1991] Audit trails may be comprehensive or specific to the individual and information. For example, an audit trail may be a record of all actions taken by anyone on a particularly sensitive file. [OTA, 1993]

Authentication: Proof of authorship that may be in the form of a written signature, or key; identification of the author of a record entry. [Abdelhak, 1996] Providing assurance regarding the identity of subject (author) or object (information). [ASTM 1762] Generally automated and formalized methods of establishing the

authorized nature of a communications partner over the Internet communications data channel itself, generally called an "in-band process." [HCFA, 1998]

Authentication of data origin: Corroboration that the source of data is received as is claimed. [ASTM E1762]

Authentication of user: The provision of assurance of the claimed identity of an individual or entity. [ASTM E1762]

Authorize: Granting of rights, which includes granting of access based on access rights. [ISO 7498-2]

Authorization: The mechanism for obtaining consent for the use and disclosure of health information. The American Health Information Management Association has recommended requirements for valid authorization. Within the context of a computer-based patient record system, these requirements would include that the authorization: be documented (electronically), be addressed to a specific health care provider, specifically identify the patient, identify the individual or entity authorized to receive the information, identify the information that is to be released, specify the purpose for the disclosure, specify under what conditions the authorization will expire unless revoked earlier, indicate that the authorization is subject to revocation, be electronically)signed by the patient or patient's legal representative, and be dated sometime after the information has been collected. [AHIMA, 1994a]

Authorized disclosure: The release of personally identifiable information to a third party upon authorization. [Abdelhak, 1996]

Biometrics: A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual (e.g., hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voiceprints, and handwritten signature). [ASTM E1762]

Breach of Confidentiality: Breach of contract as applied to confidentiality refers to an action by an individual which reveals a confidence entrusted to that individual by another without the other's consent. For example, courts have demonstrated a willingness to apply the ethical standards of the medical profession to compel physicians to maintain the confidentiality of information they obtain in the course of treating their patients. [OTA,1993]

Breach of Security: Any action by an authorized or unauthorized user which results in a negative impact upon the data in the system or the system itself, or which causes data or services within a system to suffer unauthorized disclosure, modification, destruction, or denial of service. [CPRI, 1995c]

Caregiver: An individual who directly or indirectly provides health services, the goal of which is to heal, promote health, and improve the well being of another individual.

Certification: The administrative act of approving a system for use in a particular application. [National Research Council, 1991]

Certification authority: A trusted issuer of certification. [National Research Council, 1991]

(Public key) certificate: An agreement that binds a user's name to a public key, signed by a trusted issuer. A framework for the use of public key certificates was defined in Consultative Committee on International Telephony and Telegraphy (CCITT) standard X.509. [National Research Council, 1991] The certificate contains the user's name and public key, the certification authority's name, a serial number, and a validity period. [ASTM E1762]

Checksum: Digits or bits summed according to arbitrary rules and used to verify the integrity of data. [National Research Council, 1991]

Check digit: The resultant representation of a checksum operation. [Verhoeff, 1969]

Classification level: The security level of information. [National Security Council, 1991] *See also* sensitivity label.

Clearance Level: The security level of an individual who may access information. [National Research Council, 1991]

Clinical data/information: Data/information related to the health and health care of an individual collected from or about an individual receiving health care services. Includes a caregiver's objective measurement or subjective evaluation of a patient's physical or mental state of health; descriptions of an individual's health history and family health history; diagnostic studies; decision rationale; descriptions of procedures performed; findings; therapeutic interventions; medications prescribed; description of responses to treatment; prognostic statements; and descriptions of socio-economic and environmental factors related to the patient's health. [CPRI, 1996b; ASTM 1769]

Clinical data repository: Collection of clinical data from diverse sources to support individual practitioner inquiry in ad hoc formats, stores data longitudinally, and is designed to support monitoring and analysis of patient care outcomes. It may be a component of an institutional information warehouse and/or community and state health information system. [Abdelhak, 1996]

Computer-based patient record: The Institute of Medicine patient record study committee coined the term and defined it as "an electronic patient record that

resides in a system specifically designed to support users through availability of complete and accurate data, alerts, reminders, clinical decision support systems, links to medical knowledge, and other aids." [Dick and Steen, 1991] Electronically maintained information from all sources about an individual's lifetime health status and health care, replacing the paper medical record as the primary record of care, meeting all clinical, legal, and administrative requirements and providing added value in supporting decisions about patient management. [CPRI, 1995a; CPRI, 1996d]

Computer-based patient record system: The people, data, rules and procedures, processing and storage devices, and communication and support facilities that provide the capture, storage, processing, communication, security, and presentation of computer-based patient record information. [CPRI, 1995a]

Confidential: That which is not freely disclosed; private information that is entrusted to another with the confidence that unauthorized disclosure, which would be prejudicial to the individual, will not occur. [CPRI, 1994]

Confidentiality: The act of limiting disclosure of private matters; maintaining the trust that an individual has placed in one which has been entrusted with private matters. [CPRI, 1995b] The status accorded to data or information indicating that it is sensitive for some reason, and that therefore it needs to be protected against theft or improper use and must be disseminated only to individuals or organizations authorized to have it. [Ball and Collen, 1992; OTA, 1993]

Connectivity: The potential (of a computer-based patient record system) to establish links to or interact effectively (with another computer system). [Institute of Medicine, 1994]

