Designation: E 1988 – 98

An American National Standard

Standard Guide for Training of Persons who have Access to Health Information[1]

This standard is issued under the fixed designation E 1988; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide addresses the privacy, confidentiality, and security training of employees, agents and contractors who have access to health information. This access shall be authorized and required to meet job responsibilities. Training is essential to developing an understanding about, and sensitivity for, individually identifiable health information. Anyone in a setting that collects, maintains, transmits, stores or uses health information, or provides health services, or a combination thereof, shall provide privacy, confidentiality, and security awareness training to all staff and business partners. Training shall be based on job responsibilities.

1.2 This guide applies to all individuals, groups, organizations, data-users, data-managers, and public and private firms, companies, agencies, departments, bureaus, service-providers and similar entities that collect individual, group and organizational data related to health care. Any organization which handles or stores individually identifiable health information has the obligation to educate eemployees, agents, contractors, and volunteers and others with whom they have business relationships regarding the privacy, confidentiality, and security principles and policies and procedures of the organization.

1.3 ASTM Committee E-31 gratefully acknowledges the contribution of the Computer-Based Patient Record Institute (CPRI) in providing the document, *Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Records*, to serve as the basis of this guide.

2. Referenced Documents

2.1 *ASTM Standards:*

E 1869 Guide for Confidentiality, Privacy, Access and Data Security Principles for Health Information Including Computer Based Patient Records[2]

2.2 *CPRI Guidelines:*

Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Records June, 1995[3]

3. Terminology

3.1 *Definitions:*

3.1.1 *access*, *n*—The provision of an opportunity to approach, inspect, review, retrieve, store, communicate with, or make use of health information system resources (for example, hardware, software, systems, or structure) or patient identifiable data and information, or both. **E 1869**

3.1.2 *confidential*, *adj*—status accorded to data or information indicating that it is sensitive for some reason, and therefore it needs to be protected against theft, disclosure, or improper use, or both, and must be disseminated only to authorized individuals or organizations with a need to know. **E 1869**

3.1.3 *disclosure*, *n*—to access, release, transfer, or otherwise divulge health information to any internal or external user or entity other than the individual who is the subject of such information. **E 1869**

3.1.4 *external disclosure*, *n*—to release, transfer, or otherwise divulge confidential health information beyond the boundaries of the provider, healthcare organization or other entity which collected the data or holds the data for a specific health-related purpose.

3.1.4.1 *Discussion*—external disclosure usually requires the consent of the individual who is the subject of the information; exceptions to this rule are laws that require reporting for public health purposes or emergency treatment situations.

3.1.5 *health information*, *n*—any information, whether oral or recorded in any form or medium *(1)* that is created or received by a health care provider, a health plan, health researcher, public health authority, instructor, employer, school or university, health information service, or other entity that creates, receives, obtains, maintains, uses, or transmits health information; a health oversight agency, a health information service organization; or *(2)* that relates to the past, present, or future physical or mental health or condition of an individual, or the past, present, or future payment for the provision of health care to a protected individual; and *(3)* that identifies the individual with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. **E 1869**

4. Significance and Use

4.1 Health information systems should employ generally accepted security features; however, these features alone will not protect the confidentiality of individually identifiable health

[1] This guide is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.20 on Data and System Security for Health Information.

Current edition approved Oct. 10, 1998. Published November 1998.

[2] *Annual Book of ASTM Standards*, Vol. 14.01

[3] CPRI, 4915 St. Elmo Avenue, Suite 401, Bethesda, MD 20814.

information. Each individual who has access to health information is responsible to maintain the confidentiality and security of the information. Most breaches in confidentiality occur as a result of a deliberate or inadvertent act of human behavior.

4.2 Health information primarily supports the delivery of patient care but is commonly used for health care payment, research, public health, management, and oversight purposes. Health information may migrate from the healthcare delivery system to other business record systems (insurance, employment, credit, etc.). In addition to health professionals, individually identifiable health information is available to many others not directly involved in patient care.

4.3 Education is a vital component of a comprehensive information security management program addressing the confidentiality and security of health information. It is essential that all organizations that collect, store, use, or maintain health information in all venues train all employees, agents, contractors, and volunteers.

4.4 Participants should demonstrate competency. Training should be reinforced periodically. New information should be communicated to all employees, agents, contractors, and volunteers and incorporated into continuing education programs. Training should be reinforced annually and all employees, agents, contractors, and volunteers should sign confidentiality agreements on an annual basis. Organizations responsible for health information should impose sanctions on employees, agents, contractors, and volunteers who violate confidentiality and security rules.

