NOTICE: This standard has either been superseded and replaced by a new version or withdrawn.
Contact ASTM International (www.astm.org) for the latest information

Designation: E1762 – 95(Reapproved 2009)

An American National Standard

Standard Guide for Electronic Authentication of Health Care Information[1]

This standard is issued under the fixed designation E1762; 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:

1.1.1 Defining a document structure for use by electronic signature mechanisms (Section 4),

1.1.2 Describing the characteristics of an electronic signature process (Section 5),

1.1.3 Defining minimum requirements for different electronic signature mechanisms (Section 5),

1.1.4 Defining signature attributes for use with electronic signature mechanisms (Section 6),

1.1.5 Describing acceptable electronic signature mechanisms and technologies (Section 7),

1.1.6 Defining minimum requirements for user identification, access control, and other security requirements for electronic signatures (Section 9), and

1.1.7 Outlining technical details for all electronic signature mechanisms in sufficient detail to allow interoperability between systems supporting the same signature mechanism (Section 8 and Appendix X1-Appendix X4).

1.2 This guide is intended to be complementary to standards under development in other organizations. The determination of which documents require signatures is out of scope, since it is a matter addressed by law, regulation, accreditation standards, and an organization's policy.

1.3 Organizations shall develop policies and procedures that define the content of the medical record, what is a documented event, and what time constitutes event time. Organizations should review applicable statutes and regulations, accreditation standards, and professional practice guidelines in developing these policies and procedures.

2. Referenced Documents

2.1 *ISO Standards:*

ISO 9594-8 1993: The Directory: Authentication Framework (also available as ITU-S X.509)[2]

ISO 8825-1 1993: Specification of Basic Encoding Rules for ASN.1[2]

ISO 7816 1993: IC Cards with Contacts[2]

ISO 10036 1994: Contactless IC Cards[2]

2.2 *ANSI Standards:*

ANSI X9.30 Part 3: Certificate Management for DSA, November 1994 (ballot copy)[3]

ANSI X9.31 Part 3: Certificate Management for RSA, July 1994 (draft)[3]

ANSI X9.31 Part 1: RSA Signature Algorithm, July 1994 (ballot copy) (technically aligned with ISO/IEC 9796)[3]

ANSI X9.30 Part 1: Digital Signature Algorithm, July 1994 (ballot copy) (technically aligned with NIST FIPS PUB 186)[3]

ANSI X9F1, ANSI X9.45: Enhanced Management Controls Using Attribute Certificates, September 1994 (draft)[3]

2.3 *Other Standards:*

FIPS PUB 112: Standards on Password Usage, May 1985[4]

FIPS PUB 181: Secure Hash Standard, 1994 (technically aligned with ANSI X9.30–1)[4]

FIPS PUB 186: Digital Signature Standard, 1994 (technically aligned with ANSI X9.30–1)[4]

PKCS #1: RSA Encryption Standard (version 1.5), November 1993[5]

PKCS #5: Password-Based Encryption Standard, 1994[5]

PKCS #7: Cryptographic Message Syntax Standard, 1994[5]

3. Terminology

3.1 *Definitions:*

3.1.1 *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 *accountability*—the property that ensures that the actions of an entity may be traced uniquely to the entity.

3.1.3 *attribute*—a piece of information associated with the use of a document.

[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 April 1, 2009. Published September 2009. Originally approved in 1995. Last previous edition approved in 2003 as E1762–95 (2003). DOI: 10.1520/E1762-95R09.

[2] Available from ISO, 1 Rue de Varembe, Case Postale 56, CH 1211, Geneve, Switzerland.

[3] Available from American National Standards Institute (ANSI), 25 W. 43rd St., 4th Floor, New York, NY 10036, http://www.ansi.org.

[4] Available from National Institute of Standards and Technology (NIST), 100 Bureau Dr., Stop 1070, Gaithersburg, MD 20899-1070, http://www.nist.gov.

[5] Available from RSA Data Security, 100 Marine Parkway, Redwood City, CA 64065.