Consent: The agreement of an individual for a given action relative to the individual. [Huffman, 1985] In health care, consent refers to a communication process between the caregiver and the patient, and may refer to consent for treatment, special procedures, release of information, and advanced directives (which give instructions regarding the patient's wishes in special medical situations {Patient Self-Determination Act, December 1991}). [Abdelhak, 1996]

Expressed consent: Oral or written agreement. Because it is difficult to prove that oral consent was given, most expressed consent is expected to be recorded with a signature. [Huffman, 1985]

Implied consent: An action other than an expressed consent on the part of a patient that demonstrates consent. [Huffman, 1985] For example, the presentation of a person to a caregiver implies to a certain extent consent to at least basic consent. [Abdelhak, 1996]

Informed consent: The Veteran's Administration defines that for a consent to be valid, the patient must be informed, which is "a freely given consent that follows a careful explanation by a caregiver to a patient or patient's representative of the proposed diagnostic or therapeutic procedure or course of treatment. The patient should be given the opportunity to ask questions, to indicate comprehension of the information provided, and to grant permission freely and without any coercion for performance of a procedure or course of treatment, as well as the opportunity to withhold or revoke such permission at any time without prejudice." [Huffman, 1985] Regulations promulgated by the Department of Health and Human Services for consent by human subjects in medical treatment (4 CFR Section 46.116) provides that informed consent to release of information should include the elements of disclosure, voluntariness, comprehension, and competence to consent. [OTA, 1993]

Cryptography: The art of keeping data secret, primarily through the use of mathematical or logical functions that transform intelligible data into seemingly unintelligible data and back again. [National Research Council, 1991]

Cyclic redundancy checks (CRC): A mathematical (polynomial division) means to digitally fingerprint or perform an error check on a block of data. [Prosise, 1996]

Data: A sequence of symbols to which meaning may be assigned. [National Research Council, 1991]

Data dictionary: Information describing the specifications and location of all data contained in a system. [WEDI, 1992] It provides the central resource for ensuring that standard definitions for data elements and data structures are used throughout the computer system [Abdelhak, 1996]

Data/record linkage: Bringing together two separately recorded pieces or sets of information concerning a particular individual, family, provider, facility, or other record subject. [Institute of Medicine, 1994; AHCPR, 1991]

Data Encryption Standard: The Data Encryption Standard (DES) represents the first cryptographic algorithm openly developed by the US government and has become an American National Standards Institute (ANSI) standard (number X3.92-1981/R1987). [National Research Council, 1991]

Decryption: The process of decoding a message so that its meaning becomes obvious. [OTA, 1993]

Digital signature: A means to guarantee the authenticity of a set of input data the same way a written signature verifies the authenticity of a paper document. A cryptographic transformation of data that allows a recipient of the data to prove the source and integrity of the data and protect against forgery. Specifically, an

asymmetric cryptographic technique in which each user is associated with a public key distributed to potential verifiers of the user's digital signature used to encrypt messages destined for other users, and a private key known only to the user and is used to decrypt incoming messages. To sign a document, the document and private key are input to a cryptographic process that outputs a bit string (the signature). To verify a signature, the signature, document, and user's public key are input to a cryptographic process, which returns an indication of success or failure. Any modification to the document after it is signed will cause the signature verification to fail (integrity). If the signature was computed using a private key other than the one corresponding to the public key used for verification, the verification will fail (authentication). [ASTM E1762]

Digitized signature: An electronic image of an actual written signature. A digitized signature looks much the same as the original, but it does not provide the same protection as a digital signature, as they can be forged and copied. [AHIMA, 1996a]

Disaster plan: A plan the provides direction and guidelines to protect health information from damage, minimize disruption, ensure stability, and provide for orderly recovery in the event of a disaster, such as flood, fire, etc. [AHIMA, 1996b] The Joint Commission on Accreditation of Healthcare Organizations requires that accredited facilities develop a management plan that addresses emergency preparedness. [Joint Commission, 1996]

Disaster recovery: The process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure. [CPRI, 1996c]

Disclosure: The release of information to third parties within or outside the health care provider organization from an individual's record with or without the consent of the individual to whom the record pertains. There are multitudes of internal and external users of health information for which various policies of disclosure may apply. For instance, when patients present to a health care facility or provider for treatment, it is reasonable to assume that they are authorizing the caregiver to have information about their condition and treatment. However, such assumption should not extend to all employees of a health care provider organization, but only those with a need to know. Disclosures for quality monitoring, educational purposes, research, administrative purpose, payment purposes, attorneys, law enforcement personnel and agencies, family members, and the patients themselves all must be conducted according to institutional policies. [CPRI, 1995b; CPRI, 1995c]

Electronic signature: The attribute that is affixed to an electronic document to bind it to a particular entity. An electronic signature process secures the user authentication (proof of claimed identity, such as by biometrics {fingerprints, retinal scans, handwritten signature verification, etc.}, tokens or passwords) at the time the signature is generated; creates the logical manifestation of signature (including the

possibility for multiple parties to sign a document and have the order of application recognized and proven) and supply additional information such as time stamp and signature purpose specific to that user; and ensures the integrity of the signed document to enable transportability, interoperability, independent verifiability, and continuity of signature capability. Verifying a signature on a document verifies the integrity of the document and associated attributes and verifies the identity of the signer. There are several technologies available for user authentication, including passwords, cryptography, and biometrics. [ASTM 1762]

Encryption: The process of encoding a message so that its meaning is not obvious. [OTA, 1993]

