



## Managing Information Privacy & Security in Healthcare

### Setting Standards in Healthcare Information

By Margret Amatayakul, MBA, RHIA, FHIMSS

#### Introduction

Currently, questions of health information privacy and security are of utmost importance in the United States. Hardly a day goes by that *The Washington Post*, *The New York Times*, or *USA Today* do not feature an article about some aspect of medical privacy. Opinion polls document that the American public regards the data management practices of most large organizations with great skepticism. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) created specific requirements for the Congress and the Department of Health and Human Services (HHS). Because of HIPAA, the legal and regulatory environment for managing patient medical records has dramatically changed. HHS has published regulations for managing health information privacy and security. Most providers, health plans and healthcare clearinghouses must comply with these regulations. In addition to these federal efforts, many states have passed medical privacy laws. Standards-setting and professional regulatory organizations have been busy addressing the problems of medical privacy and the security of healthcare information from their own perspectives. The European Union is also pressuring the United States government and American corporations to change their approaches to privacy on pain of embargoes against exportation of personal information about Europeans to the USA.

The HIMSS P&S Toolkit contains summaries and explanations of the HHS privacy and security rules, the HHS model medical privacy provisions, information about state laws on medical privacy, and a thorough explanation of the standards-setting process in medical informatics. As an example of how two important standards-setting organizations in healthcare are beginning to incorporate demands for adequate data security practices into their evaluation criteria, the Joint Commission on the Accreditation of Healthcare Organizations and the National Committee on Quality Assurance have permitted the reprinting of the Executive Summary of Protecting Personal Health Information: *A Framework for Meeting the Challenges in a Managed Care Environment*. A discussion of the European Privacy Directive concludes this chapter.

#### Security Standards

This section provides an introduction to standards development, an overview of information systems standards in general and as they relate specifically to healthcare, a summary of the frameworks under development for healthcare information systems security standards, including HIPAA regulations, and brief descriptions of the major information system security standards efforts and standards themselves that may be applicable to the healthcare industry.

See the glossary of acronyms and Internet addresses at the end of the toolkit for additional information on all organizations referenced in this section.

### **Introduction to Standards**

A standard is defined as "something established by authority, custom, or general consent as a model or example." When used as an adjective, the definition includes "conforming to a standard as established by law or custom [which is] sound and usable." These definitions suggest that standards establish a set of requirements, processes, procedures, terms, options, or arrangements of objects that come into existence by common usage or a formal process and provide uniformity and constancy at a baseline level of acceptance.

The American National Standards Institute (ANSI) is a private, nonprofit organization that coordinates formal voluntary consensus standards activities in the United States and approves American National Standards. Members of ANSI include more than 1,000 companies, 30 government agencies, and more than 250 professional, technical, trade, labor, and consumer organizations. The organization ensures that a single set of nonconflicting national standards are developed by ANSI-accredited standards development organizations (SDOs) and that all interests concerned have the opportunity to participate in the development process. All ANSI approved standards also must undergo regular review and revision. ANSI has approved more than 11,000 standards in five major categories: dimensions, ratings, terminology and symbols, test methods, and performance and safety requirements. (For more information about ANSI, see [www.ansi.org](http://www.ansi.org).) ANSI is the sole representative and member of the two major nontreaty international standards organizations: the International Organization for Standardization (ISO) (see: [www.iso.ch](http://www.iso.ch)) and the International Electrotechnical Commission (IEC).

Standards also may be developed in professional societies, trade associations, government agencies, and industry consortia or may simply come about by common usage. The American Medical Association's CPT-4 procedural descriptions and codes are an example of a standard developed by a professional society. Microsoft has dominated the personal computer operating system market to such an extent that its products have become standard through common usage.

### **Information Systems Standards**

For information systems in general, the Open Systems Interconnection (OSI) reference model (shown in Figure 1) is designed to organize standards within seven layers to ensure that devices and software from different suppliers work together. Standards address many functions, such as capacity, transmission rates, protocols, and security. While very few systems are fully OSI compliant, the model is useful for the structure of layers it introduces. Standards at the lower layers are not industry specific. For example, hardware encryption devices may be used in banking and healthcare. Standards become more specific to the industry as they address the higher layers, especially the applications layer. As security standards are more fully described in this section, the reference model will be used to identify where each type of security standard is applicable.

### **Healthcare Information Systems Standards**

In healthcare, several organizations develop standards relating to the healthcare information application level. Some of these are ANSI-accredited and others are professional societies, trade

associations, industry consortia, etc. The ANSI Healthcare Informatics Standards Board (HISB) has been created within ANSI to help coordinate and promote adoption of standards relating to healthcare information system applications (see [web.ansi.org/](http://web.ansi.org/)). Examples of organizations that participate in ANSI HISB are depicted in Figure 2.

On August 21, 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) which included an Administrative Simplification section requiring the use of standards for electronic healthcare transactions, addressed the need for privacy legislation, and called for recommendations concerning standards for medical record information. Specifically, HIPAA required the Department of Health and Human Services to adopt standards that have been developed by an ANSI-accredited SDO, unless no standard had been developed or another standard would significantly reduce administrative costs and as promulgated in accordance with "negotiated rulemaking" procedures. (Information about the administrative simplification requirements can be found at <http://aspe.os.dhhs.gov/admnsimp/>.)