Copyright © ASTM International, 100 Barr Harbor Drive, PO Box C700, West Conshohocken, PA 19428-2959. United States

3.1.4 *attribute certificate*—a digitally signed data structure that binds a user to a set of attributes.

3.1.5 *authorization*—verification that an electronically signed transaction is acceptable according to the rules and limits of the parties involved.

3.1.6 *authorization certificate*—an attribute certificate in which the attributes indicate constraints on the documents the user may digitally sign.

3.1.7 *availability*—the property of being accessible and useable upon demand by an authorized entity.

3.1.8 *computer-based patient record (CPR)*—the computer-based patient record is a collection of health information concerning one person linked by one or more identifiers. In the context of this guide, this term is synonymous with electronic patient record and electronic health record.

3.1.9 *computer-based patient record system (CPRS)*—the CPRS uses the information of the CPR and performs the application functions according to underlying processes and its interacting with related data and knowledge bases. CPRS is synonymous with electronic patient record systems.

3.1.10 *data integrity*—the property that data has not been altered or destroyed in an unauthorized manner.

3.1.11 *data origin authentication*—corroboration that the source of data received is as claimed.

3.1.12 *digital signature*—data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, for example, by the recipient.

3.1.13 *document access time*—the time(s) when the subject document was accessed for reading, writing, or editing.

3.1.14 *document attribute*—an attribute describing a characteristic of a document.

3.1.15 *document creation time*—the time of the creation of the subject document.

3.1.16 *document editing time*—the time(s) of the editing of the subject document.

3.1.17 *domain*—a group of systems that are under control of the same security authority.

3.1.18 *electronic document*—a defined set of digital information, the minimal unit of information that may be digitally signed.

3.1.19 *electronic signature*—the act of attaching a signature by electronic means. After the electronic signature process, it is a sequence of bits associated with an electronic document, which binds it to a particular entity.

3.1.20 *event time*—the time of the documented event.

3.1.21 *one-way hash function*—a function that maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

3.1.21.1 It is computationally infeasible to find for a given output an input that maps to this output.

3.1.21.2 It is computationally infeasible to find for a given input a second input that maps to the same output.

3.1.22 *private key*—a key in an asymmetric algorithm; the possession of this key is restricted, usually to one entity.

3.1.23 *public key*—a key in an asymmetric algorithm that is publicly available.

3.1.24 *public key certificate*—a digitally signed data structure which binds a user's identity to a public key.

3.1.25 *repudiation*—denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.1.26 *role*—the role of a user when performing a signature. Examples include: physician, nurse, allied health professional, transcriptionist/recorder, and others.

3.1.27 *secret key*—a key in a symmetric algorithm; the possession of this key is restricted, usually to two entities.

3.1.28 *signature*—the act of taking responsibility for a document. Unless explicitly indicated otherwise, an electronic signature is meant in this guide.

3.1.29 *signature attribute*—an attribute characterizing a given user's signature on a document.

3.1.30 *signature purpose*—an indication of the reason an entity signs a document. This is included in the signed information and can be used when determining accountability for various actions concerning the document. Examples include: author, transcriptionist/recorder, and witness.

3.1.31 *signature time*—the time a particular signature was generated and affixed to a document.

3.1.32 *signature verification*—the process by which the recipient of a document determines that the document has not been altered and that the signature was affixed by the claimed signer. This will in general make use of the document, the signature, and other information, such as cryptographic keys or biometric templates.

3.1.33 *user authentication*—the provision of assurance of the claimed identity of an entity.