Firewall: A dedicated computer equipped with safeguards that acts as a single, more easily defined, Internet connection [Cheswick and Bellovin, 1994]

Freedom of Information Act: Requires that records pertaining to the executive branch of the federal government be available to the public except for matters that fall within exempted areas, including "medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." [U.S.C. & sect; 552]

Functional requirements: A statement of the system behavior needed to enforce a given policy. Requirements are used to derive the technical specification of a system. [National Security Council, 1991]

Gateway: A device in the computer communications environment that directs information traffic. Gateways are often employed to connect a network under the control of one organization (an internal network) to a network controlled by another organization (an external network such as a public network). Thus gateways are natural points at which to enforce access control policies. [National Research Council, 1991]

Granularity: An expression of the relative size of a unit. The smallest discrete information that can be directly retrieved. [ASTM E1769] In security, degree of protection. Protection at the file level is considered coarse granularity, whereas protection at the field level is finer granularity. Granularity at a single user is fine granularity because it means the access-control mechanism can be adjusted to include or exclude any single user. [Fites and Kratz,1993]

Hash-function: A function which maps strings of bits to fixed-length strings of bits satisfying that it is computationally infeasible to find for a given output an input which maps to this output and computationally infeasible to find for a given input a second input which maps to the same output. [ASTM E1762]

One-way hash function: A (mathematical) function that is comparatively easy to compute but, when knowing a result, it is computationally infeasible to find any of the values that may have been supplied to obtain it. [ASTM E1762]

Health care data/information: *See clinical data/information*

Identification: Refers to less formal methods of establishing the authorized nature of a communications partner, which are usually manual, involve human interaction, and do not use the Internet data channel itself, but another "out-of-band" path such as the telephone or US mail. [HCFA, 1998]

Information: Data to which meaning is assigned, according to context and assumed conventions. [National Security Council, 1991]

Integrity: The property or state of being whole or unimpaired. Data integrity refers to the accuracy and completeness of the data. [Ball and Collen, 1992] Program integrity, system integrity, and network integrity are all relevant to consideration of computer and system security. [National Research Council, 1991]

Key: An input that controls the transformation of data by an encryption algorithm. [National Research Council, 1991]

Longitudinal/lifetime patient record: The concept of access to health information across an individual's lifetime. [Dick and Steen, 1991] A permanent, coordinated record of significant information, in chronological sequence. It may include all historical data collected or be retrieved as a user-designated synopsis of significant demographic, genetic, clinical, and environmental facts and events maintained within an automated system. [ASTM E1384]

Master patient index: An index of patients, persons, members of health care plans, guarantors, physicians, health care practitioners, payers, employees, employers or others. It may also be called an enterprise master patient index (EMPI), enterprise patient index (EPI), corporate person index (CPI), or other similar description. [AHIMA, 1997a] The means for locating a patient record in a numeric identification system. [Abdelhak, 1996] It has generally referred to an index within a given health care facility, in which case it serves as a patient directory. [CPRI, 1996a]

Non-repudiation: Proof (to a third party) that only the signer could have created a signature. A basis of legal recognition of electronic signatures. [ASTM E1762]

Open systems architecture: Use of standardized technology and structures for hardware, operating system, data bases, fault tolerances, and networking and communications transport. [ASTM E1769]

Orange Book: Common name for the Department of Defense document that is the basic definition of the Trusted Computer System Evaluation Criteria (US DOD, 1985d). The Orange Book provides criteria for the evaluation of different classes of trusted systems and is supplemented by many documents relating to its extension and interpretation. [National Research Council, 1991]

Ownership: It is a generally accepted principle that the primary patient record is maintained and owned by the health care provider. This principle is established by statutes and licensing regulations in many states, which grant the provider control over the physical document, but give the patient ownership-type rights to the information contained in the record. Therefore, the patient generally has control over the release of patient-identifiable (confidential) information, except in circumstances identified by case law, by federal or state statutes and regulations, and by provider policy. [CPRI, 1994]

Password: A sequence that an individual presents to a system for purposes of authentication. [National Research Council, 1991]

Personally identifiable health information: Health information that contains an individual's identifiers (e.g., name, social security number, and birth date) or contains a sufficient number of variables to allow identification of an individual. [OTA, 1993, Institute of Medicine, 1994]

PIN: Personal identification number. Typically used in connection with automated teller machines to authenticate a user. [National Research Council, 1991]

PKI: *See Public Key Infrastructure*

Primary patient record (primary record of care): The primary legal record documenting the health care services provided to a person in any aspect of health care delivery. This term is synonymous with medical record, health record, primary patient record, client record, and resident record; when stored in a computer system and used by caregivers while providing patient care services to review patient data, receive decision support, and document their own observations, actions, or instructions, it is synonymous with all terms associated with computer-based patient record. [ASTM E1384; CPRI, 1996d]

Privilege: The individual's right to hold private and confidential the information given to a health care provider in the context of a professional relationship. The individual may by overt act of consent or by other means waive the right to privilege. For example, if a patient brings a lawsuit against a facility and the records are needed to present the facility's case, the privilege is waived. [Fites and Kratz, 1993]

Privacy: The right of individuals to keep information about themselves from being disclosed to anyone. [CPRI, 1995c] As set forth by Samuel Warren and Louis

