Designation: E 1902 – 02

An American National Standard

Standard Specification for Management of the Confidentiality and Security of Dictation, Transcription, and Transcribed Health Records[1]

This standard is issued under the fixed designation E 1902; 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:*

E 1762 Guide for Electronic Authentication of Health Care Information[2]

E 1869 Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records[2]

E 1959 Guide for Requests for Proposals Regarding Medical Transcription Services for Healthcare Institutions[2]

E 1985 Guide for User Authentication and Authorization[2]

E 1986 Guide for Information Access Privileges to Health Information[2]

E 1988 Guide for Training of Persons who have Access to Health Information[2]

E 2017 Guide for Amendments to Health Information[2]

E 2084 Specification for Authentication of Healthcare Information Using Digital Signatures[2]

E 2085 Guide for Security Framework for Healthcare Information[2]

E 2147 Specification for Audit and Disclosure Logs for Use in Health Information Systems[2]

E 2184 Specification for Healthcare Document Formats[2]

2.2 *Other Documents:*

Public Law 104-191 Health Insurance Portability and Accountability Act of 1996 (HIPAA)[3]

45 CFR Part 142 Security and Electronic Signature Standards; Proposed Rule, U.S. Department of Health and Human Services[3]

45 CFR, Parts 160-164 Standards for Privacy of Individually Identifiable Health Information; U.S. Department of Health and Human Services, Office of the Secretary[3]

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. **E 1869**

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 mental health or condition of an individual, the provision of

[1] This specification is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.22 on Health Information Transcription and Documentation.

Current edition approved June 10, 2002. Published July 2002. Originally published as E 1902–97. Last previous edition E 1902–97.

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

[3] 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

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. **E 1869**

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. **E 1869**

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 E 1985 and E 2085, and Specification E 2084.

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 E 1986 and E 1988.

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 E 1869. 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 information shall be transmitted by fax only when the sender and receiver take precautions to ensure that receipt will be by an authorized

receiver in a secure environment that will ensure that no unauthorized party may have access to it.

5.2.4 Dictation on analog audiocassettes, CDs, or other portable storage media shall be transported by express courier, or other secure rapid delivery services, that can track shipments. An authorized receiver shall be designated on the official shipping document. An authorized receiver shall sign for all shipments.

5.2.5 When transmitting voice data, dictation shall not be done or loaded into equipment with an activated auto answer, for example, answering machines or voice mail.

5.2.6 Once a voice file has been transcribed and the document has been received and verified by the healthcare provider in either electronic or paper form, the voice file shall be deleted from a digital system or erased from an analog system in a manner that prevents unauthorized access.

NOTE 1—Some contractual obligations may require retention. For further guidance, see Guide E 1959.

5.3 *Dictation Equipment Shall Be Protected from Unauthorized Access*:

5.3.1 Access to confidential information, records, tapes, and dictation, or any combination thereof, shall be limited to those authorized to be involved in the dictation process. All access privileges shall be limited to information related to an individual's role, and a log of access to data shall be maintained. For additional guidance regarding audit and disclosure logs, see Specification E 2147.

5.3.2 An individual authorized to dictate shall use unique identifiers to protect against inappropriate dictation system access. Formal documented procedures shall be in place to disable access by persons no longer authorized to use the system. User identifiers shall be unique to individuals and shall not be shared. Identifiers serve as a permanent record and shall not be reassigned to another individual.

5.3.3 Dictation equipment repairs, modifications, and maintenance shall be made only by authorized persons. A log of all repairs, modifications, and maintenance shall be maintained and include sufficient detail to allow for tracking of breaches of confidentiality or security. Individually identifiable information shall be deleted from dictation systems that are removed from facilities or from use.

5.4 Individually identifiable information shall be restricted to demographic sections of reports and shall not be included within the narrative portion of reports.

5.4.1 Individually identifiable information shall be removed from documents prior to access by researchers, statisticians, and others not responsible for healthcare. This shall include removal of the patient's name, employer, Social Security number, address, telephone number, names of relatives, and any other identifying information within the demographic or narrative portions of such reports. For further guidance as provided in the HIPAA Privacy Rule, see Public Law 104–191, section 164–514.

5.5 *Dictation Playback Shall Be Done in a Secure Environment*—Playback of dictation shall be done in a manner that protects the information from being overheard by unauthorized persons.

5.6 *Dictation Storage Shall Be Limited*:

5.6.1 Dictation shall be stored only for the length of time necessary to transcribe and review documentation and in a manner that protects against unauthorized access. Dictated healthcare information shall then be destroyed or deleted in a way that prevents recovery by unauthorized persons. Transcribed tapes shall not be reused until erased.