### **Healthcare Information Systems Security Standards Frameworks**

Healthcare information systems security standards are critical for ensuring the confidentiality and integrity of private health information.

Privacy determines who should have access, what constitutes the patient's rights to confidentiality, and what constitutes inappropriate access to health records. In the United States today, privacy law exists in state statutes, but there is no comprehensive federal privacy law. HIPAA called for the Secretary of Health and Human Services (HHS) to submit recommendations to Congress "on standards with respect to the privacy of individually identifiable health information," and that was done on September 11, 1997. (The recommendations are available at <http://aspe.os.hhs.gov/admnsimp/pvcrec0.htm>.) Congress had until August 21, 1999, to pass privacy legislation pursuant to HIPAA; otherwise, the Secretary was mandated to issue privacy regulations by August 21, 2000. Because Congress failed to enact privacy legislation by the self-imposed deadline, the Secretary of HHS issued Notice of Proposed Rule Making on November 3, 1999. The comment period closed on January 3, 2000. It should be noted that the proposed privacy rules are related exclusively to electronic transactions—which is all HIPAA will permit. Many would like to see federal privacy legislation extended to all health information.

Security is embodied in standards and technology that enable confidentiality of healthcare information and health data integrity policies to be carried out. Figure 3 demonstrates the relationship among the concepts of privacy, confidentiality and data integrity, and security and their embodiment in law, policy, and standards.

Several healthcare informatics SDOs are developing frameworks for healthcare security service mechanisms to protect against security threats.

### **Security Threats**

ASTM was organized in 1898 as the American Society for Testing and Materials and has grown into one of the largest SDOs in the world. It is a not-for-profit organization that provides a forum for producers, users, ultimate consumers, and those have a general interest to meet on common ground and write standards for materials, products, systems, and services. ASTM Committee E-31

on Healthcare Informatics was established in 1970 as an ANSI-accredited committee to develop standards for health information and health information systems. Current standards address architecture, content, portability, format, privacy, security, and communication of healthcare information. ASTM's Provisional Standard (PS 101) "Guidelines for a Technical Security Framework for Transmission and Storage of Healthcare Information" identifies the following security threats relative to healthcare information:

- Masquerade, in which one entity pretending to be another entity, facilitating the following other attacks.
- Modification of information, including message or data content, destruction of messages, data or management information.
- Message sequencing threats, including replay, pre-play, and delay of messages.
- Unauthorized disclosure, which reveals to an unauthorized user message content, information derived from observing message flow, and information held in storage on an open system.
- Repudiation, in which a user or system denies having performed some action, such as modification of information.
- Denial of service - prevents the systems from performing its functions.

### **HL7 Security Exposures**

HL7 (Health Level Seven) was founded in 1987 to develop standards for the electronic interchange of clinical, financial, and administrative information among independent healthcare-oriented computer systems (e.g., hospital information systems, clinical laboratory systems, enterprise systems, and pharmacy systems). In June of 1994, HL7 was designated by ANSI as an ANSI-accredited standards developer. HL7, in its draft Security Services Framework, categorizes healthcare information security exposures in the following manner:

#### **Disclosure**

Exposure  
Interception  
Inference Intrusion

#### **Deception**

Masquerade  
Falsification  
Repudiation

#### **Disruption**

Incapacitation  
Corruption  
Obstruction

## **Usurpation**

Misappropriation

## **Misuse**

HL7 further references the Crisis Emergency Response Team (CERT) for specific instances of some of these security failures (see: [www.cert.org/](http://www.cert.org/)).

## **Security Services**

Security services are defined in the HL7 and ASTM references as:

- Identification and Peer Entity Authentication, which provides proof of the identity of communicating parties, primarily through digital signatures or other cryptographic integrity mechanisms.
- Data Origin Authentication, which provides corroboration that the source of data is received as is claimed, and is also provided using digital signatures or other cryptographic means.
- Authorization and Access Control, which supports the granting of rights to access and the prevention of unauthorized use of resources. This is accomplished through digital signatures and access control lists that identify entities and their access rights that may be context-based, role-based, and/or user-based and provide for mandatory, discretionary, time-of-day, classification, and/or subject-object separation access.
- Confidentiality, which ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes. Encryption is used to provide this service and may include selective field confidentiality, which generally requires modification of existing message structures or encapsulation of the entire message for complete confidentiality. Key escrow also provides for confidentiality.
- Integrity, which ensures that data or system software have not been undetectably altered or destroyed in an unauthorized manner or by unauthorized users. This can be provided by various integrity check values.
- Nonrepudiation, which provides proof of origin or receipt that will protect against an originator or recipient falsely denying responsibility for the action. This protection is afforded through use of a digital signature and encryption.

## **Security Mechanisms**

HL7 also identifies additional security mechanisms relating to administrative and physical aspects of security:

- Accountability refers to tracing of actions of an individual or entity so that responsibility can be determined. Audit trails, logs, and receipts are examples of means to provide accountability.