Brandeis in a 1890 article that first enunciated the concept of privacy as a legal interest deserving an independent remedy, privacy was described as "the right to be let alone." Further, Alan Westin conceived of privacy as "an instrument for achieving individual goals of self realization." [OTA, 1993] Ball and Collen describe privacy as the right of an individual to be left alone, to withdraw from the influence of the environment; to be secluded, not annoyed, and not intruded upon by extension of the right to be protected against physical or psychological invasion or against the misuse or abuse of something legally owned by an individual or normally considered by society to be property. [Ball and Collen, 1992]

Privacy Act of 1974: Grants people certain rights to information collected about them by the federal government and its agencies. Rights include finding out what information has been collected, to see and have a copy of the information, to correct or amend the information, and to exercise limited control of the disclosure of that information to other parties. [U.S.C. sect; 552a(b), 1977]

Private key: A key in an asymmetric algorithm; the possession of this key is restricted, usually to one entity. [ASTM E1762]

Public key: A key in an asymmetric algorithm that is publicly available. [ASTM E1762]

Public Key Infrastructure (**PKI**): PKIs are designed to solve the key management process problems that deal with creation, distribution, authentication and storage of keys. [RSA 1999]

Redisclosure: The disclosure by a third party recipient of disclosed health information without the authorization of the patient. [Abdelhak, 1996]

Release of Information: The disclosure of documents containing patient-identifiable information to a third party requestor. [Huffman, 1985]

Reliability: A measure of consistency of data items based on their reproducibility and an estimation of their error of measurement. [Institute of Medicine, 1994]

Repudiation: Denial by one of the entities involved in a communication of having participated in all or part of the communication.[ASTM 1762]

Retention: The maintenance and preservation of information in some form (e.g., paper, microfilm, or electronic storage) for a given period of time. [Abdelhak, 1996] There are no federal laws outlining time frames for the retention of health information. Many states, however, have specific requirements, and these, as well as the statutes of limitation, Medicare Conditions of Participation, and use for patient care, legal, research, or educational purposes, should be used as a basis for developing a retention policy. [AHIMA, 1994]

RSA: A public key crypto-system, invented and patented by Ronald Rivest, Adi Shamir, and Leonard Adelman, based on large prime numbers. [National Security Council] RSA is the most well-known asymmetric algorithm. [ASTM E1762]

Safety: The property that a system will satisfy certain criteria related to the preservation of personal and collective freedom from risk. [National Research Council, 1991]

Secondary record: A record that is derived from the primary record and contains selected data elements. [ASTM E1384]

Secrecy: The intentional concealment or withholding of information [OTA, 1993]

Secret key: A key in a symmetric algorithm; the possession of this key is restricted, usually to two entities. [ASTM E1762]

Secure Sockets Layer (SSL): An Internet security handshake protocol that provides data security and integrity through data encryption, server authentication, message integrity, and optional client authentication between HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol) and Telnet protocols and the TCP/IP connection. Utilizes the RSA public key cryptosystem. (*See RSA above*.) [RSA 1999]

Security: Means to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss. [CPRI, 1995b]Protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. [National Security Council]

Data/information security: The result of effective protection measures that safeguard data/information from undesired occurrences and exposure to accidental or intentional disclosure to unauthorized persons, accidental or malicious alteration, unauthorized copying, loss by theft and/or destruction by hardware failures, software efficiencies, operating mistakes, or physical damage by fire, water, smoke, excessive temperature, electrical failure, or sabotage. [Institute of Medicine, 1994] The protection of the integrity, availability, and confidentiality of computer-based information and resources used to enter, store, process, and communicate it. [NIST, 1994]

Security education program: The systematic, defined method to provide information and to teach skills related to all activities of the organization related to information security. A complete information security education program addresses policies, standards, training, controls, risk assessment, auditing and monitoring, and assigned responsibility for management of the program. [CPRI, 1995c]

Security manager: The person assigned responsibility for management of the organization's security program. [CPRI, 1996c]

Security policy: The framework within which an organization establishes needed levels of information security to achieve the desired confidentiality goals. A policy is a statement of information values, protection responsibilities, and organization commitment for a system. It is a set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. [OTA, 1993] The American Health Information Management Association recommends that security policies apply to all employees, medical staff members, volunteers, students, faculty, independent contractors, and agents. [AHIMA, 1996c]

System security: The result of all safeguards including hardware, software, personnel policies, information practice policies, disaster preparedness, and oversight of these components. [Institute of Medicine, 1994]

System security administrator: The person who controls access to computer systems by entering commands to perform such functions as assigning user access codes and privileges, revoking user access privileges, and setting file protection parameters. [CPRI, 1996c]

Sensitivity label: A security level associated with the content of the information. [National Security Council] Society has historically considered information that has a heightened potential for causing harm to the patient or data subject, or to others, such as the subject's spouse, children, friends, or sexual partners. The degree to which the information will cause public humiliation, stigmatization, lost employment, insurance problems, or loss of family and friends all contributes to it being identified as "sensitive." Records that contain information about socially or politically prominent persons have also been accorded special protections. Society is beginning to attribute special sensitivity to any and all health information. [Kunitz and Associates, Inc., 1995]

Secure/Multipurpose Internet Mail Extensions (S/MIME): A protocol that adds digital signatures and encryption to Internet MIME messages, a standard format for extended Internet e-mail. [RSA 1999]

Technical specification: A technical description of the desired behavior of a system, as derived from its requirements. A specification is used to develop and test an implementation of a system. [National Research Council, 1991]

Threat: The potential for exploitation of a vulnerability. [National Research Council, 1991]

Timestamp: A computer system-generated indication of time and action, such as access, documentation, signature, etc., occurred. [CPRI 1996e]

Token: When used in the context of authentication, a physical device necessary for user identification. [National Research Council, 1991] Smart cards are a form of token.

