Designation: E1986 – 09 (Reapproved 2013)

An American National Standard

# Standard Guide for Information Access Privileges to Health Information[1]

This standard is issued under the fixed designation E1986; 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 process of granting and maintaining access privileges to health information. It directly addresses the maintenance of confidentiality of personal, provider, and organizational data in the healthcare domain. It addresses a wide range of data and data elements not all traditionally defined as healthcare data, but all elemental in the provision of data management, data services, and administrative and clinical healthcare services. In addition, this guide addresses specific requirements for granting access privileges to patient-specific health information during health emergencies.

1.2 This guide is based on long-term existing and established professional practices in the management of healthcare administrative and clinical data. Healthcare data, and specifically healthcare records (also referred to as medical records or patient records), are generally managed under similar professional practices throughout the United States, essentially regardless of specific variations in local, regional, state, and federal laws regarding rules and requirements for data and record management.

1.3 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.

1.4 This guide applies to all collection, use, management, maintenance, disclosure, and access of all individual, group, and organizational data related to health care.

1.5 This guide does not attempt to address specific legislative and regulatory issues regarding individual, group, and organizational rights to protection of privacy.

1.6 This guide covers all methods of collection and use of data whether paper-based, written, printed, typed, dictated, transcribed, forms-based, photocopied, scanned, facsimile, telefax, magnetic media, image, video, motion picture, still picture, film, microfilm, animation, 3D, audio, digital media, optical media, synthetic media, or computer-based.

1.7 This guide does not directly define explicit disease-specific and evaluation/treatment-specific data control or access, or both. As defined under this guide, the confidential protection of elemental data elements in relation to which data elements fall into restrictive or specifically controlled categories, or both, is set by policies, professional practice, and laws, legislation and regulations.

## 2. Referenced Documents

2.1 *ASTM Standards:*[2]

E1869 Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records

E2595 Guide for Privilege Management Infrastructure

## 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. **(E1869)**

3.1.2 *access control*—the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2.1 *Discussion*—Access control counters the threat of unauthorized access to, disclosure of, or modification of data. **(ISO 7498-2)**

3.1.3 *accountability*—the property that ensures that the actions of an entity can be traced. **(ISO 7498-2)**

3.1.4 *audit trail*—data collected and potentially used to facilitate a security audit. **(ISO 7498-2)**

3.1.5 *authentication*—the corroboration that an entity is the one claimed. **(ISO 7498-2)**

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

Current edition approved March 1, 2013. Published March 2013. Originally approved in 1998. Last previous edition approved in 2009 as E1986 –09. DOI: 10.1520/E1986-09R13.

[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.

***A Summary of Changes section appears at the end of this standard**

3.1.6 *authorize*—the granting to a user the right of access to specified data and information, a program, a terminal, or a process. **(E1869)**

3.1.7 *authorization—(1)* The granting of rights, which includes the granting of access based on access rights. *(2)* The mechanism for obtaining consent for the use and disclosure of health information. **(ISO 7498-2, CPRI, AHIMA)**

3.1.8 *confidential*—status accorded to data or information indicating that it is sensitive for some reason and needs to be protected against theft, disclosure, or improper use, or both, and must be disseminated only to authorized individuals or organizations with an approved need to know. Private information which is entrusted to another with the confidence that unauthorized disclosure that will be prejudicial to the individual will not occur. **(E1869)**

3.1.9 *confidentiality*—the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. **(ISO 7498-2)**

3.1.10 *database*—a collection of data organized for rapid search and retrieval. **(Webster's, 1993)**

3.1.11 *data element*—the combination of one or more data entities that forms a unit or piece of information, such as the social security number, a diagnosis, an address, or a medication.

3.1.12 *data entity*—a discrete form of data such as a number or word.

3.1.13 *disclosure (health care)*—the release of information to third parties within or outside the healthcare provider organization from an individual's record with or without the consent of the individual to whom the record pertains.

3.1.13.1 *Discussion*—Under this guide the definition is slightly modified to read: the release of information to an individual, group or organization from an individual's health information with or without the authorization of the individual to whom the health information pertains. **(CPRI)**

3.1.14 *emergency*—a sudden demand for action. Condition that poses an immediate threat to the health of the patient.

3.1.15 *healthcare data*—data which are input, stored, processed or output by the automated information system which support the business functions of the healthcare establishment. These data may relate to person identifiable records or may be part of an administrative system where persons are not identified. **(CEN)**

3.1.16 *health information*—any information, whether oral or recorded in any form or medium *(1)* that is created or received by a healthcare 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, the provision of health care to an individual, or the past, present, or future payments 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. **(HIPAA, E1869)**

3.1.17 *information*—data to which meaning is assigned, according to context and assumed conventions. **(National Security Council, 1991, E1869)**

3.2 *Definitions of Terms Specific to This Standard:*

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

3.2.1.1 *external disclosure*—disclosure outside an organization.

3.2.1.2 *internal disclosure*—disclosure within an organization.

## 4. Significance and Use

4.1 The maintenance of confidentiality in paper-based, electronic, or computer-based health information requires that policies and procedures be in place to protect confidentiality. Confidentiality of information depends on structural and explicit mechanisms to allow persons or systems to define who has access to what, and in what situation that access is granted. For guidelines on the development and implementation of privilege management infrastructures supporting these mechanisms, see Guide E2595.