- Availability ensures that information is accessible and usable upon demand by an authorized entity. Availability is the result of appropriate security services and data capture policies.
- Administration is the management of security policy, including the existence of physical and environmental security, disaster planning and recovery, personnel security, training and awareness, information technology facilities management, authentication and access control, database security, system maintenance, and legislation compliance. These guidelines were drawn from the Computer-based Patient Record Institute's *Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Records* (CPRI, January 1996 and see Chapter 4 below) and *Security Features for Computer-based Patient Record Systems* (CPRI, September 1996 and see Chapter 4 below) ([www.cpri-host.org](http://www.cpri-host.org)), as well as work performed by the Secure Environment for Information Systems in Medicine (SEISMED) project (see: [www.semper.org/sirene/projects/seismed/](http://www.semper.org/sirene/projects/seismed/)).

### Security Service Standards

The table below summarizes the standards that exist for the technical security services identified by ASTM (from ASTM's Provisional Standard [PS 101]) *Guidelines for a Technical Security Framework for Transmission and Storage of Healthcare Information*. Many of the standards that supply the healthcare-specific information security service framework were not developed for healthcare specifically, and few healthcare security standards have been written until recently. While confidentiality of private health information has always been a concern in healthcare, special measures were not considered necessary when it was believed that only authorized personnel had access to paper records.

### ASTM Healthcare Information Security Framework

	Link	Sub-network	End-to-end	Application (Session-oriented)	Application (Store and forward)
Authentication (peer entity)	None	IPSEC	IPSEC	FIPS 196, SPKM	PKCS-7
Authentication (data origin)	SILS	IPSEC	IPSE	SSL, SPKM	PKCS-7
Authorization and access control	N/A	IPSEC	IPSEC	Draft standard in ASTM E31	Draft standard in ASTM E31
Integrity	SILS	IPSEC	IPSEC	SSL, SPKM	PKCS-7

Confidentiality	SILS	IPSEC	IPSEC	SSL, SPKM	PKCS-7
Nonrepudiation	N/A	N/A	N/A	ASTM E1762, Draft standard in ASTM E31 S-HTTP	ASTM E1762 Draft standard in ASTM E31

### National Research Council Findings

In 1995, the National Library of Medicine, as one of the lead agencies within the government for facilitating healthcare applications of the national information infrastructure, identified privacy and security as primary issues that needed to be addressed to facilitate greater use of information technology within healthcare. As a result, the National Research Council (NRC) initiated a study to observe and assess existing technical and non-technical mechanisms for protecting the privacy and maintaining the security of healthcare information systems. The report, *For the Record: Protecting Electronic Health Information*, published by the National Academy Press in 1997, revealed serious inadequacies in how healthcare providers were safeguarding their healthcare information. It recommended several security procedures for immediate adoption, including:

- Individual authentication of users in which every individual has a unique username and password for access and is held accountable for all actions taken while logged on.
- Access controls to allow viewing of clinical information on a need-to-know basis.
- Audit trails to log all accesses to information so they're available for patient and clinician review on demand.
- Physical security and disaster recovery encompass positioning of computer terminals where unauthorized users cannot view displays, denial of access to paper printouts and electronic storage by unauthorized personnel, and the use of frequent backup tapes housed off-site.
- Protections of remote access points, or firewalls that should be implemented and all remote accesses protected by single session or encrypted passwords.
- Protection of external electronic communications requires all patient-identifiable data transmitted over public networks to be encrypted.
- Software discipline, the installation of virus-checking programs and limitations on downloads from the Internet on all servers.
- System assessment, or audits that should be performed on a monthly basis to examine vulnerability to password-cracking programs and to verify procedures implemented to detect system vulnerabilities.

For future adoption, the NRC report recommended:

- Strong authentication in the form of "hardware tokens."
- Enterprise-wide authentication, wherein users may authenticate once and have access to all relevant systems in an enterprise.
- Access validation, where both system function and content detail should be controlled by role.
- Expanded audit trails that provide a consolidated audit for all software.
- Electronic authentication of record, an electronic signature for "signing" medical records and cryptographic digital signature for retrieving records.

*For the Record: Protecting Electronic Health Information* is available online at <http://www.nap.edu/books/0309056977/html/index.html>

### **HIPAA's Security Regulations**

HIPAA's security regulations reflect the recommendations of the NRC report and the work of the SDOs to establish a security framework. Security regulations will apply to claims clearinghouses, health plans, employers, and healthcare providers that maintain or transmit automated health information. The proposed HIPAA Security Rule was published in the Federal Register on August 12, 1998. The final rule adopting HIPAA standards for security was published in the Federal Register on February 20, 2003. (see: [http://www.cms.hhs.gov/SecurityStandard/02\\_Regulations.asp#TopOfPage](http://www.cms.hhs.gov/SecurityStandard/02_Regulations.asp#TopOfPage)). The standards to safeguard data integrity, confidentiality, and availability of a healthcare entity's electronic data are categorized in HIPAA's security matrix as:

- Administrative safeguards - documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relationship to the protection of data.
- Physical safeguards - protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Covers use of locks, keys, and administrative measures to control access to computer systems.
- Technical security services - processes to protect and to control and monitor information access.
- Technical security mechanisms - processes to prevent unauthorized access to data that are transmitted over a communications network.