3.2 *Acronyms:*

AAMT	American Association for Medical Transcription
ABA	American Bar Association
AHIMA	American Health Information Management Association
AIM	Advanced Informatics in Medicine
ASC X3	Accredited Standards Committee X3
ASC X9	Accredited Standards Committee X9
ASC X12N	Accredited Standards Committee X12N
CA	Certification Authority
CEN	Comité Européen de Normalisation (European Standards Committee)
CLC	Comité Européen de Normalisation Electrotechnique (CENELEC)
CRL	Certificate Revocation List
DSA	Digital Signature Algorithm (NIST)
EWOS	European Workshop for Open Systems
ES	Electronic Signature
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standard
ISO	International Standards Organization
ITSTC	International Technology Steering Committee
JCAHO	Joint Commission on Accreditation of Healthcare Organizations
MAC	Message Athentication Code
NIST	National Institute for Standards and Technology
NTP	Network Time Protocol
PCMCIA	Personal Computer Memory Card Interface Association
RSA	Rivest-Shamir-Adleman (signature algorithm)

iTeh Standards (https://standards.iteh.ai) Document Preview
https://standards.iteh.ai/catalog/standards/sist/9c3fe282-1ed3-4f1f-8d7d-87faf6140eeb/astm-e1762-952009

SEISMED	Secure Environment for Information Systems in Medicine
THIS	Trusted Health Information Systems
TTP	Trusted Third Party

4. Significance and Use

4.1 This guide serves three purposes:

4.1.1 To serve as a guide for developers of computer software providing, or interacting with, electronic signature processes,

4.1.2 To serve as a guide to healthcare providers who are implementing electronic signature mechanisms, and

4.1.3 To be a consensus standard on the design, implementation, and use of electronic signatures.

5. Background Information

5.1 The creation of computer-based patient record systems depends on a consensus of electronic signature processes that are widely accepted by professional, regulatory, and legal organizations. The objective is to create guidelines for entering information into a computer system with the assurance that the information conforms with the principles of accountability, data integrity, and non-repudiation. Although various organizations have commenced work in the field of electronic signatures, a standard for the authentication of health information is needed. Consequently, this standard is intended as a national standard for electronic signatures for health care information. Technological advances and increases in the legitimate uses and demands for patient health information led the Institute of Medicine (IOM) to convene a committee to identify actions and research for a computer-based patient record (CPR). The committee's report endorsed the adoption of the CPR as the standard for all health care records and the establishment of a Computer-based Patient Record Institute (CPRI). National Information Infrastructure initiatives, the ever increasing complexity of health care delivery, a growing need for accessible, affordable, and retrievable patient data to support clinical practice, research, and policy development support this recommendation. Major issues identified by CPRI as essential to the timely development of CPRs include authentication of electronic signatures (as replacements for paper signatures), as well as patient and provider confidentiality and electronic data security.

5.2 User authentication is used to identify an entity (person or machine) and verify the identity of the entity. Data origin authentication binds that entity and verification to a piece of information. The focus of this standard is the application of user and data authentication to information generated as part of the health care process. The mechanism providing this capability is the electronic signature.

5.3 Determination of which events are documented and which documents must be signed are defined by law, regulation, accreditation standards, and the originating organization's policy. Such policy issues are discussed in Appendix X4.

5.4 Signatures have been a part of the documentation process in health care and have traditionally been indicators of accountability. Health care providers are faced with the inevitable transition toward computerization. For electronic health record systems to be accepted, they must provide an equivalent or greater level of accurate data entry, accountability, and appropriate quality improvement mechanisms. In this context, a standard is needed that does not allow a party to successfully deny authorship and reject responsibility (repudiation).

5.5 The guide addresses the following requirements, which any system claiming to conform to this guide shall support:

5.5.1 Non-repudiation,

5.5.2 Integrity,

5.5.3 Secure user authentication,

5.5.4 Multiple signatures,

5.5.5 Signature attributes,

5.5.6 Countersignatures,

5.5.7 Transportability,

5.5.8 Interoperability,

5.5.9 Independent verifiability, and

5.5.10 Continuity of signature capability.

5.6 Various technologies may fulfill one or more of these requirements. Thus, a complete electronic signature system may require more than one of the technologies described in this guide. Currently, there are no recognized security techniques that provide the security service of non-repudiation in an open network environment, in the absence of trusted third parties, other than digital signature-based techniques.

