



Standard Specification for Management of the Confidentiality and Security of Dictation, Transcription, and Transcribed Health Records¹

This standard is issued under the fixed designation E1902; 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 specification covers a broad description of certain steps that shall be taken by those involved in the processes of dictation and transcription of healthcare documentation to protect the documentation during its development, maintenance, transmission, storage, and retrieval. Variations or exceptions may be appropriate in special situations or because of particular contractual obligations, institutional policies and rules, or provisions of law or regulation.

1.2 Healthcare clients trust and expect that personal health information will be maintained in a confidential and secure manner. This specification has been developed for the purpose of protecting the confidentiality and security of all forms of dictation, transcription, and transcribed healthcare documentation.

1.3 This specification supports the patient's right to confidential, private, and secure healthcare documentation and identifies procedures for preventing breaches of these patient rights.

1.4 This specification seeks to identify certain dictation and transcription practices that may increase the risks of breaching confidentiality, infringing on privacy, and violating security of healthcare documentation.

2. Referenced Documents

2.1 ASTM Standards:²

E1762 Guide for Electronic Authentication of Health Care Information²

E1869 Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records²

E1959 Guide for Requests for Proposals Regarding Medical Transcription Services for Healthcare Institutions²

E1985 Guide for User Authentication and Authorization²

E1986 Guide for Information Access Privileges to Health Information²

E1988 Guide for Training of Persons who have Access to Health Information^{3 2}

E2017 Guide for Amendments to Health Information²

E2084 Specification for Authentication of Healthcare Information Using Digital Signatures^{3 2}

E2085 Guide on Security Framework for Healthcare Information^{3 2}

E2147 Specification for Audit and Disclosure Logs for Use in Health Information Systems²

E2184 Specification for Healthcare Document Formats

2.2 Other Documents:

Public Law 104-191 Health Insurance Portability and Accountability Act of 1996 (HIPAA)⁴

45 CFR Part 142 Security and Electronic Signature Standards; Proposed Rule, U.S. Department of Health and Human Services⁴

45 CFR, Parts 160-164 Standards for Privacy of Individually Identifiable Health Information; U.S. Department of Health and Human Services, Office of the Secretary⁴

3. Terminology

3.1 Definitions:

3.1.1 *author, n*—the person originating content for a healthcare document.

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 a combination thereof, and must be disseminated only to authorized individuals or organizations with a need to know.

E1869

3.1.3 *confidentiality, n*—the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

45 CFR Part 142

3.1.4 *individually identifiable health information, n*—any information, including demographic information collected from an individual, that (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or

¹ This specification is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.15 on Health Information Capture and Documentation.

Current edition approved June 10, 2002. Published July 2002. Originally published as E1902–97. Last previous edition E1902–97. DOI: 10.1520/E1902-02.

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

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

⁴ Available from U.S. Government Printing Office, Superintendent of Documents, 732 N. Capitol St., NW, Mail Stop: SDE, Washington, DC 20401. See also <http://aspe.hhs.gov/admnsimp>

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 (i) identifies the individual, or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Public Law 104-191, Section 1171 (6)

3.1.5 *privacy, n*—the right of an individual to be left alone and to be protected against physical or psychological invasion or 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. **E1869**

3.1.6 *provider, n*—a business entity which furnishes health care to a consumer; it includes a professionally licensed practitioner who is authorized to operate a healthcare delivery system. **E1869**

3.1.7 *secure environment, n*—free from access by unauthorized persons and from unauthorized or accidental alteration.

3.1.8 *security, n*—encompasses all of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness, and the oversight of all these areas. The purpose is to protect both the system and the information it contains from unauthorized access from without and from misuse from within.

45 CFR Part 142

4. Significance and Use

4.1 This specification acknowledges the importance of heightened awareness concerning the protection of confidentiality and security of healthcare documentation by all individuals associated with the dictation and transcription process.

4.2 This specification suggests methods to protect the confidentiality and security of healthcare documentation during the processes of dictation and transcription, including maintenance, transmission, storage, and retrieval.

4.3 Federal and state laws and regulations govern the extent of confidentiality and security and define the exceptions when disclosures of individually identifiable health information can be legally required. Third party payer rules, provider rules, institutional rules, and other contractual provisions also may affect the procedures utilized by medical transcriptionists and other healthcare personnel to maintain the confidentiality and security of healthcare documentation. There are certain conditions prescribed by law or regulation under which disclosure of health information is permissible.

4.4 Ensuring the confidentiality and security of individually identifiable health documentation through appropriate policies, procedures, continuing education, and training of healthcare personnel has become an important element of risk management. It is intended that this specification will contribute to compliance with laws and regulations to improve protection of such documentation, and it will help to minimize the risk of litigation against healthcare professionals, thereby reducing healthcare costs.

4.5 Policies and procedures adopted to protect healthcare documentation and ensure its authenticity and accuracy shall apply to all parties who participate in the processes of

dictation, transcription, maintenance, transmission, storage, and retrieval of that data.

4.6 Security and confidentiality statements, policies, and agreements shall be maintained, reviewed, and signed by all involved in the process of dictation and transcription of healthcare documentation. Formal orientation and continuing education regarding confidentiality, patient privacy, and documentation security shall continue.

4.7 Procedures for reporting real or potential breaches, or both, in confidentiality and security to the appropriate risk management personnel, medical transcription business management personnel, internal auditor, department manager, privacy officer, or other appropriate person(s) shall be clearly documented and communicated.

4.8 This specification is intended to assist in developing appropriate policies that provide protection of individually identifiable healthcare information and documentation.

5. Dictation Security Policies and Procedures

5.1 Security and confidentiality obligations shall be thoroughly explained at the time that access privileges are granted, and understanding and agreement shall be acknowledged by signed statements that are reviewed and renewed periodically. For additional guidance, see Guides **E1985** and **E2085**, and Specification **E2084**.

5.1.1 Those individuals who dictate healthcare documents and those who have access to dictation equipment including, but not limited to, business owners, supervisors, managers, coders, billing and file clerks, other healthcare providers, students, vendors, and equipment maintenance personnel, shall receive instruction during the orientation phase regarding security and confidentiality obligations. These individuals shall acknowledge that they have been informed about and will fulfill their obligation to protect security and to maintain confidentiality by signing statements of understanding and agreement at the time that access privileges are granted and at regularly scheduled reviews. Upon changes in policies or procedures, orientation and acknowledgment shall be repeated. For additional guidance see Guides **E1986** and **E1988**.

5.2 Dictation Procedures Shall Ensure Data Security:

5.2.1 Dictation shall not be done in any environment in which persons other than the patient or the patient's legal representative may overhear confidential information.

5.2.2 Individuals involved in the patient documentation process shall refrain from utilizing telephones or dictation equipment in locations where individually identifiable health information is likely to be overheard. For example, individuals shall not dictate healthcare documentation into public telephones, cellular phones, or other recording devices that are located within the hearing distance of others.

5.2.3 Electronic transmission of patient information shall comply with Guide **E1869**. Patient demographics or other individually identifiable health information shall not be transmitted via computer bulletin boards or similar public media. Internet or e-mail shall be used only when sender and receiver understand that data will be transmitted in this manner and take adequate precautions, for example, through encryption or other security technologies, to secure the data and to ensure that no unauthorized access is allowed. Such documentation shall be