Recognizing that an industry consensus on security standards did not yet exist, the regulations are intended to establish a flexible framework for security practices that meet the goals of security without prescribing the means. Definition and penalties for wrongful disclosure of individually

identifiable health information were also included in the proposed rules, as was a section on electronic signature, which requires use of a digital signature if an electronic signature is to be used.

### **Security Standards for Healthcare Information Systems**

The proposed HIPAA Security Rule Matrix mapped some 55 documents to the various security requirements and methods of implementation in the proposed regulations. While the documents are illustrative and not all standards, they are an appropriate starting point for summarizing the standards that may be appropriately applied to protect healthcare information. The following list of standards and other documents has been arranged in general by OSI level and then by organization. It should be understood, however, that a number of the standards have evolved from proprietary standards, to ANSI-accredited (United States) standards, to international standards. Every effort has been made to categorize the standard according to the organization currently responsible for its maintenance as well as to reference it to other designations. Also included are works that are not standards, but which are applicable reference material for the domain.

### **United States General Security Standards**

There are a number of standards groups, industry consortia, government agencies, and vendors that have developed security standards at the lower OSI layers. The following are referenced in the proposed HIPAA Administrative Simplification security matrix and/or other standards: **ANSI X3S3.3** - An ANSI-accredited standards committee for the development of standards for lower layers, **X3.92 Data Encryption Standard (DES)**, is the most well known in the security arena. **DES - Data Encryption Standard** was developed by IBM in the 1960s for the U.S. Department of Defense and was subsequently published as ANSI X3.92. It is also available as **NIST, FIPS PUB 46-2**. It is sometimes referred to as **DEA** (data encryption algorithm). It is a symmetrical key system for use at the physical, or data link (for LANs) layer over asynchronous lines. DES has generally been considered adequate for most practical commercial purposes, but not sufficiently secure for top-secret applications. As computer power increases, however, the length of the key has become an issue. (See discussion under RSA.) The main drawback of DES, however, is in exchanging the keys and keeping them secure because the same key is used to encrypt and decipher the message, thus it is unsuitable for communicating with unidentified, untrusted parties. Public key algorithms that are asymmetrical are more suitable for such communications.

**ANSI X9F1** - ANSI has approved as American National Standards a number of standards for the Public-Key Infrastructure (PKI). Many of these had their origins in proprietary standards developed by industry. Many of the standards have also been approved as ISO standards. (For information about X9F1, see [www.csrc.nist.gov/pki](http://www.csrc.nist.gov/pki)).

**ANSI X9.17 - Cryptographic Service Messages** - describes a multi-layer key management scheme used in interbank communications, and in other applications for communicating between trusted hosts.

**ANSI X9.26 - Secure Sign-On Standard** - provides a simply implemented challenge and response password system many times more secure than a normal ID/password combination.

**ANSI X9.30 Part 1: Public Key Cryptography Using Irreversible Algorithms: Digital Signature Algorithm, 1995.** Also available as NIST, FIPS PUB 186.

**ANSI X9.30 Part 2: Public Key Cryptography Using Irreversible Algorithms: Secure Hash Algorithm (SHA-1) ANSI X9.31 Reversible Digital Signature Algorithms ANSI X9.42 Management of Symmetric Keys Using Diffie-Hellman ANSI X9.44 Key Transport Using RSA**

**RSA - (Rivest-Shamir-Adleman)** - is an asymmetrical algorithm named after the mathematicians who described it in 1978. It is proprietary (although subject to U.S. government regulations) and commercially available (e.g., PGP), having been implemented in a number of products. It is cumbersome to use for encryption of data streams and is being replaced by newer schemes with larger, and possibly variable, key sizes that incorporate key management and key transmission. Some of the contenders include Clipper, which is a hardware-based encryption scheme supported by the U.S. Department of Defense, the Japanese-invented Fast Encryption Algorithm (FEAL), the Australian LOKI, and the International Data Encryption Algorithm (IDEA).

**ANSI X9.45 - Enhanced Management Controls Using Digital Signatures and Attribute Certificates ANSI X9.52 - Triple DES Modes of Operation ANSI X9.55 - Extensions to Public Key Certificates and Certificate Revocation Lists ANSI X9.57 - Certificate Management ANSI X9.62 - Elliptic Curve Digital Signature Algorithm (draft) ASC X12**

**Accredited Standards Committee X12** - The Data Interchange Standards Association (DISA) (see [www.disa.org](http://www.disa.org)) is the not-for-profit organization that supports X12. X12 develops, maintains, interprets, publishes, and promotes the proper use of American National and UN/EDIFACT International Electronic Data Interchange Standards. Its main objective is to facilitate electronic interchange relating to business transactions such as order placement and processing, shipping and receiving information, invoicing, payment and cash application data, and data to and from entities involved in finance, insurance, education, and state and federal governments. X12N addresses health insurance specifically, and its transaction standards are being proposed under HIPAA. The following X12 standards address security:

**ANSI X12 .42 Cryptographic Service Message (815)** - provides the data format required for cryptographic key management, including automated distribution and exchange of keys.

