HIPAA, Security, and Electronic Signature: A Closer Look

Save to myBoK

by Holly Ballam, RRA

A recent notice of proposed rule making for an electronic signature standard, if adopted, will affect the way health information is managed for years to come. Here's what you need to know about electronic signature and what the proposed standard may mean for HIM.

The Health Insurance Portability and Accountabity Act of 1996 (HIPAA) is popularly known as a law designed to protect consumer insurance coverage in the event of job loss or change. But for the healthcare industry, HIPAA introduces other dimensions—providing controls to prevent fraud and abuse, protect privacy, and simplify healthcare administration.

Of particular interest to HIM professionals are HIPAA's ramifications for security and confidentiality. HIPAA's administrative simplification provision requires that the Department of Health and Human Services (HHS) adopt security standards to which healthcare industry players must adhere. A recent notice of proposed rule making for one such standard, which outlines a framework for the way healthcare entities will electronically maintain, transmit, and protect data, will affect the way health information is managed for years to come.

A Clearer Guideline

On August 12, 1998, HHS published a notice of proposed rule making on standards for the security of individual health information and electronic signature use by health plans, healthcare clearinghouses, and healthcare providers. These standards would comply with the statutory requirement that health information be protected to ensure privacy and confidentiality. This would particularly apply to information that is electronically stored, maintained, or transmitted on media ranging from magnetic tape, disk, CD-ROM, the Internet, leased lines, dial-up lines, and networks. Telephone voice response, "faxback" systems, and HTML interaction would not be included.[1]

The proposed rule provides a more succinct guideline on the use of electronic signature than previous directives. The Medicare Conditions of Participation for Hospitals state that authentication of medical records by computer entry is permitted. The Health Care Financing Administration (HCFA) permits computerized physician certifications, under appropriate safeguards. On a state level, legislation permitting electronic authentication of medical records varies widely.

Joint Commission for Accreditation of Healthcare Organizations information management (IM) standards address the issue of authentication, although digital signature is not specifically addressed. The standards that can apply to digital signature are:

- IM.2.1—the organization determines appropriate levels of security and confidentiality for data and information
- IM.2.2—collection, storage, and retrieval systems are designed to allow timely and easy use of data and information without compromising their security and confidentiality
- IM.2.3—records and information are protected against loss, destruction, tampering, and unauthorized access or use
- IM.7.1.1—only authorized individuals make entries in medical records
- IM.7.3.2.1—the complete operative report is authenticated by the surgeon and filed in the medical record as soon as possible
- IM.7.8—all medical record entries are dated and authenticated and their authors are identified

The proposed security standard is an improvement upon the less prescriptive guidelines previously set forth. The security measures are designed to protect and ensure the availability, integrity, and confidentiality of information. They are also scalable to meet the needs of organizations of various sizes at a reasonable cost.

The measures must meet four categories:

- Administrative procedures are formal practices used to oversee the selection and performance of security steps to protect information. Procedures also assist in monitoring personnel in regards to data protection. These procedures include requirements such as certification, information access control, internal audits, and training
- Physical safeguards cover the protection of physical systems, buildings, and equipment from destruction and encroachment. These safeguards include requirements such as assigned security responsibility, policies on workstation use, physical access controls, and security awareness training
- Technical security services are processes that protect information and control individual access to it. These require access control, audit control, and data and entity authentication
- Technical security mechanisms are processes established to prevent unauthorized access to data that is transmitted over a communication network

Each requirement has implementation features that must be met to demonstrate compliance. Requirement and implementation features are described in detail in the August 12, 1998 *Federal Register*.[2]

What Is Electronic Signature?

An individual's signature serves many purposes—both professionally and personally. A signature is a unique imprint left on the world that identifies the creation or review of a document, e.g., discharge summaries, operative reports, etc. A signature can enable action to take place, such as processing a physician's application to become a staff member. It is also utilized to meet legal prerequisites, such as contracts. Historically, signatures have always been a part of the healthcare documentation process, but with the advent of computer-based patient records, the means of entering a signature has changed. According to the proposed rule, organizations and providers that choose to use electronic signatures must use digital signature technology.