5. Privacy, Confidentiality, and Security Awareness Training

5.1 *General Security Awareness Training*—All employees, agents, contractors, and volunteers shall participate in information security awareness training programs.[4] Based on job responsibilities, individuals may be required to attend customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security. Training programs should address:

5.1.1 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.

5.1.2 *Impact of Information Technology on Privacy, Confidentiality, and Security, Including*:

5.1.2.1 Benefits, risks, and process changes related to computerization,

5.1.2.2 Legislation and regulatory requirements,

5.1.2.3 Code of ethics and professional obligations,

5.1.2.4 Social interests and demands for health data,

5.1.2.5 Policies, procedures, and expectations, and

5.1.2.6 Issues specific to remote access.

5.1.3 Personal responsibility of trainees for information security management and the extent to which scope and accountability vary within positions.

5.1.4 Sensitivity of health data and the type and degrees of protection needed in relation to the role and context of the data and the role of the user.

5.1.5 Sensitivity of employee data and the type and degree of protection needed.

5.1.6 *Types of Threats to Information Security*:

5.1.6.1 Human error (erasures, accidental damage, deliberate acts, improper disposal of paper and disks, etc.).

5.1.6.2 Nature (fire, water, lightning, earthquake, etc.).

5.1.6.3 Technical (lack of backup, system failure, virus, loss of power, etc.).

5.1.6.4 Deliberate (unauthorized disclosure, modification).

5.1.7 *Individual Responsibilities*:

5.1.7.1 Knowledge of organizations' information security policies and procedures.

5.1.7.2 Collection of valid, accurate data.

5.1.7.3 Challenging unauthorized users.

5.1.7.4 Protection of passwords, codes, etc.

5.1.7.5 Reporting security irregularities.

5.1.7.6 Protection of hardware and software.

5.1.7.7 Attending inservice education programs and participating in quality improvement activities (see CPRI Guidelines).

5.1.8 Consequences and sanctions of security breaches to the involved individual, the organization, patients, and the healthcare goals

5.2 *Job-Specific Health Information Training*—Based on job responsibilities individual training needs will vary. Each provider, organization, or entity will need to determine the content of its educational programs based on job responsibilities. For those employees, agents, contractors, and volunteers who are authorized to access health information, training should address:

5.2.1 *Methods of Data Protection Including*:

5.2.1.1 Physical security (environmental, installation),

5.2.1.2 Area access controls,

5.2.1.3 Accountability controls,

5.2.1.4 Equipment enclosures, lockdown, locks,

5.2.1.5 Fire protection systems,

5.2.1.6 Encryption, and

5.2.1.7 System security software (mainframes, networks, etc.)

5.2.2 *Technical Controls* (what data may be accessed or removed from original location to remote areas) like disaster recovery.

5.2.3 *Operational Security* (the who, which, what, where, when, why, and how often actions):

5.2.3.1 Standards operational policies and procedures.

5.2.3.2 Accountability controls.

5.2.3.3 Nondisclosure contracts and confidentiality statements.

5.2.3.4 Regular scheduled inservices.

5.2.3.5 Definitions of levels of information security.

5.2.3.6 Need-to-know basis.

5.2.3.7 Backing up data.

5.2.3.8 Audit trails.

5.2.4 *Individual Responsibilities*:

[4] Abdelhak, M., Grostick, S., Hanken, M. A., Jacobs, E., "Health Information: Management of a Strategic Resource," W.B. Saunders, Philadelphia, 1996.

5.2.4.1 Knowledge of organization's information security policies and procedures

5.2.4.2 Collection of valid, accurate data

5.2.4.3 Challenging unauthorized users

5.2.4.4 Protection of passwords, codes, etc.

5.2.4.5 Reporting security irregularities

5.2.4.6 Protection of hardware and software

5.2.4.7 Attending inservice education programs and participating in quality improvement activities

5.2.5 Issues specific to remote access.

5.2.6 Sensitivity to employee data and type and degree of protection needed.

5.2.7 *Types of Threats to Information Security*:

5.2.7.1 Human error (erasures, accidental damage, deliberate acts, improper disposal of paper and disks, etc.).

5.2.7.2 Nature (fire, water, lightning, earthquake, etc.).

5.2.7.3 Technical (lack of backup, system failure, virus, loss of power, etc.).

5.2.7.4 Deliberate (unauthorized disclosure, modification) (see CPRI Guidelines).

5.2.8 Types of potential confidentiality breaches.

5.3 *External Disclosure of Health Information Requirements Training*—Only specifically authorized staff is allowed to disclose individually identifiable health information to external requesters or to another organization or entity. All employees, agents, contractors, and volunteers shall know who is authorized to perform this function in order to refer requests for health information to the appropriate organizational component or individual.