5.7 The electronic signature process involves authentication of the signer's identity, a signature process according to system design and software instructions, binding of the signature to the document, and non-alterability after the signature has been affixed to the document. The generation of electronic signatures requires the successful identification and authentication of the signer at the time of the signature. To conform to this guide, a system shall also meet health information security and authentication standards. Computer-based patient record systems may also be subject to statutes and regulations in some jurisdictions.

5.8 While most electronic signature standards in the banking, electronic mail, and business sectors address only digital signature systems, this standard acknowledges the efforts of industry and systems integrators to achieve authentication with other methods. Therefore, this standard will not be restricted to a single technology.

6. Document Structure

6.1 For any data or information for which authentication is required, the system shall:

6.1.1 Provide to the signer an accurate representation of the health care information being signed,

6.1.2 Append one or multiple signatures,

6.1.3 Include, with each signature, information associated with the signer (that is, signature attributes and possibly unsigned attributes), and

6.1.4 Append zero or more document identifiers and attributes associated with the document.

6.2 A document therefore consists of the health care information, one or more signatures with corresponding signature attributes, and, when desired, one or more document attributes. A user's signature then applies to the health care information, the document attributes, and that user's signature attributes.

iTeh Standards (https://standards.iteh.ai) Document Preview
ASTM E1762-95(2009)
https://standards.iteh.ai/catalog/standards/sist/1ed5...7d-841af6140eeb/astm-e1762-952009

The signer need not be accountable for those document attributes supplied by the system, but they are rendered non-alterable by the signature process. The verifier must be made aware of which document attributes the signer takes responsibility for. This might be done via bilateral agreements or other contractual arrangements, or it might be signalled explicitly as part of the signer's signature attributes.

6.3 This guide describes the physical representation of one or more of the document components when presented to the signature mechanism. This does not imply that the document must be stored, transmitted, or otherwise manipulated using this representation at any time other than signature processing.

6.4 This guide does not put any explicit restrictions on the type or format of the health information content. Health information may be of a particular type, or may be a combination of several information types, for example:

6.4.1 Numeric data (either encoded, or not),

6.4.2 Text,

6.4.3 Graphic,

6.4.4 Images, for example, scanned documents, and clinical digital images,

6.4.5 Audio,

6.4.6 Video, and

6.4.7 Waveforms.

6.5 It is expected that the internal structure of the health information content, while not visible to the electronic signature mechanism, will be defined in other standards.

6.6 Document attributes allow a cataloguing and or interpretation of the content of a document according to a standard without having to examine the health information content itself.

6.7 Policies, procedures, and other standards of the originator and recipient will dictate which attributes are required in various documents and applications (see Appendix X4). The scope of accountability for a given document, in terms of each individual signatory, relates to the combined set of document content, document attributes, and signature attributes visible (that is, displayed or otherwise accessible) to the user at the time the signature is applied. This information may be conveyed between originator and recipient as part of bilateral agreements or trade practice.

6.8 The system shall support the presence of at least the following attributes:

6.8.1 Document creation time,

6.8.2 Document type information, which may be hierarchical,

6.8.3 Event time (user or system assigned),

6.8.4 Document modification and access times,

6.8.5 Location of origin,

6.8.6 Data type(s),

6.8.7 Data format(s), including character sets,

6.8.8 Originating (source) organization,

6.8.9 Patient identifier,

6.8.10 Event type, and

6.8.11 Document identifier.

6.9 Although this guide does not specify the structure of a document identifier, it shall convey sufficient information to locate and retrieve the document, including the originating organization identifier, originating system or application identifier, a document serial number assigned by the application, and (if needed) a revision number. The document identifier is also used as a signature attribute to link related documents, as described in Section 8.

6.10 The electronic signature model discussed in Sections 7-9 requires the ability to attach multiple signatures to a document, as well as the ability to include per-signer information in the signature process.

