Designation: E1869 – 04

An American National Standard

Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records[1]

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 (ε) 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:*[2]

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[3]

E1988 Guide for Training of Persons who have Access to Health Information[3]

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.

3.1.4 *clinical data centers*—all computer-based (and manual) systems which handle and store patient records and health information, for example, solo practitioners, clinics,

[1] This guide is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and are the direct responsibility of Subcommittee E31.25 on Healthcare Management, Security, Confidentiality, and Privacy.

Current edition approved Nov. 1, 2004. Published December 2004. Originally approved in 1997. Last previous edition approved in 1997 as E1869 – 97. DOI: 10.1520/E1869-04.

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

[3] Withdrawn. The last approved version of this historical standard is referenced on www.astm.org.

hospitals, state departments of health, data centers, and health maintenance organizations.

3.1.5 *clinical information*—data and information collected from the patient or patient's family by a healthcare practitioner or healthcare organization. A healthcare practitioner's objective measurement or subjective evaluation of a patient's physical or mental state of health, descriptions of an individual's health history and family health history, diagnostic studies, decision rationale, descriptions of procedures performed, findings, therapeutic interventions, medications prescribed, description of responses to treatment, prognostic statements and descriptions of socioeconomic factors, and environmental factors related to the patient's health.

3.1.6 *computer-based patient record*—see *patient record*.

3.1.7 *confidential*—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.

3.1.8 *data*—collection of elements on a given subject; things known, given, or assumed, as the basis for decision making; the raw material of information systems expressed in text, numbers, symbols and images; facts.

3.1.9 *data protection measure*—a planned operation, for example, procedure, policy, program, or technology, employed in the privacy system to prevent, detect, or sanction breaches of security.

3.1.10 *disclosure*—to release, transfer, or otherwise divulge confidential health information to any entity other than the individual who is the subject of such information.

3.1.11 *health care*—*(1)* preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, public health, counseling, service, or procedure with respect to the physical or mental condition of an individual; or affecting the structure or function of the human body; or *(2)* any sale or dispensing of a drug, device, equipment, or other item to an individual, or for the use of an individual, pursuant to a prescription.

3.1.12 *health information*—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, life insurer, school or university; health care clearinghouse, 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, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an 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.

3.1.13 *inference*—refers to the ability to deduce the identity of a person associated with a set of data through "clues" contained in that information. This analysis permits determination of the individual's identity based on a combination of facts associated with that person even though specific identifiers have been removed, like name and social security number.

3.1.14 *information*—data that have been processed for use; human interpretation of data; data that have been processed into a meaningful form.

3.1.15 *informed consent*—informed consent requires that individuals be informed, in advance, of the information being collected from them, or generated, and the purposes for which it will be used; and be given an opportunity to accept, reject, or modify the terms presented. Central to the principle of informed consent is providing individuals with the ability to control the use of information once collected. The general rule is that information collected for one purpose must not be used for another purpose without the individual's consent. In practice, this requires that no use or disclosure occur, except to a documented request by, or with the prior consent of, the individual to whom the record pertains unless the disclosure is permitted by law. Under some circumstances a guardian or designee may consent on behalf of the individual.

3.1.16 *informational privacy*—*(1)* a state or condition of controlled access to personal information. *(2)* The ability of an individual to control the use and dissemination of information that relates to himself or herself. *(3)* The individual's ability to control what information is available to various users and to limit redisclosures of information.

3.1.17 *patient record:*

3.1.17.1 *longitudinal patient record*—a permanent, coordinated patient record of significant information, in chronological sequence. It may include all historical data collected or be retrieved as a user designated synopsis of significant demographic, genetic, clinical and environmental facts and events maintained within an automated system.

3.1.17.2 *patient health record*—the primary legal record documenting the healthcare services provided to a person, in any aspect of healthcare delivery.

Discussion—The term *patient health record* is synonymous with: medical record, patient care record, hospital record, clinical record, client record, resident record, electronic medical record, and computer-based patient record. The term includes routine clinical or office records, hospital records, records of care in any health-related setting, research protocols, preventive care, life style evaluation, special study records, and various clinical databases.

3.1.17.3 *patient record system*—the set of components that form the mechanism by which patient records are created, used, stored, and retrieved. A patient record system is usually located within a healthcare provider/practitioner setting. It includes people, data, rules and procedures, processing and storage devices (for example, paper and pen, hardware and software), and communications and support function.