Transaction Layer Security (TLS): Internet security protocol being developed by merging Secure Sockets Layer (SSL) with other protocols and authentication methods.

Transmission: The exchange of data between person and program, or program and program, when the sender and receiver are remote from each other. [Longley, 1987]

Trusted system: A system believed to enforce a given set of attributes to a stated degree of assurance (confidence). [National Research Council, 1991]

Trusted Third Party: An entity that issues certificates. It uses cryptographic mechanisms to ensure that the authenticity and integrity of the evidence that it stores can be verified during any dispute resolution process. [ASTM E1762, 1995]

Universal identifier: A means to provide positive recognition of a particular individual for all people in a population. A universal health care or patient identifier provides the identifier for use in health care transactions. [ASTM E1714]

Validity: The extent to which data correspond to the actual state of affairs or an instrument that measures what it purports to measure. Validity concerns relate to the issue of whether analyses done on a given database are appropriate for the questions being asked and whether those analyses will provide defensible answers that are internally consistent and externally generalizable. [Institute of Medicine, 1994]

Virus: A computer program, typically hidden, that attaches itself to other programs and has the ability to replicate. In personal computers, "viruses" are generally Trojan horse programs that are replicated by inadvertent human action and which when executed result in undesired side effects generally unanticipated by the user.

Vulnerability: A weakness in a system that can be exploited to violate the system's intended behavior. There may be security, integrity, availability, and other vulnerabilities. The act of exploiting a vulnerability represents a threat, which has an associated risk of being exploited. [National Research Council, 1991]

Online References

The following Web sites are excellent resources for authoritative and up-to-date information on technological terms. These Web sites contain encyclopedias, search

engines, frequently asked questions (FAQs), and entire areas dedicated to security technology.

Netscape: Developed the Internet security SSL protocol among others. URL: http://home.netscape.com/products/security/

PC Web: An online encyclopedia and search engine dedicated to computer technology. URL: http://www.pcwebopedia.com

RSA Data Security: A leading developer of cryptosystems in use today. URL: www.rsa.com

Tech Encyclopedia: A technology newsite with an online encyclopedia of over 11,000 definitions of computer terms and concepts.URL: www.techweb.com/encyclopedia/

Whatis?.com: An online encyclopedia of technology terms relating to computers, networks, the Internet or the Web. URL: www.whatis.com

References

Abdelhak M (Ed.), 1996 Health Information: Management of a Strategic Resource. Philadelphia: W.B. Saunders Company.

AHA, 1993. Toward a National Health Information Infrastructure: Report of the Work Group on Computerization of Patient Records to the Secretary of the U.S. Department of Health and Human Services. AHA Work Group on Computerization of Patient Records. Chicago: American Hospital Association, April.

AHCPR, 1991. Report to Congress: The Feasibility of Linking Research-Related Data Bases to Federal and Non- Federal Medical Administrative Data Bases. Agency for Health Care Policy and Research Pub. No. 91-0003. Rockville: MD: AHCPR, PHS, U.S. DHHS, April.

AHIMA, 1994a. Guidelines on Maintenance, Disclosure, and Redisclosure of Health Information. Chicago: American Health Information Management Association.

AHIMA, 1994b. Retention of Health Information. Chicago: American Health Information Management Association, March.

AHIMA, 1996a. Electronic Signatures. Chicago: American Health Information Management Association, March.

AHIMA, 1996b. Disaster Planning for Health Information. Chicago: American Health Information Management Association, April.

AHIMA, 1996c. Information Security – An Overview. Chicago: American Health Information Management Association, June.

AHIMA, 1997a. Practice Brief Issue: Maintenance of Master Patient (Person) Index (MPI)--Single Site or Enterprise. Chicago: American Health Information Management Association, October.

ASTM E1384. Standard Guide for Description for Content and Structure of the Computer-Based patient Record. ASTM Committee E-31 on Computerized Systems, Subcommittee E31.19 on Vocabulary for Computer-Based Patient Records Content and Structure. West Conshohocken, PA: ASTM, Jan. 10, 1996.

ASTM E1714. Guide for the Properties of a Universal Healthcare Identifier. Committee E-31 on Computerized Systems, Subcommittee E31.12 on Medical Records. West Conshohocken, PA: ASTM, Aug. 15, 1995.

ASTM 1762. Guide for Electronic Authentication of Health Care Information. Committee E-31 on Computerized Systems, Subcommittee E31.20 on Authentication. West Conshohocken, PA: ASTM, Oct. 10, 1995.

ASTM E1769. Guide for Properties of Electronic Health Records and Record Systems. Committee E-31 on Computerized Systems, Subcommittee E31.12 on Medical Records. West Conshohocken, PA: ASTM, Dec. 10, 1995.

Amatayakul M, 1996. Privacy protections afforded by computer-based patient record systems. Topics in Health Information Management. Gaithersburg, MD: Aspen Publishers, Inc., 16(4), May.

Ball MJ, Collen MF, 1992 (Eds.). Aspects of the Computer-based Patient Record. New York: Springer-Verlag.

