Managing Information Privacy & Security in Healthcare

Organizing Privacy and Security Training

By the CPRI Security Workgroup

Introduction
When healthcare 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 healthcare organizations to inform staff about universal precautions in handling blood borne pathogens represents a good model to follow in security training. Healthcare organizations either purchase or prepare standard educational programs in universal precautions that occur regularly and that all staff must attend. Like universal precautions themselves, education in universal precautions comprises part of any hospital’s annual schedule of continuing medical education. Healthcare organizations should adopt the same approach to educating staff about issues in managing the privacy and security and confidentiality of patient information. HIMSS Privacy and Security Toolkit Workgroup has prepared the following information that outlines an approach to information privacy and security education.

Information Security Education

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 Computer-based Patient Record

The remaining guidelines will address:

- Information Security Education Programs at Organizations Using Systems
- 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 healthcare organizations and throughout the healthcare delivery system, formal information security programs must be established by each organization entrusted with healthcare 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
- Objectives
- Scope
- System security Issues
- Social context
- Technical context
- Legal-regulatory context

Goals and objectives
Involved individuals having access to health information
Management
Patients and general public
Content
Suggested content for all involved individuals
Management
Patients and clients, and general public
Methodologies
Instructional technologies and strategies
Sources of delivery
Methods of program implementation
Strategies for developing training and education programs
Training and education programs categories
Evaluation
Evaluation of teaching and learning
Evaluation methodologies
Evaluation of education effectiveness
Examples of methodologies

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 re-examine 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 healthcare 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 protecting 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, in-service 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 also may 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 how information is vulnerable.
7. Identify actions that can be taken to protect information security.
8. Communicate the consequences of system security breaches to involved individuals in regard to meeting healthcare 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 in regard to meeting healthcare 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 healthcare 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 confidentiality statements
   
   4. Regular scheduled in-services
   
   5. Definitions of levels information security
6. Need-to-know basis

7. Backing up data

8. Audit trails

8. Consequences and sanctions of security breaches to the involved individual, the organization, patients, and to achieving healthcare 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 in-services; 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)
   
k. 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 also 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 used 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 healthcare 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, the 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 the 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 in-services 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 the number of violations before training 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.

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.

Confidentiality. "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 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.** 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**