6.11 Note that a combination of signatures with various purposes (see Section 6) may be required for a document to be accepted by the recipient. For example, a transcriptionist/recorder signature by itself would likely not be sufficient for a document to be accepted. Appendix X1 discusses the use of authorization certificates to indicate which combinations of signatures are considered acceptable by a particular originating system. It also discusses mechanisms for representing the rules used to determine these signature requirements in a data structure called an authorization certificate.

7. Electronic Signature Requirements

7.1 The electronic signature uniquely identifies the signer and ensures the signed document was not modified after the signature was affixed. If the signed document is converted to another format (for example, between various image formats), the electronic signature applies only to the original format.

7.2 The electronic signature process, at an abstract level, consists of two operations, each of which has several characteristics or components.

7.2.1 Signing of a document has the following three components:

7.2.1.1 Secure user authentication (proof of claimed identity) of the signer, at the time the signature is generated,

7.2.1.2 Creation of the logical manifestation of signature, and

7.2.1.3 Ensuring the integrity of the signed document.

7.2.2 Verifying a signature on a document has the following two components:

7.2.2.1 Verifying the integrity of the document and associated attributes, and

7.2.2.2 Verifying the identity of the signer.

7.3 This leads to several general requirements, as well as requirements that are specific to one of these components. All of these requirements shall be met by systems claiming to implement electronic signatures for health care authentication.

7.3.1 *General Requirements:*

7.3.1.1 *Non-repudiation*— Proof (to a third party) that only the signer could have created a signature. Non-repudiation cannot be ensured until the completion of the applicable dispute resolution process. This process may be influenced by agreements between the signer and verifier (for example, trading partner agreements or system rules), and such agreements would implicate the appropriate technologies that could be used to provide electronic signatures.

iTeh Standards (https://standards.iteh.ai) Document Preview
ASTM E1762-95(2009) https://standards.iteh.ai/catalog/standards/sist/...-bd7d-841af6140eeb/astm-e1762-952009

7.3.1.2 *Integrity*—After a signature has been affixed, any change in the information will cause the signature verification process to detect that the information has been changed. Action taken as a result of this discovery is dependent on a number of factors, including the purpose of the signature, and might include rejection of the document, forwarding to some (human) user for manual review, etc.

7.3.2 *User Authentication Requirements:*

7.3.2.1 *Secure User Authentication* —The act of signing shall include a secure means of proving the signer's identity. Relevant technologies include the use of biometrics (fingerprints, retinal scans, handwritten signature verification, etc.), tokens, or passwords (if implemented in conformance with appropriate guidelines). The type and frequency of user authentication (for example, authentication at logon versus authentication every time a signature is applied) is determined by the rules and security policy of the signer's organization. Examples of such policies might include: (*1*) explicit user authentication at system access and explicit user authentication at signature time for each document (that is, each document requires a formal signature action or process) and (*2*) explicit user authentication at system access but thereafter implicit (that is, each document requires formal review/acceptance but not a formal signature action or process).

7.3.3 *Logical Manifestation Requirements:*

7.3.3.1 *Multiple Signatures*—It shall be possible for multiple parties to sign a document. Multiple signatures are, conceptually, simply appended to the document. Fig. 1 illustrates a document with a single signature attached. Fig. 2 illustrates a document with an additional signature attached.

7.3.3.2 *Signature Attributes*—It shall be possible for a signer to supply additional information (for example, timestamp, signature purpose), specific to that user, in the signed data. That is, the signed data consists of at least the document and the particular signer's signature attributes.

7.3.3.3 *Countersignatures*—It shall be possible to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where some party signs a document which has already been signed by another party. See Fig. 3.

7.3.4 *Verification Requirements:*

7.3.4.1 *Transportability*— The signed document can be transported (over an insecure network) to another system, while maintaining the integrity of the document, including content, signatures, signature attributes, and (if present) document attributes.

