Designation: E 1762 – 95 (Reapproved 2003)

An American National Standard

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

This standard is issued under the fixed designation E 1762; 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.

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.

[1] This guide is under the jurisdiction of ASTM Committee E-31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.20 on Authentication of Computer-Based Health Information.

Current edition approved May 10, 2003. Published July 2003. Originally approved in 1995. Last previous edition approved in 1995 as E 1762–95.

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

[3] Available from American National Standards Institute, 11 W. 42nd St., 13th Floor, New York, NY 10036.

[4] Available from NIST, Gaithersburg, MD 20899.

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

This document is now PUBLIC

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