



Standard Guide for Training of Persons who have Access to Health Information¹

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 employees, 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 Records²

2.2 CPRI Guidelines:

Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Records June, 1995³

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.