**ANSI X12.58 - Security Structures (version 2)**

**ANSI X12.376 Secure Authentication and Acknowledgment (993)** - used by the recipient of a transaction set to authenticate and acknowledge the origin, content, or sequence of data received with the originator of the transactions.

**IEEE - Institute of Electrical and Electronics Engineers** - is an industry consortium (see: [www.ieee.org](http://www.ieee.org)) that has developed the Medical Information Bus (MIB) standard, IEEE 1073, for automated data capture from bedside patient medical devices. In the security arena, the following standard has been developed by this group:

**IEEE 802.10 - Standard for Interoperable Local Area Network Security (SILS), Draft 1992 - 1996** - IEEE 802.10 is seeking to expand the ISO 7498-2 Security Architecture so that security services (i.e., authentication, access control, and data integrity) can be provided at layer two. The document has eight parts, including a model, secure data exchange, key management, security management, Ethernet, sublayer management, SDE security labels, and protocol information conformance statement (PICS) proforma. X3S3.3, the ANSI-accredited standards committee for lower layers, has not supported this project because it departs from the familiar ISO Security Architecture and because it incorporates material subject to copyright protection.

**IETF - Internet Engineering Task Force** - (see: [www.ietf.org](http://www.ietf.org);) is a large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. IETF standards are created by committees that are submitted to the networking community through a set of documents called Requests for Comments (RFCs). All RFCs are considered draft documents because any document can be superseded by a newer RFC. IETF provides a suite of protocols under **IPSec** to secure communication at the network layer between communicating peers. The following are applicable standards from IETF:

**IETF ID Combined SSL/CPT Transport Layer Security Protocol SSL - Secure Sockets Layer Protocol** - is a programming interface developed by Netscape for World Wide Web applications and is currently undergoing standardization through IETF. It augments the sockets programming interface, which in turn is an interface to TCP. SSL ensures that eavesdroppers cannot read data, allows either side to verify the identity of the other side, and assures data integrity because any change to a byte will invalidate the check sum on each SSL chunk. SSL solves the problem of authentication and privacy between two sites using TCP, but is not a good choice for "store and forward" environments because once data is read all proof of origin is lost.

**IETF ID FTP Authentication Using DSA**

**IETF ID Secure HyperText TP Protocol (S-HTTP)**

**S-HTTP - Secure HyperText Transfer Protocol** - defines a request/response protocol on top of the HTTP protocol used in the World Wide Web. This protocol can secure each request/response pair separately, and provides data origin authentication, integrity, and confidentiality. It also provides nonrepudiation of responses. It emphasizes record or document level protection rather than session-level protection.

**IETF RFC 1422 Privacy Enhanced Mail: Part 1: Message Encryption and Authentication Procedures**  
**IETF RFC 1424 Privacy Enhanced Mail: Part 2: Certificate-Based Key Management**  
**IETF RFC 1423 Privacy Enhanced Mail: Part 3: Algorithms, Modes, and Identifiers**  
**SMIME - Secure Multipurpose Internet Mail Extensions** - is a public key encryption protocol originally developed by RSA

Laboratories for secure e-mail.

**IETF RFC 1510 - Kerberos Authentication Service**

**IETF RFC 1825 - Security Architecture for the Internet Protocol****IETF RFC 1826 - Internet Protocol Authentication Header****IETF RFC 1827 - Internet Protocol Encapsulating Security Payload (ESP)****IETF RFC 1828 - Internet Protocol Authentication using Keyed MD5****IETF RFC 1829 - The ESP DES-CBC Transform****IETF RFC 2025 - Simple Public Key Mechanism****SPKM - Simple Public Key Mechanism** - is designed for use with any session-oriented application, providing confidentiality, integrity, entity and origin authentication, and (optional) nonrepudiation. It also handles all peer-to-peer and client-server applications, is designed for use with GSS-API, and is recommended for use in CORBA applications.

### **IETF RFC 2104 HMAC: Keyed-Hashing for Message Authentication**

**NIST - National Institute of Standards and Technology** - through its Computer Security Resource Clearinghouse (CSRC) (see: <http://csrc.nist.gov>) is taking a leadership role in the development of a federal Public Key Infrastructure (PKI) that supports digital signatures and other public key-enabled security services. NIST is coordinating with industry and technical groups such as the federal PKI Steering Committee and its Technical Work Group (TWG) that has developed initial versions of a requirements document, a concept of operations, a technical security policy, an **X509 v3** certificate profile, and an interoperability report.

### **NIST, FIPS PUB 112 - Password Usage**

**NIST, FIPS PUB 196 - Entity Authentication Using Public Key Cryptography****PKCS #7 Cryptographic Message Syntax Standard, Version 1.5, November 1993, from RSA Laboratories** - supports encryption and signature of arbitrary data, including support for multiple signatures. PKCS #7 is used as the basis for the S/MIME secure e-mail standard, S-HTTP, and the ANS X9.45 authorization certificate originator to encrypt a message and by the recipient to decrypt a message.