3.1.17.4 *secondary patient record*—a record that is derived from the primary health record and contains selected data elements to aid nonclinical persons (that is, persons not involved in direct patient care) in supporting, evaluating, or advancing patient care. Patient care support refers to administration, regulation, and payment functions. Patient care evaluation refers to quality assurance, utilization management, and medical or legal audits. Patient care advancement refers to research. These records are often combined to form a secondary database, for example, an insurance claims database.

3.1.18 *personally identifiable health information*—health information which contains an individual's identifiers (name, social security number) or contains a sufficient number of variables to allow identification of an individual.

3.1.19 *practitioner (licensed/certified)*—an individual at any level of professional specialization who requires a public license to deliver health care to individuals. An individual at any level of professional specialization who is certified by a public agency or professional organization to provide health services to individuals. A practitioner may also be a provider.

3.1.20 *privacy*—the right of individuals to be left alone and to be protected against physical or psychological invasion or the misuse of their property. It includes freedom from intrusion or observation into one's private affairs, the right to maintain control over certain personal information, and the freedom to act without outside interference. See also *informational privacy*.

3.1.21 *privilege*—the individual's right to hold private and confidential the information given to a healthcare provider in the context of a professional relationship. The individual may, by overt act of consent or by other means, waive the right to privilege. For example, if a patient brings a lawsuit against a facility and the records are needed to present the facility's case, the privilege is waived.

3.1.22 *provider*—a business entity which furnishes health care to a consumer; it includes a professionally licensed practitioner who is authorized to operate a healthcare delivery facility.

3.1.23 *security:*

3.1.23.1 *data security*—the result of effective data protection measures; the sum of measures that safeguard data and computer programs from undesired occurrences and exposure to: *(1)* accidental or intentional access or disclosure to unauthorized persons, or a combination thereof, *(2)* accidental or malicious alteration, *(3)* unauthorized copying, *(4)* loss by theft or destruction by hardware failures, software deficiencies, operating mistakes; physical damage by fire, water, smoke, excessive temperature, electrical failure or sabotage; or a combination thereof. Data security exists when data are protected from accidental or intentional disclosure to unauthorized persons and from unauthorized or accidental alteration.

3.1.23.2 *system security*—security is the totality of safeguards including hardware, software, personnel policies, information practice policies, disaster preparedness, and oversight of these components. Security protects both the system and the information contained within from unauthorized access from without and from misuse from within. Security enables the entity or system to protect the confidential information it stores from unauthorized access, disclosure, or misuse; thereby protecting the privacy of the individuals who are the subjects of the stored information.

4. Significance and Use

4.1 Many U.S. healthcare and health information systems leaders believe that electronic health information systems that include computer-based patient records will improve health care. To achieve this goal these systems will need to protect individual privacy of patient data, provide appropriate access, and use adequate data security measures. Sound information policies and practices must be in place prior to the wide-scale deployment of health information systems. Strong enforceable privacy policies must shape the development and implementation of these systems.

4.2 The purposes of patient records are to document the course of the patient's illness or health status during each encounter and episode of care; to furnish documentary evidence of the course of the patient's health evaluation, treatment and change in condition; to document an individual's health status; to provide data for preventive care; to document communication between the practitioner responsible for the patient's care and any other healthcare practitioner who contributes to the patient's care; to assist in protecting the legal interest of the patient, the health care facility and the responsible practitioner; to provide continuity of care; to provide data to substantiate insurance claims; to provide a basis for evaluating the adequacy and appropriateness of care; and to provide data for use in continuing education and research.

4.3 Health information is a broad concept. It includes all information related to an individual's physical and mental health, the provision of health care generally, and payment for health care. The patient record is a major component of the health information system. The creation of electronic databases and communication protocols to transfer data between systems presents new opportunities to implement more effective systems for health information, to enhance patient care, reduce the cost of health care, and improve patient outcomes. National standards guide all that have responsibilities for records and information systems containing person identifiable health data and information.

4.4 This guide also acknowledges the large and growing list of health information databases already in existence. These databases have been assembled to pay for services rendered (insurance), to validate the appropriate use of patient services (utilization management), to support policy (national levels), to gather data for research/tracking of specific problems (registries—such as tumor, trauma, birth defects, mental health case management), to prevent the spread of disease (required reporting of communicable diseases such as tuberculosis, gonorrhea, AIDS), and to respond to new uses which are proposed each year.

4.5 National standards delineating principles and practices in the areas of confidentiality, privacy, access, and data security will provide a guide for policy, law, and systems development and a base for standards for electronic health information regardless of its location.