Cheswick WR, Bellovin SM, 1994 Firewalls and Internet Security. Reading, MA: Addison-Wesley.

CPRI, 1996a. Action Plan for Implementing a Universal Patient Identifier, Draft Version 1.0. Schaumburg, IL: Computer-based Patient Record Institute, May.

CPRI, 1996b. Computer-based Patient Record Description of Content. Work Group on CPR Description, Schaumburg, IL: Computer-based Patient Record Institute, April.

CPRI, 1996c. Guidelines for Managing Information Security Programs at Organizations

Using Computer-based Patient Records. Work Group on Confidentiality, Privacy and Security, Schaumburg, IL: Computer-based Patient Record Institute, January.

CPRI, 1996d. CPR Project Evaluation Criteria, Version 2.1. Work Group on CPR Systems Evaluation, Schaumburg, IL: Computer-based Patient Record Institute, March.

CPRI, 1996e. Guidelines for Electronic Signature Policies at Organizations Using Computer-based Patient Record Systems

CPRI, 1995a. Description of the Computer-based Patient Record and Computer-based Patient Record System. Work Group on CPR Description, High Level Description Project Team, Ver. 1.0. Schaumburg, IL: Computer- based Patient Record Institute, April.

CPRI, 1995b. Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Records. Work Group on Confidentiality, Privacy and Security, Schaumburg, IL: Computer-based Patient Record Institute, February.

CPRI, 1995c. Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Records. Work Group on Confidentiality, Privacy and Security, Schaumburg, IL: Computer-based Patient Record Institute, June.

CPRI, 1994. Position Paper: Access to Patient Data. Schaumburg, IL: Computer-based Patient Record Institute, April.

Dick RS, Steen EB (Eds.), 1991. The Computer-based Patient Record: An Essential Technology for Health Care. Washington, DC: National Academy Press.

Fites PE, Kratz MPJ, 1993. Information Systems Security: A Practitioner's Reference. New York: Van Nostrand Reinhold.

Harris-Equifax, 1993. Health Information Privacy Survey 1993. Louis Harris and Associates for Equifax. Atlanta: Equifax Inc.

HCFA, 1998. HCFA Internet Security Policy. Published November 24, 1998.

Huffman EK, 1985. Medical Record Management. Berwyn, IL: Physicians' Record Company.

Institute of Medicine, 1994. Health Data in the Information Age: Use, Disclosure, and Privacy. MD Donaldson and KN Lohr (Eds). Washington, DC: National Academy Press.

ISO 7498-2. Information Processing Systems – Open Systems Interconnection– Basic Reference Model – Part 2: Security Architecture. International Standards Organization, 1989.

Joint Commission, 1996. Accreditation Manual for Hospitals, Volume 1, Standards. Oakbrook Terrace, IL: Joint Commission on Accreditation of Healthcare Organizations.

Kunitz and Associates, Inc., 1995. Final Report of the Task Force on the Privacy of Private-Sector Health Records. Contract HHS-100-91-0036. Rockville, MD: KAI, September.

Longley, D. Data & Computer Security: Dictionary of Standards, Concepts, and Terms. UK:

MacMillan. MTR-8201. Trusted Computer Systems – Glossary. Technical Report, The Mitre Corporation, Mar. 1987.

National Research Council, 1991. Computers at Risk: Safe Computing in the Information Age. System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications. Washington, DC: National Academy Press.

NIST, 1994. An Introduction to Computer Security: The NIST Handbook. Washington, DC: National Institute of Standards and Technology.

OTA, 1993. Protecting Privacy in Computerized Medical Information. Office of Technology Assessment, OTA- TCT-576. Washington, DC: U.S. Government Printing Office, September.

Prosise J, 1996. Digital signatures: how they work. PC Magazine. April 9.

RSA Data Security, 1999. Website www.rsa.com

Tuttle, M, 1994. Bringing knowledge to the point of care, Handout at ANSI HISPP Meeting, January 20. USC §552a(b), 1977

Verhoeff J, 1969. Error detecting decimal codes. Mathematical Centre Tract 29. Amsterdam: The Mathematical Center.

WEDI, 1992. Workgroup for Electronic Data Interchange Report, Cambridge, MA: Work Group for Electronic Data Interchange.

CPRI's Home Page URL www.cpri.org
Computer-based Patient Record Institute
4915 St. Elmo Avenue, Suite 401
Bethesda, MD 20814
Tel: 301-657-5918, Fax: 301-657-1296

Toolkit Section 9.0

Chapter Nine

BIBLIOGRAPHY

ABA, *Digital Signature Guidelines.*

Abdelhak M (Ed.), 1996 *Health Information: Management of a Strategic Resource.* Philadelphia: W. B. Saunders Company.

AHA, 1993. *Toward a National Health Information Infrastructure: Report of the Work Group on Computerization of Patient Records to the Secretary of the US Department of Health and Human Services.* AHA Work Group on Computerization of Patient Records. Chicago: American Hospital Association, April.

Alexander M. *Net Security: Your Digital Doberman.* Research triangle park, North Carolina: Ventana Communications Group. 1997.

Alexander M. The Real Security Threat: The Enemy Within. *Datamation* (July 15, 1995: 30-33).

AHCPR, 199 1. *Report to Congress: The Feasibility of Linking Research-Related Data Bases to Federal and Non-Federal Medical Administrative Data Bases.* Agency for Health Care Policy and Research Pub. No. 91-0003. Rockville: MD: AHCPR, PHS, U.S. DHHS, April.