**PKCS #11 Cryptoki B - A Cryptographic Token Interface****TCSEC - Trusted Computer System Evaluation Criteria ("The Orange Book") - DOD-5200.28 STD, U.S. Department of Defense** - originally published in 1983, TCSEC provides categorization of security products by seven classes (from the lowest level D to the highest A1). A similar body exists in Europe (the European Information Technology Security Evaluation and Certification Scheme (ITSEC). Products are tested on identification and authentication, access control, accountability, audit, object reuse, accuracy, reliability of service, and data exchange.

**United States Healthcare Security Standards and Guidelines** Security standards and guidelines specific to healthcare information systems applications have also been developed by ANSI-accredited SDOs, such as ASTM, DICOM, HL7, and NCPDP and industry consortia such as the Object Management Group (CORBAsec and CORBAmed), American Medical Informatics Association (AMIA), American Health Information Management Association (AHIMA), and the Computer-based Patient Record Institute (CPRI).

**American Health Information Management Association (AHIMA)** - (see:[www.ahima.org](http://www.ahima.org)) is the organization of health information management professionals. As the official custodians of medical records and health information within healthcare providers, health information management

professionals have long focused on protecting the confidentiality of patient information. AHIMA has developed a number of Practice Briefson:

- Authentication of Medical Record Entries
- Confidential Health Information and the Internet
- Destruction of Patient Health Information
- Disaster Planning for Health Information
- Disclosure of Health Information
- Electronic Signatures
- E-Mail Security
- Facsimile Transmission of Health Information
- Managing Health Information Relating to Infection with HIV
- Managing Multimedia Medical Records
- Patient Anonymity
- Patient Photography, Videotaping, and Other Imaging
- Protecting Patient Information after a Closure
- Release of Information Laws and Regulations (by State)
- Release of Information for Marketing Purposes

**American Medical Informatics Association (AMIA)** - is a professional association intended to advance the public interest in medical informatics through charitable, scientific, literary, and educational activities. It promotes the development and application of medical informatics in the support of patient care, teaching, research, and healthcare administration. In 1997, it published *Guidelines on the Use of Electronic Mail with Patients*, which provides communication, technical, and administrative and medicolegal guidelines on communicating with patients via e-mail.

**ASTM, Committee E31 - Healthcare Informatics** - includes subcommittees addressing privacy (E31.17) and data and system security (E31.20). These committees have produced the following standards:

**ASTM E1762 - Standard Guide for Electronic Authentication of healthcare Information** - Defines a document structure for use by electronic signature mechanisms; describes the characteristics of an electronic signature process; defines signature attributes for use with electronic signature mechanisms; describes acceptable electronic signature mechanisms and technologies; defines minimum requirements for user identification, access control, and other security requirements for electronic signatures; and outlines technical details for all electronic signature mechanisms in sufficient detail to allow interoperability between systems supporting the same signature mechanism.

**ASTM E1869 - Standard Guide for Confidentiality, Privacy, Access and Data Security Principles for Health Information Including Computer-Based Patient Records** - This proposed standard works toward achieving consensus on the issues of confidentiality, access, and privacy of patient records; and recommends standards, policies, procedures, and other safeguards for computer-based patient records and the secondary databases that are related to the patient

record. The goals are to recognize the patient's right to privacy, to preserve the confidentiality of the data, and to provide appropriate access.

**ASTM E1902 - Standard Guide for the Management of the Confidentiality and Security of Dictation, Transcription, and Transcribed Health Records** - This standard identifies the steps that must be taken to assure that dictation, transcription, and handling of the transcribed health records protect patient privacy.

**ASTM PS100-97 - Provisional Standard Specification for Authentication of Healthcare Information Using Digital Signatures** - This specification describes the use of digital signatures to provide authentication of healthcare information as described in ASTM E1762, Standard Guide for Authentication of healthcare Information. It includes specification of allowable signature and hash algorithms, management of public and private keys, and specific formats for keys, certificates, and signed healthcare documents.

**ASTM PS101-97 - Provisional Standard Guidelines for a Technical Security Framework for Transmission and Storage of Healthcare Information** - As previously described under "Security Service Standards," this guidelines describes a framework for the protection of healthcare information both in storage and transmission.

**ASTM PS102-97 - Provisional Standard Guide for Internet and Intranet Security** - This guide describes security mechanisms that can be used to protect healthcare information that is being transmitted over networks using the Internet Protocol Suite (IPS). This includes the Internet as well as corporate intranets constructed from off-the-shelf components implementing these protocols. This standard describes relevant security standards and recommends, where needed, particular options such as cryptographic transformations to be used with the standards.

**ASTM E1985-98- Standard Guide for User Authentication and Authorization** - This document describes mechanisms that may be used to authenticate users to computer systems as well as mechanisms to authorize particular actions by users. These actions may include access to healthcare information documents as well as specific operations on those documents. It addresses both centralized and distributed environments by defining the requirements that a single system must meet and the kinds of information that must be transmitted between systems to provide distributed authentication and authorization services.

**ASTM E2017-99 —Standard Guide for Amendments to Health Information** - This addresses the criteria for amending individually identifiable health information. Paper-based and computer-based amendments to healthcare records must have comparable methods, practices, and policies to ensure an unambiguous representation of the sequence and timing of documented events. Original and amended health information entries and documents must both be displayed, and must be consistent across both domains.