4.2 Confidential protection of data elements is a specific requirement. The classification of data elements into restrictive and specifically controlled categories is set by policies, professional practice, and laws, legislation, and regulations.

4.3 There are three explicit concepts upon which the use of and access to health information confidentiality are defined. Each of these concepts is an explicit and unique characteristic relevant to confidentiality, but only through the combination (convergence) of all three concepts can appropriate access to an explicit data element at a specific point in time be provided, and unauthorized access denied. The three concepts are:

4.3.1 The categorization and breakdown of data into logical and reasonable elements or entities.

4.3.2 The identification of individual roles or job functions.

4.3.3 The establishment of context and conditions of data use at a specific point in time, and within a specific setting.

4.4 The overriding principle in preserving the confidentiality of information is to provide access to that information only under circumstances and to individuals when there is an absolute, established, and recognized need to access that data, and the information accessed should itself be constrained only to that information essential to accomplish a defined and recognized task or process. Information nonessential to that task or process should ideally not be accessible, even though an individual accessing that information may have some general right of access to that information.

## 5. Principles

5.1 The following principles are based upon U.S. state and federal laws, current European Economic Community initiatives and laws and regulations resulting from those initiatives, and professional practice within the U.S. and European healthcare domains.

5.2 Individuals, groups, and organizations retain rights over the specific, intermediate, and ultimate use of any data collected from them and about whom the data is retained and managed.

5.3 No individual, group, or organizational data shall be collected, used, maintained, released, or disclosed without the specific explicit informed consent of the individual, group, or organization, unless specifically required for the protection of public health, and mandated by local, state, regional, or federal law.

5.4 Individual, group, or organizational data may only be used for the purpose for which it was collected. Explicit informed consent of the individual, group, or organization from which the data was collected is required if the data is to be used for any additional purpose. Organizational policies shall state the purposes for which data will be collected, maintained, and used.

5.5 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 healthcare related data, are required to collect, manage, maintain, disclose, provide access to, or release that data only in strict compliance with the data access rules defined in this guide. If they are unable to adhere to this guide they will not retain data beyond its initial collection and use, or will securely and confidentially entrust that data to an authorized organization that can abide by the rules under this guide.

5.6 Data and data elements under this guide are defined at a discrete level. This is necessary in order to define data access and use rights down to discrete elemental data. This guide is established under the assumption that there is no such thing as "dis-identified data" in that as long as data exist as discrete elemental data they are ultimately identifiable with an individual. For example a diagnosis or a patient weight is not dis-identified within a population just because it does not have a name or other outward identifying information attached or linked to it. The average weight within a population or the incidence of a given disease, both calculated or derived from a population aggregate, may be dis-identified from an individual within a population, but might still predispose the population to identification or prejudice. For example an "abnormal" average weight might increase the health risk to a population, therefore providing valuable preventative and epidemiological data, but if that data is assumed to be dis-identified and generally available for review, then it might allow population-based prejudicial pricing for healthcare services or insurance. Disease incidence can also be used to target populations at health risk, but if considered dis-identified and generally available for review, disease incidence can also be used to identify populations as to race, religion, ethnicity, genetics, sexual preferences, and other prejudicial indicators. The protection of individual, group, and organizational data confidentiality under this guide is, therefore, absolute and is always based upon the connection of that data to the individual, group, or organization from which the data was collected and for or about whom the data is retained and managed. No data is releasable as discrete data or discrete data-types under any assumption that since another related data element (for example, name, age, sex, address, etc.) was not released, that the data is no longer individual, group, or organizational data, or can no longer be identified or connected to any individual, group, or organization.

5.7 All access shall be explicitly authorized. Unauthorized access is explicitly forbidden.

## 6. Data Elements

6.1 Data elements under this guide represent fragmentation (separation) of data into discrete entities. These entities (data elements) represent discrete elemental data types that can be reconstructed into complete data sets according to varying needs and requirements of access and use, by appropriate data-users, under appropriately defined and authorized roles. Data elements exist as discrete data in their own right or can be aggregated as data sets that represent data about a specific individual, provider, group, or organization, or they can be aggregated across individuals, providers, groups, or organizations.

6.2 Data elements and data entities under this guide are explicitly delineated and apply to healthcare related data in aggregate as well as discrete forms.

6.3 If data exist in aggregate form and cannot be broken down or protected from improper use or disclosure at the data element or entity level, then the aggregate data itself cannot be released for use or disclosure to any data-user other than those who meet the access privilege rules for the most confidential data within that aggregate.

6.3.1 *Example*—HIV data within a document, even if only a small fraction of the content of that document, makes the entire document subject to the rules of disclosure defined for HIV data, unless that HIV data (or any other data of that class) can be stripped (removed) from the document.

6.3.2 In addition, if aggregate data is stripped of any non-disclosable data for disclosure to a data-user, then the disclosed data can have no evidence, sign, or indication of the fact that it was stripped of non-disclosable data. An exception under this requirement should be granted only in the instance where it is impossible or impractical to screen or filter confidential data from the aggregate form in which it was entered into the health record, such as handwritten or dictated and transcribed physician notes or histories and physicals that contain data of differing levels of confidentiality. In the instance of hand written or dictated and transcribed data, non-disclosable data should still be masked when these data are reviewed or accessed by data-users without appropriate authorization to review and access the most confidential elemental data within that data set.