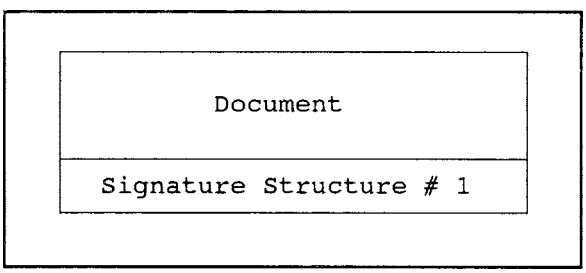

FIG. 1 Single Signature

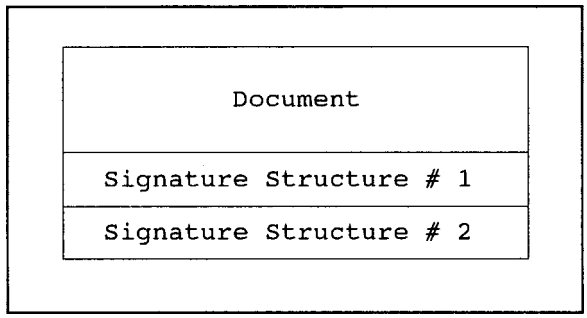

FIG. 2 Multiple Signatures

7.3.4.2 *Interoperability*— The signed document can be processed by a recipient, while maintaining the integrity of the document, including content, signatures, signature attributes, and (if present) document attributes.

7.3.4.3 *Independent Verifiability*—It shall be possible to verify the signature without the cooperation of the signer.

7.3.4.4 *Continuity of Signature Capability*—The public verification of a signature shall not compromise the ability of the signer to apply additional secure signatures at a later date.

8. Signature Attributes

8.1 Signature attributes identify characteristics about the signature and the signer. The signature attributes include:

8.1.1 Signature purpose,

8.1.2 Signature sub-purpose (for use with the addendum Signature),

8.1.3 Signature time,

8.1.4 Location,

8.1.5 Signer's identity,

8.1.6 Signer's role,

8.1.7 Signer's organization,

8.1.8 Document link,

8.1.9 Biometric information,

8.1.10 Annotation, and

8.1.11 Other attributes, as defined by organizations or other standards.

8.1.12 Signature time and signer identity are mandatory attributes; the others may be optional in a given application or signed document, depending on the originating organization's security policy.

8.1.13 The signer identity may be implicit in some cases. For example, when using digital signatures, it may be the identity contained in a certificate used to verify the signature.

8.2 *Health Information Electronic Signature Purposes:*

8.2.1 The following signature purposes shall be supported under this guide:

8.2.1.1 Author's signature,

8.2.1.2 Coauthor's signature,

8.2.1.3 Co-participant's signature,

8.2.1.4 Transcriptionist/Recorder signature,

8.2.1.5 Verification signature,

8.2.1.6 Validation signature,

8.2.1.7 Consent signature,

8.2.1.8 Witness signature,

8.2.1.9 Event witness signature,

iTeh Standards (https://standards.iteh.ai) Document Preview
ASTM E1762-95(2009)
https://standards.iteh.ai/catalog/standards/sist/9c3fe282-1ed3-4...140eeb/astm-e1762-952009

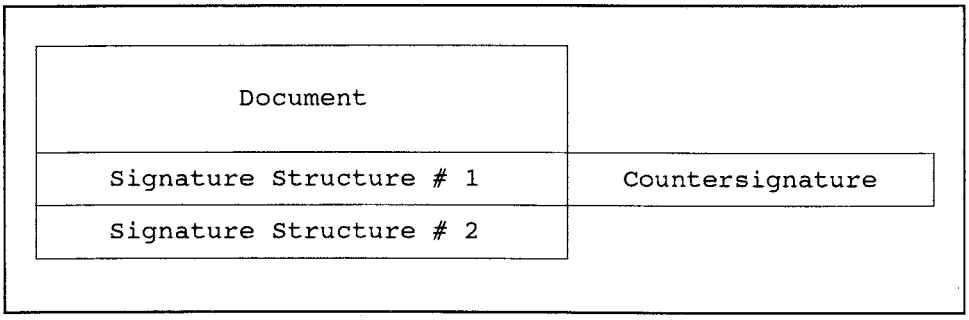

FIG. 3 Countersignatures

8.2.1.10 Identity witness signature,
8.2.1.11 Consent witness signature,
8.2.1.12 Interpreter signature,
8.2.1.13 Review signature,
8.2.1.14 Source signature,
8.2.1.15 Addendum signature,
8.2.1.16 Administrative signature,
8.2.1.17 Timestamp signature, and
8.2.1.18 Other.