5.6.2 If original voice files are stored, precautions shall be taken to secure the files and to ensure that no unauthorized individual shall have or obtain access to them. If offsite storage is done, the policy for offsite storage, retention, access, destruction, and disposal shall be disclosed in writing and agreed upon by all involved parties.

6. Transcription Security Policies and Procedures

6.1 Security and confidentiality obligations shall be thoroughly explained at the time access privileges are granted, and understanding and agreement shall be acknowledged by signed statements that are reviewed and renewed periodically.

6.1.1 Individuals who perform medical transcription or who have access to healthcare documentation during the transcription process including, but not limited to, business owners, supervisors, managers, billing and file clerks, coders, proofreaders, students, vendors, equipment maintenance personnel, and couriers, 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 extended and at regularly scheduled reviews. Upon changes in policies or procedures, orientation and acknowledgment shall be repeated. Maintain a record of receipt of these statements in appropriate departmental files. For additional guidance, see Guides E 1986 and E 1988.

6.1.2 If medical transcription is done in a location other than that in which the patient is being treated (for example, offsite locally or in another state or country), disclosure of such arrangement shall be made to the healthcare provider organization. For additional guidance in this regard, see Guide E 1959.

6.1.3 After transcription is complete, it shall be authenticated by the medical transcriptionist's identifier. Note that the medical transcriptionist's authentication does not constitute authentication of the document, which must be done by the author. Access and authority to make changes on the transcript prior to its authentication by the author shall be limited and documented, including identification of the individual making such changes. Following authentication by the report's author, the document shall be released as a read-only file, and subsequent additions, corrections, or revisions shall be addenda to the document and shall likewise be authenticated. For additional guidance regarding authentication, see Guide E 1762. For additional guidance regarding amendments, see Guide E 2017 and Specification E 2184.

6.2 *Transcription Computer Systems, Storage Equipment, and Related Materials Shall Be Protected from Unauthorized Access*:

6.2.1 Access to equipment and materials containing confidential information shall be limited to those authorized to be

involved in the transcription process. All access privileges shall be limited to information related to an individual's role, and a log of access to data shall be maintained. For additional guidance regarding audit and disclosure logs, see Specification E 2147.

6.2.2 Individuals authorized to transcribe or access transcription for quality review, coding, analysis or other document processing functions shall use one or more unique identifiers to protect against inappropriate dictation and transcription system access. Formal documented procedures shall be in place to disable access by persons no longer authorized to use the system. User identifiers shall be unique to individuals and shall not be shared. Identifiers serve as a permanent record and shall not be reassigned to another individual.

6.2.3 Repairs, modification, and maintenance of transcription hardware and software and other transcription equipment shall be done only by authorized persons. A log of all repairs, modifications, and maintenance, whether performed on-site or remotely, shall be maintained and include sufficient detail to allow for tracking of breaches of confidentiality or security. Systems testing shall not be done with individually identifiable information. Individually identifiable information shall be deleted from transcription systems that are removed from facilities or from use.

6.3 *Medical Transcription Shall Be Done in a Secure Environment*—The environment in which medical transcription is done shall not be accessible to the public or unauthorized personnel. Computer monitors, printers, typewriters, and other equipment shall be located so that the individually identifiable material on them is not visible from windows, doors, or other open areas to reduce the risk of inappropriate viewing of confidential information.

6.4 *Transcriptionists Should Log Off Computers, Word Processors, and Dictation Equipment when not Transcribing*:

6.4.1 When not transcribing, reviewing, editing, etc., even for a short period of time, the medical transcriptionist shall log off all equipment that could permit unauthorized access to individually identifiable health information. If a pause feature is incorporated into the transcription system, this shall remove the documentation from view and access until the system is reactivated by the authorized user. Digital or other electronic dictation systems shall be logged off when medical transcriptionists are not physically present at their workstations.

6.4.2 When manual systems such as typewriters or analog transcribe machines are used, materials such as documents and tapes containing individually identifiable information shall be removed immediately when the equipment is not in use and protected from unauthorized access.

6.4.3 In many cases, medical transcription involves the use of accessory materials such as patient lists, handwritten reports or notes, printed test results, instruction manuals, lists of unique identifiers, and other materials that either include individually identifiable information or would facilitate access to dictation and transcription systems. These accessory materials shall also be protected from unauthorized access.

