



# Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records<sup>1</sup>

This standard is issued under the fixed designation E1869; 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 ( $\epsilon$ ) indicates an editorial change since the last revision or reapproval.

## 1. Scope

1.1 This guide covers the principles for confidentiality, privacy, access, and security of person identifiable health information. The focus of this standard is computer-based systems; however, many of the principles outlined in this guide also apply to health information and patient records that are not in an electronic format. Basic principles and ethical practices for handling confidentiality, access, and security of health information are contained in a myriad of federal and state laws, rules and regulations, and in ethical statements of professional conduct. The purpose of this guide is to synthesize and aggregate into a cohesive guide the principles that underpin the development of more specific standards for health information and to support the development of policies and procedures for electronic health record systems and health information systems.

1.2 This guide includes principles related to:

|                                  | Section |
|----------------------------------|---------|
| Privacy                          | 7       |
| Confidentiality                  | 8       |
| Collection, Use, and Maintenance | 9       |
| Ownership                        | 10      |
| Access                           | 11      |
| Disclosure/Transfer of Data      | 12      |
| Data Security                    | 13      |
| Penalties/Sanctions              | 14      |
| Education                        | 15      |

1.3 This guide does not address specific technical requirements. It is intended as a base for development of more specific standards.

## 2. Referenced Documents

### 2.1 ASTM Standards:<sup>2</sup>

<sup>1</sup> This guide is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and are the direct responsibility of Subcommittee E31.25 on Healthcare Data Management, Security, Confidentiality, and Privacy.

Current edition approved April 1, 2014. Published April 2014. Originally approved in 1997. Last previous edition approved in 2010 as E1869–04(2010). DOI: 10.1520/E1869-04R14.

<sup>2</sup> For referenced ASTM standards, visit the ASTM website, [www.astm.org](http://www.astm.org), or contact ASTM Customer Service at [service@astm.org](mailto:service@astm.org). For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

E1384 Practice for Content and Structure of the Electronic Health Record (EHR)

E1714 Guide for Properties of a Universal Healthcare Identifier (UHID)

E1762 Guide for Electronic Authentication of Health Care Information

E1769 Guide for Properties of Electronic Health Records and Record Systems

E1986 Guide for Information Access Privileges to Health Information

E1987 Guide for Individual Rights Regarding Health Information (Withdrawn 2007)<sup>3</sup>

E1988 Guide for Training of Persons who have Access to Health Information (Withdrawn 2007)<sup>3</sup>

E2017 Guide for Amendments to Health Information

E2147 Specification for Audit and Disclosure Logs for Use in Health Information Systems

## 3. Terminology

### 3.1 Definitions:

3.1.1 *access*—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.

### 3.1.2 *authentication*:—

3.1.2.1 *authentication (data entry)*—to authorize or validate an entry in a record by a signature including first initial, last name, and discipline or a unique identifier allowing identification of the responsible individual.

3.1.2.2 *authentication (data origin/sender)*—corroboration that the source/sender of data received is as claimed.

3.1.2.3 *authentication (user/receiver)*—the provision of assurance of the claimed identity of an entity/receiver.

3.1.3 *authorize*—the granting to a user the right of access to specified data and information, a program, a terminal, or a process.

<sup>3</sup> The last approved version of this historical standard is referenced on [www.astm.org](http://www.astm.org).