8.2.2 Each of these signature types can be executed by multiple user types. Any definition rules as to user type and signature type should be system configurable and not be part of the digital signature standard.

8.2.2.1 *Author's Signature*—the signature of the primary or sole author of a health information document. There can be only one primary author of a health information document.

8.2.2.2 *Coauthor's Signature*—the signature of a health information document coauthor. There can be multiple coauthors of a health information document.

8.2.2.3 *Co-participant's Signature* —the signature of an individual who is a participant in the health information document but is not an author or coauthor. (*Example*—a surgeon who is required by institutional, regulatory, or legal rules to sign an operative report, but who was not involved in the authorship of that report.)

8.2.2.4 *Transcriptionist/Recorder Signature*—the signature of an individual who has transcribed a dictated document or recorded written text into a digital machine readable format.

8.2.2.5 *Verification Signature*—a signature verifying the information contained in a document. (*Example*—a physician is required to countersign a verbal order that has previously been recorded in the medical record by a registered nurse who has carried out the verbal order.)

8.2.2.6 *Validation Signature*—a signature validating a health information document for inclusion in the patient record. (*Example*—a medical student or resident is credentialed to perform history or physical examinations and to write progress notes. The attending physician signs the history and physical examination to validate the entry for inclusion in the patient's medical record.)

8.2.2.7 *Consent Signature*—the signature of an individual consenting to what is described in a health information document.

8.2.2.8 *Signature Witness Signature* —the signature of a witness to any other signature.

8.2.2.9 *Event Witness Signature*—the signature of a witness to an event. (*Example*—the witness has observed a procedure and is attesting to this fact.)

8.2.2.10 *Identity Witness Signature* —the signature of an individual who has witnessed another individual who is known to them signing a document. (*Example* —the identity witness is a notary public.)

8.2.2.11 *Consent Witness Signature*—the signature of an individual who has witnessed the health care provider counselling a patient.

8.2.2.12 *Interpreter Signature*—the signature of an individual who has translated health care information during an event or the obtaining of consent to a treatment.

8.2.2.13 *Review Signature*— the signature of a person, device, or algorithm that has reviewed or filtered data for inclusion into the patient record. (*Examples:* (*1*) a medical records clerk who scans a document for inclusion in the medical record, enters header information, or catalogues and classifies the data, or a combination thereof; (*2*) a gateway that receives data from another computer system and interprets that data or changes its format, or both, before entering it into the patient record.)

8.2.2.14 *Source Signature*— the signature of an automated data source. (*Examples:* (*1*) the signature for an image that is generated by a device for inclusion in the patient record; (*2*) the signature for an ECG derived by an ECG system for inclusion in the patient record; (*3*) the data from a biomedical monitoring device or system that is for inclusion in the patient record.)

8.2.2.15 *Addendum Signature*—the signature on a new amended document of an individual who has corrected, edited, or amended an original health information document. An addendum signature can either be a signature type or a signature sub-type (see 8.1). Any document with an addendum signature shall have a companion document that is the original document with its original, unaltered content, and original signatures. The original document shall be referenced via an attribute in the new document, which contains, for example, the digest of the old document. Whether the original, unaltered, document is always displayed with the addended document is a local matter, but the original, unaltered, document must remain as part of the patient record and be retrievable on demand.

8.2.2.16 *Modification Signature*—the signature on an original document of an individual who has generated a new amended document. This (original) document shall reference

iTeh Standards (https://standards.iteh.ai) Document Preview
ASTM E1762-95(2009)
https://standards.iteh.ai/catalog/standards/sist/e3fe7d22-1ed3-4001-bd1c-841af6140eeb/astm-e1762-952009