AHIMA, 1994a. *Guidelines on Maintenance, Disclosure, and Redisclosure of Health Information.* Chicago: American Health Information Management Association.

AHIMA, 1994b. *Retention of Health Information.* Chicago: American Health Information Management Association, March.

AHIMA, 1996a. *Electronic Signatures.* Chicago: American Health Information Management Association, March.

AHIMA, 1996b. *Disaster Planning for Health Information.* Chicago: American Health Information Management Association, April.

AHIMA, 1996c. *Information Security - An Overview.* Chicago: American Health Information Management Association, June.

ANSI, ASC X12.58, Security Structures, June, 1997.

ASTM E 1384. *Standard Guide for Description for Content and Structure of the Computer-Based Patient Record.* ASTM Committee E31.19 on Computerized Systems,

Subcommittee E31.19 on Vocabulary for Computer-Based Patient Records Content and Structure. West Conshohocken, PA: ASITM, Jan, 10, 1996.

ASTM E 1714. *Guide for the Properties of a Universal Healthcare Identifier.* Committee E-31 on Computerized Systems, Subcommittee E31.12 on Medical Records. West Conshohocken, PA: ASTM, Aug. 15, 1995.

ASTM 1762. *Guide for Electronic Authentication of Health Care Information.* Committee E-31 on Computerized Systems, Subcommittee E31.20 on Authentication, West Conshohocken, PA: ASTM, Oct. 10, 1995.

ASTM E 1769. *Guide for Properties of Electronic Health Records and Record Systems.* Committee E-31 on Computerized Systems, Subcommittee E31.12 on Medical Records. West Conshohocken, PA: ASTM, Dec. 10, 1995.

ASTM, *A Security Framework for Healthcare Information,* ASTM Committee E-31 on Computerized Systems, Subcommittee E31.20 on Authentication. West Conshohocken, PA, February 11, 1997.

Amatayakul M, 1996. Privacy protections afforded by computer-based patient record systems. Topics *in Health Information Management,* Gaithersburg, MD: Aspen Publishers, Inc., 16(4), May.

Ball MJ, Collen MF, 1992 (Eds.). *Aspects of the Computer-based Patient Record.* New York: Springer-Verlag.

Brandt M. Information Security: How Safe is Your System? *Healthcare Informatics* 12, No. 10 (October 1996): 24-32.

Brandt M, Practice Brief: Electronic Signatures. *Journal of the American Health Information Management Association.* 67, No. 3 (March 1996).

Cheswick WR, Bellovin SM, 1994 *Firewalls and Internet Security.* Reading, MA: Addison-Wesley

CPRI, 1996a. *Action Plan for Implementing a Universal Patient Identifier*. Draft Version 1.0. Schaumburg, IL Computer-based Patient Record Institute, May.

CPRI, 1996b. *Computer-based Patient Record Description of Content.* Work Group on CPR Description, Schaumburg, IL: Computer-based Patient Record Institute, April.

CPRI, 1996c. *Guidelines for Managing Information Security Programs at Organizations Using Computer-based Patient Records.* Work Group on Confidentiality, Privacy & Security, Schaumburg, IL: Computer-based Patient Record Institute, January.

CPRI, 1996d. CPR *Project Evaluation Criteria*, Version 2. 1. Work Group on CPR Systems Evaluation, Schaumburg, IL: Computer-based Patient Record Institute, March.

CPRI, 1995 a, *Description of the Computer-based Patient Record and Computer-based Patient Record System.* Work Group on CPR Description, High Level Description Project Team, Ver. 1. 0. Schaumburg, IL: Computer-based Patient Record Institute, April.

CPRI, 1995b. *Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Records.* Work Group on Confidentiality, Privacy & Security, Schaumburg, IL: Computer-based Patient Record Institute, February.

CPRI, 1995c. *Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Records.* Work Group on Confidentiality, Privacy & Security, Schaumburg, IL: Computer-based Patient Record Institute, June.

CPRI, 1994. *Position Paper: Access to Patient Data.* Schaumburg, IL: Computer-based Patient Record Institute, April.

Dennis JC, When the Worst Happens (Handling Security Breaches). *In Confidence* 3, No. 6 (November/December 1996): 3.

:

Dick RS, Steen EB (Eds.), 1991. *The Computer-based Patient Record: An Essential Technology for Health Care.* Washington, DC: National Academy Press.

Donaldson MS, Lohr KN (Eds.), *Health Data in the Information Age: Use, Disclosure, and Privacy.* Washington, DC: National Academy Press, 1994.

Endrijonas J, *Data Security.* Rocklin, CA: Prima Publishing, 1995.

Fites PE, Kratz MPJ, 1993. *Information Systems Security: A Practitioner's Reference.* New York: Van Nostrand Reinhold.

Goldman J, Mulligan D. *Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality.* Center for Democratic Technology, 1996.

Griecser G, (1989). Data protection in hospital information systems: 1. Definition and overview. *Implementing Health-care Information Systems.* New York: Springer-Verlag.

Hannah KJ, Ball MJ, Edwards MJA (Eds), (1994). *Computers in Health Care: Introduction to Nursing Informatics.* New York: Springer-Verlag.

Harris-Equifax, 1993. *Health Information Privacy Survey 1993.* Louis Harris and Associates for Equifax. Atlanta: Equifax Inc.