By industry definitions, use of a digital signature assures the user of authentication, message integrity, and nonrepudiation. Authentication refers to confirmation that the information the user utilizes is true and complete. Integrity of any message refers to the validity and wholeness of the message received. Nonrepudiation is verification that the originator of the document is, indeed, the originator and cannot deny that fact.

Pen-based and unique PIN password electronic signature applications are two of the most common electronic signature applications currently in use. Both of these have security weaknesses that could potentially allow the authentication, message integrity, and nonrepudiation of any electronic signature applied using these applications to be compromised. The security weaknesses that exist in these electronic signature applications have prompted HHS and the Department of Commerce's National Institute of Standards and Technology to propose adoption of a cryptographically based digital signature as the standard.

The proposed standard says that authentication, message integrity, and nonrepudiation must be assured for electronic signature to be used. Other features are optional for healthcare players, depending on their needs. These implementation features include:

- ability to add attributes
- continuity of signature capability
- countersignatures
- independent verifiability
- interoperability
- multiple signatures
- transportability of data

A digital signature is most often attached to a document after the document is created. It is activated in order to complete corroboration of electronic documents. Digital signatures are created and verified using cryptography and, generally, a coordinated pair of public and private keys are used. Public and private keys can encrypt and decrypt and provide confidentiality of the documents. One key is employed to encrypt the document, and only the corresponding key can decrypt it.

A digital ID has four basic components: a public key, which is matched to a particular person and is publicly known; a private key, which is known only to the user; the name and identification of the person; and a digital signature from a trusted digital ID issuer (a certificate authority).

In addition to compliance with federal regulation, digital signatures offer potential advantages—for HIM processes and the healthcare organization as a whole. Their added layers of authentication will help assure the security of health information. Because of their ability to ensure authentication, validation, and nonrepudiation, their use may simplify documentation methods and decrease the need to maintain manual (paper) records for legal and medical purposes. What's more, one of the barriers to computer-based record development has been the lack of a reliable means of authentication. As computerization becomes more thorough, physicians will have increased access to patient reports and will need to make fewer visits to the HIM department to complete charts. It is hoped that this facilitation will make the completion process simpler. As HIM staff need to retrieve fewer files to obtain signatures, a decrease in delinquent medical records could result. As processes flow more smoothly, the potential for decreases in turnaround time for reimbursement, legal, and medical needs grows.

Considerations for Implementation

The proposed standards require that a facility safeguard the confidentiality, availability, and integrity of health information. Although there will be a grace period in the event that the standard is adopted, organizations would be wise to begin planning for HIPAA compliance sooner rather than later. An organization can and must take steps in order to comply with the requirements—including measures that could mean changes in hardware, software, connectivity, and other technical approaches. Administrators must work closely with vendors to determine strategies and guidelines to insure implementation of security standards and maintenance of those standards.

One aspect of implementation will involve taking a long, hard look at existing systems. An organization must assess all systems used and ensure the physical security of health information and systems. Electronic systems must be able to authenticate users, and access controls need to be established and maintained consistently. The presence and utilization of a monitoring system or audit trail will assist in maintaining secure systems.

In some cases, it may be necessary to purchase new hardware or software to meet the requirements. The proposed rule states that the standard will be "technologically neutral"—giving "providers/plans/clearinghouses the flexibility to choose their own technical solutions."[3] In other words, the standard will apply no matter what systems, hardware, and software a facility selects. In this context, facilities can choose the systems that best meet their needs (and budgets) and comply with the standards. Various facilities will implement different processes to meet the basic requirements of HIPAA. Extraordinary measures are not required or recommended in order to implement the standards—but measures must be taken to necessitate information security and confidentiality compliance.

Should the proposed standard be adopted, health plans, clearinghouses, and providers will have 24 months from the effective date to prepare before the requirements are enforced. Small health plans will have 36 months to prepare.

The reengineering process will succeed if an organization is organized and thorough throughout the restructuring. Education is the foundation of any program's success. With their training and experience in security and confidentiality issues, HIM professionals are well positioned to showcase themselves and their abilities during this transition.