**ASTM PS115-99 - Provisional Standard Specification for Security Audit and Disclosure Logs for Use in Health Information Systems** - This draft standard identifies the data to be recorded in an audit log that serves to document and maintain a permanent record of all authorized and unauthorized access to confidential healthcare information so that providers, organizations, and

patients can retrieve evidence of that access to meet clinical, organization, risk management, and patient rights needs. The draft also describes the functionality needed for audit log management and the use of audit logs as tools by organizational managers.

**ASTM E1986-98 - Standard for Information Access Privileges to Health Information** - This document addresses the process of granting and maintaining access privileges to health information. It directly addresses maintenance of confidentiality of personal, provider, and organizational data in the healthcare domain. It addresses a wide range of data and data types, not all of which are traditionally defined as healthcare data. They are, however, elemental in the provision of data management, data services, and administrative and clinical healthcare services.

**ASTM E1987-98 - Standard Guide for Individual Rights Regarding Health Information** - This guide outlines the rights of individuals, both patients and providers, regarding health information and recommends procedures for the exercise of those rights.

**ASTM E1988-98 - Standard Guide for the Training of Persons Who Have Access to Health Information** - This standard addresses the privacy, confidentiality, and security training of employees, agents, and contractors who have access to health information.

**ASTM Draft Standard Specification for Transmission of Healthcare Information Using Secure Messaging Protocols** - This standard will describe the use of existing standard secure messaging protocols to convey healthcare information over store-and-forward communications networks (e.g., e-mail). The standard will address point-to-point transmission of healthcare information from a single originator to one or more recipients, and secure encapsulation of healthcare information and associated access control information that is used to determine which users can access the information. The standard is based on the S/MIME specifications produced by IETF.

**ASTM Draft Standard Privilege Management Infrastructure** - This standard will define interoperable mechanisms to manage privileges in a distributed environment.

**Computer-based Patient Record Institute** - CPRI was founded in 1992 as a result of recommendations in the Institute of Medicine patient record study report, *The Computer-based Patient Record: An Essential Technology for Health Care* (National Academy Press, 1991). The not-for-profit organization is committed to advancing improvements in healthcare quality, cost, and access through routine use of information technology. It has performed extensive work in the area of security for organizations using computer-based patient records:

**CPRI - Glossary of Terms Related to Information Security** - a compilation of terms and their referenced definitions that seek to establish consistency in use of contextually rich and complex terms associated with privacy, confidentiality, and security. The glossary provides context, demonstrates interrelationships among terms, and guides interpretation of terms. (See herein.)

**CPRI - Guidelines for Electronic Signature Policies** - provides guidance to developers and implementers of computer-based patient record systems relative to understanding the scope of electronic signature technologies and development and implementation of electronic signature

policies. The work distinguishes between electronic signature as a broad class and digital signature as special type. (See herein.)

**CPRI - Guidelines for Establishing Information Security Policies** - based on the premise that computer-based patient records offer the potential for achieving greater protection of health information over paper-based patient records, this work introduces the concept of a complete information security program consisting of policies, standards, training, technical and procedural controls, risk assessment, auditing and monitoring, and assigned responsibility for management of the program. Information security policies are the basis for all other aspects of effective information security programs and this work facilitates the development of policies within an organization. (See herein.)

**CPRI - Guidelines for Managing Information Security Programs** - essentially a job description for an information security manager, this work fosters the recognition of the need to establish an organizational infrastructure to implement and maintain an information security program and serves as a reference document for information security management.(See herein.)

**CPRI - Guidelines for Information Security Education Programs** - provides a curriculum for an information security educational program for healthcare providers and suppliers, including goals and objectives, content outline, instructional methodologies, methods of program implementation, and evaluation guidance. (See herein.)

**CPRI - Sample Confidentiality Statements and Agreements** - fosters the recognition of the need for all employees, students, volunteers, physicians, and vendors who access information systems to sign confidentiality agreements, and provides model agreements that organizations can adopt for their own use. (See herein.)

**CPRI - Security Features for Computer-based Patient Record Systems** - essentially a checklist for developers to ensure they have adequately incorporated security features in their product designs, for purchasers to use in specifying security requirements, and for auditors and consultants to use in evaluating the existence of security features in provider settings and supplier products. (See herein.)

**Three-State Health Information Planning Project** - Three consortia—the Washington-based Foundation for healthcare Quality, the Minnesota Health Data Institute, and the Massachusetts Health Data Consortium—have joined together to address a security and risk management framework that reflects HIPAA, Joint Commission on Accreditation of healthcare Organizations, and other requirements. Backed by funding from The Robert Wood Johnson Foundation and the John A. Hartford Foundation, the three groups formed a technical advisory committee in 1997, then selected the San Diego-based technology company Science Applications International Corp. (SAIC) to assist them. Their report issued in June 1998, "Security and Risk Management for Business-to-Business Health Information Networks," enumerates a security policy and a technology plan to help organizations transfer information securely.

