Managing Information Privacy & Security in Healthcare

CPRI Guidelines - Information Security Policies

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

By Ted Cooper, MD

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 following is the first in the series:

- *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 healthcare organizations and throughout the entire healthcare delivery system, each organization entrusted with healthcare information must establish formal information security programs. The first component of an information security program is information security policies that 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 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

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 healthcare organization and throughout the entire healthcare delivery system, formal information security programs must be established by each organization entrusted with healthcare 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 healthcare, people entrust healthcare 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 it. Every organization that creates, uses, stores, and communicates healthcare 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, employees, and other caregivers. These obligations and responsibilities to protect information must be considered and fulfilled when implementing computer-based patient records.

Public policy, laws, accrediting and regulatory requirements, and patient expectations require a certain standard for information security. However, the organization's unique mission, culture, and management significantly influence the policies a specific healthcare organization develops to protect the confidentiality, integrity, and availability of patient and administrative information.

Comprehensive information security policies form the foundation for a successful information security program. These policies should define the organization's philosophy anddirection for the protection of information. They must be documented and promulgated throughout the entire organization.

While the majority of the information maintained by healthcare 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 information complying with confidentiality and privacy requirements established by applicable state and federal laws, the Joint Commission on Accreditation of Healthcare Organizations, and regulatory agencies.

Promote consistent protection of information throughout the entire healthcare delivery system.

- Communicate the responsibilities for the protection of information and foster information security awareness.

- Foster good business practices related to protecting healthcare information.

- Provide the basis for information security standards and procedures and standards for the management, storage, and distribution of healthcare information.

Scope

This document is designed to be used primarily in establishing information security policies at all types of organizations that implement and use computer-based patient records. While it may be helpful in specifying security controls, features, and functions, the primary intent of this document is for use in defining 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, healthcare networks, home health agencies, healthcare 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 healthcare 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 that 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 systems that are 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 healthcare information
- Federal regulatory requirements
- Joint Commission on Accreditation of Healthcare 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 organization’s information should formally acknowledge an understanding of the policies and make a formal written commitment to comply with them 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 Healthcare 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 healthcare 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 it. 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. The organization should develop policies related to making information from the computer-based patient record available to the patient in a clear, logical, understandable format. Any policies for presenting

information in a format not maintained by the organization should be defined. The organization'spolicies 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 patient's rights 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 organization's rights to identify and explain any consequences of such blockage should also be included.

- Right to notification of disclosure of information. The patient'srights 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, or agents of the organization, applicable good business practices and laws pertaining to employee records and contracts should be considered in addition to the requirements for protecting health information. Areas for consideration include:

- Privacy. The caregivers' personal privacyshould 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 them 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.

- Addition of corrected information. The caregivers' rightsto 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

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

The organization's 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, civil litigation, and administrative proceedings should be defined. The policies should state how the institution will resolve conflicts among 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 collecting and authenticating information. The policy should specify who is responsible for determining which information is to be collected and retained.

Responsibilities for reviewing information collection policies and retention periods should be specified, as should responsibilities and provisions for verifying the accuracy of information.

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. These policies should include the responsibilities for destruction of information.

Information Security Program

Every organization should, as a matter of policy, maintain a formal information security program. The policy document should describe the responsibility for management and functions of the program and specify responsibilities for the periodic review and maintenance of the information security policies.

Accountability and Responsibilities

The policies should define specific responsibilities and accountability for information security. 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 appropriate caregivers, vendors, contractors, and temporary employees.
- Responsibility for reporting 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 patient 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 organization's 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 related to access to information, and for actually resolving them, 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

- Information that may be made public.
- Information internal to the organization that 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 organization's policy 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 organization's requirement for developing and maintaining business resumption plans to ensure that the healthcare 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 organization's information security standards. Policies for documenting attendance at training sessions should be established.

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

- 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 organization's legal counsel for review.
- Submit the draft policies to the organization's management 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, *The Computer-based Patient Record: An Essential Technology for Healthcare.* 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 clarify their usage in this document.

Access to Information -The ability to store, retrieve, or use 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 are 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 who has been entrusted with private matters.

Information Security -The process of safeguarding information; generally refers not only to safeguarding confidentiality but also 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 that collects, stores, transmits, or otherwise processes healthcare information.

Patient Information -Refers to data collected about or related to the health status and healthcare 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.