For example, the establishment of policies and procedures that address security and confidentiality of health information is the cornerstone of implementation (see "A Sample Information Security Program"). HIM professionals' experience in implementing policies and procedures and in educating employees makes them ideal candidates to manage enterprise-wide security programs.[4]

The proposed rule specifically states that security responsibilities should be assigned to a certain person or organization. Organizations will need the services of an information security officer. HIM professionals, with their unique qualifications—such as an understanding of federal regulations and comprehension of information flow—are certainly candidates for such a role, using skills they apply on a daily basis.

Education of all employees and medical staff is an essential factor for compliance with any new system. It is critical for HIM professionals to educate themselves to provide the best leadership in the process. Reading and becoming knowledgeable about HIPAA, the proposed rule, administrative simplification, and other related legislation is the basic first step. Your tools are as close as the Internet and your local library, as well as your state government, hospital association, and organization legal counsel.

(Editor's note: For more about electronic signatures, digital signatures, and digital certificates, see "Electronic Signatures, Digital Signatures, and Digital Certificates" Journal of AHIMA 70:3, 14-15.)

Notes

1. Massachusetts Health Data Consortium. "Health Insurance Portability and Accountability Act of 1996 (HIPAA) Notice of Proposed Rulemaking—Security and Electronic Signature Standards." Available at http://www.mahealthdata.org/mhdc/mhdc2.nsf/Documents/HIPAA-index.
2. Frawley, Kathleen, and Donald Asmonga. "HHS Publishes Notice of Proposed Rule Making for Security, Electronic Signature Standards." *Journal of AHIMA* 69, no. 9 (1998): 14-16.
3. Department of Health and Human Services. "Security and Electronic Signature Standards; Proposed Rule." *Federal Register* 63, no. 55 (August 12, 1998): 43249.
4. Kloss, Linda. "Information Security—A Wider Area Net-work." *Journal of AHIMA* 68, no. 5 (1997): 18.

References

Brandt, Mary. "New Rules for the CPR: No More Signing on the Dotted Line." *Healthcare Informatics* 11, no. 10 (1994): 30-34.

Massachusetts Health Data Consortium. "An Overview of the Health Insurance Portability and Accountability Act of 1996 (PL 104-191)—Administrative Simplification Provisions—Legislative Background—The 'Kennedy-Kassebaum Act.'" Available at http://www.mahealthdata.org/mhdc/mhdc2.nsf/Documents/ HIPAA-index.

McLendon, Kelly. "Encryption: The Key to CPR Signatures." *Advance for Health Information Professionals* 6, no. 17 (1996): 10-15.

National Research Council. *For The Record—Protecting Electronic Health Information*. Washington, DC: National Academy Press, 1997.

Rhodes, Harry. "Practice Brief: Electronic Signatures (Updated)." *Journal of AHIMA* 69, no. 9 (1998).

A Sample Information Security Program

for further reading

- Fuller, Sandra R. *Security and Access: Guidelines for Managing Electronic Patient Information*. Chicago, IL: AHIMA, 1997.
- National Research Council. *For The Record: Protecting Electronic Health Information*. Washington, DC: National Academy Press, 1997.

These Web sites provide much valuable information:

- Center for Democracy and Technology—http://www.cdt.org
- Computer Security Institute—http://www.gocsi.com
- CPRI Home Page—http://www.cpri-host.org
- Department of Health and Human Services Web page on administrative simplification—http://aspe.os.dhhs.gov/admnsimp
- Friends of the National Library of Medicine—http://amia2.amia.org
- HCFA's page on HIPAA—http://www.hcfa.gov/HIPAA/HIPAAHM.HTM
- JHITA Home Page—http://www.jhita.org
- Library of Congress Home Page—http://www.lcweb.loc.gov
- Massachusetts Health Data Consortium—http://www.mahealthdata.org

Holly Ballam *is policy and compliance administrator, information security, for CareGroup in Boston, MA. She is president of the Massachusetts HIMA.*

Article Citation:
Ballam, Holly. "HIPAA, Security, and Electronic Signature: A Closer Look." *Journal of AHIMA* 70, no. 2 (1999): 26-30.