Huffman EK, 1985. *Medical Record Management.* Berwyn, IL: Physicians' Record Company.

Hughes G, Practice Brief: Disaster Planning for Health Information. *Journal of the American Health Information Management Association.* 67, No. 4 (April 1996).

Institute of Medicine, 1994. *Health Data in the Information Age: Use, Disclosure, and Privacy.* MD Donaldson and KN Lohr (Eds). Washington, DC: National Academy Press.

ISO 7498-2, *Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.* International Standards Organization, 1989.

Joint Commission, 1996. *Accreditation Manual for Hospitals, Volume 1, Standards.* Oakbrook Terrace, IL: Joint Commission on Accreditation of Healthcare Organizations.

Kelly KJ, (1992). *Nursing Staff Development: Current Competence, Future Focus.* Philadelphia: J.B. Lippincott Company.

Kunitz and Associates, Inc., 1995. *Final Report of the Task Force on the Privacy of Private-Sector Health Records.* Contract HHS-100-91-0036. Rockville, MD: KAI, September.

Longley D, *Data & Computer Security: Dictionary of Standards, Concepts, and Terms. UK:* MacMillan. MTR-820 1. *Trusted Computer Systems - Glossary.* Technical Report, The Mitre Corporation, March 1987.

Louis Harris and Associates, *Harris-Equifax: Health Information Privacy Survey 1993.* New York: Louis Harris and Associates, 1993.

Louis Harris and Associates, *Equifax-Harris: Consumer Privacy Survey 1994.* New York: Louis Harris and Associates, 1994.

MacMillan, MTR-8201. *Trusted Computer Systems-Glossary*. Technical Report, the Mitre Corporation, 1987.

Madsen W, (1992). Handbook of Personal Data Protection. New York: MacMillan Publishers.

Marcells AJ, Chan S. *EDI Security, Control and Audit.* Norwood, MA: Artech House, 1993.

Menning WR, Trussel RG, *Protecting the Security and Confidentiality of Healthcare Information. The Journal of the Healthcare Information and Management Systems Society* 12, No. 1 (Spring 1998).

Miller D, Can Confidential Clinical Information Be Protected on the Internet? *Clinical Data Management* 2, No. 12 (March 1996): 1-3.

Miller D, Securing the Client/Server Environment. *In Confidence* 3, No. 1 (January/February 1995): 6-8.

Miller D, Using Encryption to Protect Health Information. *In Confidence* 3, No. 6 (November/December 1995): 7-8

National Research Council, *For the Record: Protecting Electronic Health Information*. Washington, DC: National Academy Press, 1997.

National Research Council, 199 1. *Computers at Risk Safe Computing in the Information Age.* System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications. Washington, DC: National Academy Press.

NIST, 1994. *An Introduction to Computer Security: The NIST Handbook.* Washington, DC: National Institute of Standards and Technology.

OTA, 1993. *Protecting Privacy in Computerized Medical Information.* Office of Technology Assessment, OTA-TCT-576. Washington, DC: U.S. Government Printing Office, September.

Pfleeger CP, *Security in Computing.* 2nd Edition. Uppler Saddle River, NJ: Prentice Hall 1997.

Prosise J, 1996. Digital signatures: how they work. *PC Magazine.* April 9.

Romano CA, (1987). Privacy, confidentiality, and security of computerized systems: The Nursing responsibility. *Computers in Nursing*, 5(3): 99-104.

Schechter KS, (1988). Conversion issues and data integrity: A consultant's perspective. *Topics in Health Record Management.*_-Q(2): 62-69.

Schou CD, *Glossary of INFOSEC and INFOSEC Related Terms, Version 6.* Center for Decision Support, Idaho State University. 1996.

Schraffenberger LA, (1988). Practice bulletin, data security. JAMRA , 59.(8): 46-47.

Shaffer SL, Simon AR, (1994). *Network Security:* Boston: AP Professional.

Siwicki B, Enterprise Networks, Strategies for Integrated Delivery Systems. *Health Data Management* 5, No. 2. February 1997): 54-66.

Swanson M, Guttman B, Generally Accepted Principles and Practices for Securing Information Systems. NIST Pub 800-14. September 1996. PGP, Inc. Cryptology Reference Chart, August 1997.

System Security Study Committee, National Research Council. *Computers at Risk: Safe Computing in the Information Age.* Washington, DC: National Academy Press, 1991.

Tuttle M, 1994. Bringing knowledge to the point of care, Handout at ANSI HISPP Meeting, January 20. USC §552a(b), 1977.

U.S. Congress, Office of Technology Assessment. *Protecting Privacy in Computerized Medical Information.* OTA-TCT-576. Washington, DC: Government Printing Office, September 1993.

Verhoeff J, 1969. Error detecting decimal codes. *Mathematical Centre Tract 29.* Amsterdam: The Mathematical Center.

Waller A, The Electronic Chart: Keeping It Confidential and Secure. *Journal of the American Health Information Management Association* 64, No.11 (November 1993); 72-77.

Waters K, Murphy G, (1982). *System Analysis and Computer Applications in Health Information Management.* Silver Spring, MD: Aspen Systems.

WEDI, 1992. *Workgroup for Electronic Data Interchange Report,* Cambridge, MA: Work Group for Electronic Data Interchange.

Westin A, (1976). *Computer Health Records and Citizen Rights*. National Bureau of Standards, Monograph 157. Gaithersburg, MD: National Bureau of Standards, 348.