5. Description of Standards

5.1 The Privacy Act, although applicable only to federal agencies and federal contractors, outlines basic tenets useful for any group, facility, or individual that maintains records on individuals. These tenets should be incorporated into policies and practices for electronic health record systems and health information systems. The basic tenets are:

5.1.1 The individual has the right to know that identifiable, personal information is available in a record system and to know what that information is used for.

5.1.2 The individual may have access to the records, has a right to have a copy made, and has the right to amend or correct the records.

5.1.3 The data may not be used for any use beyond that for which the data are collected (as specified by law or regulation).

5.1.4 Written consent of the individual shall be obtained for all other uses (beyond those specified by law or regulation).

NOTE 1—Technology provides means for electronic forms of consent and authentication.

5.1.5 The data shall be collected and used only for a necessary and lawful purpose.

5.2 In addition to the Privacy Act, the U.S. Department of Health and Human Services has adopted privacy regulations that support the principles outlined in this standard. The privacy regulations are part of an Administrative Simplification component of the Health Insurance Portability and Accountability Act of 1996. The regulations apply to health plans, health care clearinghouses, and health care providers who transmit health information in electronic form to carry out financial or administrative activities related to health care.

5.3 The electronic health record and many electronic health information systems provide flexibility in collecting, organizing, and disseminating data. It is possible to segment data and provide only needed data to legitimate users both within and external to a healthcare facility, for example, lab technician, business office, switchboard, third party payer, or workmen's compensation agency. This same technology allows easier linking of data. This guide does not address the specifics of data linkage. However, the value of appropriate data linkage and its potential uses are recognized.

5.3.1 Electronic health record systems and other health information systems should facilitate access to patient information by authorized healthcare practitioners during the active phase of treatment. The needs of emergency care situations should be given special attention and procedures.

5.3.2 This guide is intended to provide a base for construction of laws, regulations, systems, and policies for health information systems and electronic health records systems by all entities that use, handle, or store health information pertaining to individuals, or a combination thereof. The focus of this standard is primarily the individual recipient of healthcare; however, in some principles the privacy and confidentiality interests of practitioners and the confidentiality interests of providers are also recognized. While not developed in this standard it is recognized that patients are responsible for certain aspects of their care. This responsibility may include collecting and communicating personal health data. This data may reside in a health information system database or record.

6. Principles

6.1 The following statements of principles are organized into categories. Each category lists principles and provides a discussion related to the principle. The categories are:

6.1.1 Privacy.

6.1.2 Confidentiality.

6.1.3 Collection, Use, and Maintenance.

6.1.4 Ownership.

6.1.5 Access.

6.1.6 Disclosure/Transfer of Data.

6.1.7 Data Security.

6.1.8 Penalties/Sanctions.

6.1.9 Education.

7. Privacy

7.1 Individuals have privacy rights related to how information about them is collected, used, and disclosed.

7.1.1 Privacy is the right of an individual to be left alone. It includes freedom from intrusion or observation into one's private affairs and the right to maintain control over certain personal information. Individuals share personal information with healthcare providers and practitioners in the care process. However, individuals are entitled to expect the healthcare system and those involved to respect the individual's privacy.

7.1.2 Respect for individual privacy is demonstrated in the way the health information is collected, used, and disclosed. For individuals who are receiving health services the process of data collection, whether through interview, examination, or testing should respect the individual's privacy. The use of the information must be appropriate and respect the individual's privacy. Disclosures of information shall be sensitive to an individual's privacy and either be allowed by law or involve the consent of the individual or his or her designated representative.

7.2 Individuals have a right to know that identifiable, personal information is available in a health record, health information system, or other information system and to know to whom the information is available and the use of that information.

7.2.1 Those who collect data and maintain record systems should notify individuals of the types of information collected and generally how the information will be used and, if known, specific uses and locations of health information databases which will contain a patient's information, especially those that go beyond the boundaries of the provider healthcare organization. Examples of databases outside the provider organization are: regional registries for cancer, trauma, and implants; the Medical Information Bureau; third party payers; health data organizations; state and regional data systems; and research databases.

7.3 Healthcare organizations, practitioners, and others with access to health information shall respect an individual's right to privacy and provide appropriate protections to identifiable data and information.

7.3.1 Electronic health record systems and health information systems shall protect individual privacy. These systems should be capable of providing this protection to patients, practitioners and organizations. More extensive protections of data are typically required in the areas of mental health, sexually transmitted disease, obstetrics and drug/alcohol treatment. For example, drug/alcohol treatment regulations protect an individual's privacy by requiring that the facility not acknowledge an admission except to those individuals designated by the patient.

8. Confidentiality

8.1 Personally identifiable health information shall be treated confidentially.