5.3.1 There are federal and state statutes and regulations regarding disclosure of individually identifiable health information. The appropriate statutes and regulations should be integrated into the organization's policies and procedures. These policies and procedures should be presented and discussed as part of the external disclosure training process.

5.3.2 The role of the individual in this disclosure process shall be clear. In most instances, individually identifiable health information about an individual is only disclosed with the authorization of the individual. The individual has the right to limit the scope of the disclosure. The instances in which disclosure does not require the authorization of the individual should be made clear. These instances include, for example, required reporting for public health purposes and emergency treatment.

5.3.3 The various forms of appropriate authorization (court order, authorization from patient or legal guardian or pursuant to federal or state statutes or regulations) should be presented or reviewed. The circumstances in which an authorization will be accepted from someone other than the subject of the health information should be explained.

6. Training Schedule

6.1 *First-time Training or Education, or Both*:

6.1.1 Conduct training or education, or both, at the generic institutional level or the specific to job function level.

6.1.2 Document trainee attendance.

6.1.3 Grant access to health information only after training is completed and agreements are signed.

6.1.4 Focus on concrete examples.

6.1.5 Use appropriate outside resources.

6.1.6 Choose attention-getting themes (for example, patient-centered focus).

6.2 *Continuing Education and Training*:

6.2.1 Renew confidentiality and security statements and inservices annually.

6.2.2 Conduct continuing awareness campaigns to provide organizational reinforcement.

6.2.3 Ensure familiarity with specially protected information.

6.2.4 Make information security training a precondition for any credentialling processes.

6.2.5 Focus on training as part of risk reduction strategy.

6.2.6 Identify champion of security awareness and offer awards or incentives, or both.

6.2.7 Conduct patient/client surveys that include questions regarding privacy, confidentiality, and security. Give feedback to staff (surveys should be done with concepts of reliability and validity incorporated into the design and preparation of a survey).

7. Instructional Methods

7.1 A variety of instructional methods should be employed to address the specific learning objectives of each program and meet the needs of target audiences. The program should challenge learners to participate and strive to find ways to incorporate feedback to learners about how well they learned the material presented. Training methods and training schedules should meet the learners' needs. Examples of instructional technologies, methods, and strategies are:

7.1.1 Case study.

7.1.2 Discussion of issues.

7.1.3 Scenarios or role play.

7.1.4 Computer-based training.

7.1.5 Videotaped instruction.

7.1.6 Interactive technology.

7.1.7 Handouts, audiovisuals, references, self-study information.

7.1.8 Briefings and lectures.

7.1.9 Reviews during performance evaluations.

7.1.10 Network (email) briefings (see CPRI Guidelines).

8. Learning Outcome Measurement

8.1 Evaluation of individual information security education programs or offerings, or both, should include the following criteria:

8.1.1 Learner achievement of program objectives.

8.1.2 Learner achievement of personal objectives.

8.1.3 Teaching effectiveness of faculty (trainers).

8.1.4 Relevance of content to objective or job performance, or both. (Can the learner apply the information to their practice?)

8.1.5 Appropriateness of faculty (trainers).

8.1.6 Appropriateness of teaching methodologies.

8.1.7 Appropriateness of the teaching/learning environment.

8.1.8 Recommendation for improvement.

8.2 Examples of evaluation methodologies for individual information security programs or offerings, or both:

8.2.1 Participant evaluation teams (focus group) sessions.

8.2.2 Questionnaires.
8.2.3 Group discussions.
8.2.4 Test.
8.2.5 Simulations and case study reviews.

8.3 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 be depend on the organization's current needs and available resources.

8.3.1 Examples of methodologies for evaluation of the total program:

8.3.1.1 Quality improvement risk assessments

8.3.1.2 Comparison of number and severity of security violations with pretraining statistics to assess levels of improvement

8.3.1.3 Pattern analysis methods
8.3.1.4 Discrepancy evaluation models
8.3.1.5 Audit evaluation models
8.3.1.6 Impact evaluation models (see CPRI Guidelines).

9. New Training Needs

9.1 Training programs must be periodically updated based on changes in the system. Examples of such changes are: the use of the internet to transfer individually-identifiable health information, new software applications, changes in federal or state statutes or regulations, or changes in the healthcare delivery system model.

10. Keywords

10.1 confidentiality; health information; health information access; privacy; security; training