**U.S. Department of Health and Human Services, Health Care Financing Administration** - HCFA released its **Internet Security Policy on Authentication and Identification Procedures** in

1998, which provides policy and guidelines for the security and appropriate use of the Internet to transmit HCFA Privacy Act—protected and other sensitive HCFA information (see Chapter Four)

### International General Security Standards

ISO/IEC has developed a security architecture and promulgated a number of security protocols for use at various layers. Figure 5 provides a summary of how security services are allocated to the OSI layers in the ISO 7498.2 framework for security architecture.

#### Allocation of Security Services to OSI Layers per ISO 7498.2 Framework for a Security Architecture

OSI Reference Model Layer							
Security Service	1 Physical	2 Data Link	3 Network	4 Transport	5 Session	6 Presentation	7 Application
Peer entity authentication			Y	Y			Y
Data origin authentication			Y	Y			Y
Access control service			Y	Y			Y
Connection confidentiality	Y	Y	Y	Y		Y	Y
Connectionless confidentiality		Y	Y	Y		Y	Y
Selective field confidentiality						Y	Y
Traffic flow confidentiality	Y		Y				Y
Connection integrity w/recovery				Y			Y
Connection integrity wo/recovery			Y	Y			Y
Selective field							Y

connection integrity							
Connectionless integrity			Y	Y			Y
Selective field connectionless integrity							Y
Nonrepudiation of origin							Y
Nonrepudiation of delivery							Y

Other applicable ISO/IEC standards include:

- ISO/IEC 9798-1: Information Technology - Security Techniques-Entity Authentication Mechanisms - Part 1: General Model
- ISO/IEC 9798-2: Information Technology - Security Techniques-Entity Authentication Mechanisms - Part 2: Entity Authentication Using Asymmetric Techniques
- ISO/IEC 10164-4 Information Technology - Open Systems Connection - System Management: Alarm Reporting Function
- ISO/IEC 10164-5 Information Technology - Open Systems Connection - System Management: Event Report Management Function
- ISO/IEC 10164-7 Information Technology - Open Systems Connection - System Management: Security Alarm Reporting Function
- ISO/IEC 10164-8 Information Technology - Open Systems Connection - System Management: Security Audit Trail Function
- ISO/IEC 10164-9 Information Technology - Open Systems Connection - System Management: Objects and Attributes for Access Control
- ISO/IEC 10181-2 Information Technology - Security Frameworks in Open Systems - Authentication Framework
- ISO/IEC 10181-3 Information Technology - Security Frameworks in Open Systems - Access Control Framework
- ISO/IEC 10181-4 Information Technology - Security Frameworks in Open Systems - Non-repudiation Framework
- ISO/IEC 10181-5 Information Technology - Security Frameworks in Open Systems - Confidentiality Framework
- ISO/IEC 10181-7 Information Technology - Security Frameworks in Open Systems - Security Audit Framework
- ISO/IEC 10736 Information Technology - Telecommunications and Information Exchange Between Systems - Transport Layer Security Protocol (TLSP)

- **ISO/IEC 11577 Information Technology - Telecommunications and Information Exchange Between Systems - Network Layer Security Protocol (NLSP)**

### **Other International Security Standards Efforts**

A new international standard for evaluating the security features of computer products has been developed through ISO. The Common Criteria for Information Technology Security Evaluation (ISO FDIS 15408) was expected to be published as an ISO standard in spring 1999. The Common Criteria builds upon previously developed security evaluation criteria for healthcare information technology of the U.S. (Trusted Computer System Evaluation Criteria [TCSEC], "The Orange Book," U.S. Department of Defense, 1985), Canada, and some members of the European Union. The Common Criteria is based on three major components: The Protection Profile, which is a statement of security needs for information technology products; The Security Target, which is a statement of security claims for a particular information technology security product or system; and a combination of security requirement components (see: <http://csrc.nist.gov/cc>). The European committee for standardization Technical Committee 251 - Medical Informatics (CEN TC251) (see: [www.cen251.org](http://www.cen251.org)) has a working group on security, privacy, quality, and safety. A prestandard on Security Categorization and Protection of Healthcare Information Systems (COMPUSEC) and a digital signature standard have been developed.

In July 1995, the European Union's Council of Ministers adopted the "Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data." The European Privacy Directive, as it became known, became effective October 25, 1998. U.S. businesses are expected to understand the directive to provide the means in their systems to comply, if they are selling abroad. The Department of Commerce is working with the European Union to define a "safe harbor" approach for American companies that would require them to self-certify that they are in compliance with the Directive. Standards development organizations and governmental entities in Japan, Singapore, Australia, and New Zealand are also currently developing standards to insure the security, confidentiality, and privacy of healthcare data as it resides in systems or as it is being passed in message transactions between systems.

### **Updates, Additions, and Corrections to this Work**

This work was developed in January 1999 and reflects what is believed to be the most current information on security standards and other related documents. Standards development, however, is an ongoing process. Updates, additions, and corrections to this work are most welcome and should be addressed to the Computer-based Patient Record Institute, now a partner with HIMSS ([www.himss.org](http://www.himss.org)). Margret Amatayakul, MBA, RRA, a health information management professional and former executive director of the Computer-based Patient Record Institute, compiled this work. She may be contacted through [margretcpr@aol.com](mailto:margretcpr@aol.com)