6.5 *Backup Copies of Documentation Shall Be Restricted*:

6.5.1 When healthcare documentation is backed up, retain the original and protect it in accordance with the applicable state and federal regulations. Restrict backup copies of such documentation as to retention time and accessibility, and protect them in accordance with the applicable state and federal regulations.

6.5.2 If offsite transcription backup is done, the policy for offsite storage, retention access, destruction, and disposal shall be disclosed in writing and agreed upon by all involved parties. For additional guidance, see Guide E 1959.

6.6 *Distribution of Healthcare Documents Shall Be Protected*:

6.6.1 When any electronic technology is used to distribute healthcare documentation, it shall be done in a secure manner appropriate to the technology and in accordance with state and federal regulations. Access shall be obtained by a unique identifier to protect against unauthorized access and inappropriate changes being made to documents.

6.6.2 Text files of individually identifiable healthcare documentation shall not be transmitted into equipment such as remote printers or fax machines unless sender and receiver take precautions to secure the data and to ensure that no unauthorized party may have or obtain access to it.

6.6.3 All individually identifiable health information stored on any form of portable storage media shall be encrypted and distributed directly to authorized personnel.

6.6.4 Healthcare documentation that is distributed by courier shall be secured in a locked opaque container and shall be distributed only to a prearranged authorized receiver. It shall not be dropped off in an unattended area, such as hallway or outside a door. Receipt shall be acknowledged.

6.6.5 The Internet, intranets, e-mail, and similar public media shall not be used to transmit or store healthcare documentation or other identifiable personal information unless sender and receiver agree that data will be transported and stored in this manner and adequate precautions, such as encryption of all voice and data files, have been taken to secure the data and to ensure that no unauthorized access is allowed. Protection of individually identifiable health information is paramount regardless of the technology used.

6.6.6 Individually identifiable healthcare documentation shall be transmitted by fax only when the sender and receiver take precautions to ensure that receipt will be by an authorized receiver in a secure environment that will ensure that no unauthorized party may have access to it.

6.7 *Transcription Storage and Retention*:

6.7.1 Transcription shall be stored only for the length of time necessary to complete, review, and correct documentation. The data contained on tapes, disks, digital storage, optical disks, CDs, microfiche, salvage utilities, and other media containing individually identifiable health information shall be carefully destroyed, erased, or deleted in a manner that prevents recovery by unauthorized persons. Transcribed tapes shall not be reused until erased.

6.7.2 Copies of individually identifiable health information shall not be retained any longer than necessary, and access during retention shall be restricted and documented. After documents have been distributed to the electronic health record or other system and have been appropriately backed up,

verified, and validated, they shall be permanently removed from the transcription system and no copies retained.

6.8 *Discarding or Destroying Paper*—Destruction of printed material containing individually identifiable health information shall be done in a manner that prevents recovery (for example, shredding).

6.9 *Release of Information is Restricted*—Except as authorized by institutional policies and procedures, and consistent with the law, medical transcriptionists shall not release healthcare information. If a transcriptionist is unsure as to whether the release of healthcare information is lawful or authorized, the information shall not be released and the request shall be referred to the appropriate authority.

6.10 *Medical Transcription Students*:

6.10.1 Medical transcription students or others who are serving externships or are participating in other on-the-job educational projects 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 maintain confidentiality by signing statements of understanding and agreement at the time that access privileges are granted and at regularly scheduled reviews. For additional guidance, see Guides E 1986 and E 1988.

6.10.2 Actual healthcare dictation, or reports, or both, shall not be used for education, testing, or demonstration purposes.

NOTE 2—Actual healthcare dictation or reports could be used for education, testing, or demonstration purposes, after all individually identifiable healthcare information has been removed, as provided in the HIPAA Privacy Rule. For additional guidance, see Public Law 104–191, section 164–514.

6.11 *Individually Identifiable Information Shall Be Restricted to Demographic Sections of Reports and Shall Not Be Included Within the Narrative Portion of Reports*:

6.11.1 Individually identifiable information shall be removed from documents prior to access by researchers, statisticians, and others not responsible for healthcare. This shall include removal of the patient's name, employer, Social Security number, address, telephone number, names of relatives, and any other identifying information within the demographic or narrative portions of such reports.

7. Keywords

7.1 confidentiality; dictation; documentation; individually identifiable health information; medical transcription; security

RELATED MATERIAL

ASTM Standard Guide E 1987 for Individual Rights Regarding Health Information[2]

ASTM Standard Guide E 2086 for Internet and Intranet Healthcare Security[2]