Get Ready for Digital Signatures (HIPAA on the Job)

by Bonnie S. Cassidy, MPA, FHIMSS, RHIA

In the next few years, the healthcare industry will see a mad scramble to comply with the numerous requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Not least among HIPAA's provisions is a mandate for the standardization of electronic signatures.

With their expertise in information security, HIM professionals are prime candidates to assist in the implementation of electronic signature in their facility. With HIPAA compliance looming, this need will be even more pressing. Now is the time for HIM professionals to learn all they can about HIPAA requirements and to prepare to lead compliance efforts. Be informed and spread the word. Make sure that you have written policies and procedures in your organization regarding the use of electronic signatures. How to begin? In this installment, we'll take a closer look at electronic signatures.

What Does the Proposed Rule Say?

HIPAA's administrative simplification provisions include sub-sections on the privacy and security of patient data that mandate standards in safeguards for physical storage and maintenance, transmission, and access to individual health information.

The rule proposes standards for the security of individual health information and electronic signature use by health plans, clearinghouses, and providers. These entities would use the security standards to develop and maintain the security of all electronic individual health information.

The electronic signature standard is applicable only with respect to use with specific transactions defined by HIPAA, and only when it has been determined that an electronic signature must be used.

There is considerable motivation to implement a standard for electronic signature. Its use would improve the Medicare and Medicaid programs and other federal health programs and private health programs, as well as the effectiveness and efficiency of the industry in general.

Does HIPAA Require Electronic Signatures?

HIPAA does not specifically require use of electronic signature across the board. Instead, it says that whenever a HIPAA-specified transaction requires the use of an electronic signature, the standard must be used. *It should be noted that an electronic signature is not required for any of the currently proposed standard transactions.*

Use of an electronic signature refers to the act of attaching a signature by electronic means. 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. To generate an electronic signature, a system should be able to identify and authenticate the signer at the time of the signature.

The proposed standard for electronic signature is presented in section 142.310 of the August 12, 1998, *Federal Register* and would be digital.

What Is a Digital Signature?

A digital signature is formed by applying a mathematical algorithm to an electronic document. This process yields a unique string of characters or "bit string," referred to as a message digest. The digest (only) is encrypted using the originator's private key, and the result is appended to the electronic document.

The recipient of the transmitted document decrypts the message digest with the originator's public key, applies the same message algorithm to the document, then compares the resulting digest with the transmitted version. If they are identical, then the recipient is assured that the message is unaltered and the identity of the signer is proven. Because only the signatory authority can hold the private key used to digitally sign the document, the critical feature of nonrepudiation is enforced.

What Are the HIPAA Requirements For Electronic Signatures?

According to the proposed rule, organizations and providers that use electronic signatures must use digital signature technology. For what the rule requires, see All About Digital Signatures.

Various technologies may fulfill one or more of the requirements. Authentication systems (such as passwords, biometrics, physical feature authentication, behavioral actions, and token-based authentication) can be combined with cryptographic techniques to form an electronic signature. However, a complete electronic signature system may require more than one of the technologies mentioned above. Currently no technically mature techniques provide the security service of nonrepudiation in an open network environment, in the absence of trusted third parties, other than digital signature-based techniques. Therefore, *if electronic signatures are employed, the law would require that digital signature technology be used.*

What Do Providers Need to Know?

First, providers need to know that section 142.306(a) of the August 12, 1998, proposed rule requires them to apply the security standard to all health information pertaining to an individual that is electronically maintained or electronically transmitted.

In 142.310(a), entities would not be required to use an electronic signature. However, if a plan elects to use an electronic signature in one of the transactions named in the law, it would be required to apply the electronic signature standard described in 142.310(b) to that transaction. In the future, it is anticipated that the standards for other transactions may include requirements for signatures. In particular, the proposed standard for claims attachments, which will be issued in a separate regulations package later, may include signature requirements on some or all of the attachments. If the proposed attachments standard includes such signature requirements, they will address the issue of how to reconcile such requirements with existing state and federal requirements for written signatures as part of the proposed rule.

What About Implementation?

If an entity elects to use an electronic signature in a transaction, or if an electronic signature is required by a transaction standard adopted by the secretary of Health and Human Services, the entity must apply the electronic signature standard described in ß 142.310(b).

How the security standard would be implemented depends on industry trading partner agreements for electronic transmissions. The industry would be able to adapt the security matrix to meet its business needs.

The security standard would supersede contrary provisions of state law, including laws requiring medical or health plan records to be maintained or transmitted in other electronic formats. There are certain exceptions when the standards would not supersede contrary provisions of state law; section 1178 of the Social Security Act, Title XI, part C, identifies those conditions and directs the secretary of HHS to determine whether a particular state provision falls within one or more of the exceptions.

The electronic signature standard (digital signature) would be deemed to satisfy federal and state statutory requirements for written signatures with respect to the named transactions referred to in the legislation.

Several accreditation organizations, such as the Electronic Healthcare Network Accreditation Commission, the Joint Commission on Accreditation of Healthcare Organizations, and the National Committee for Quality Assurance indicate that they will require compliance with the HIPAA security and electronic signature (if applicable) standards.

What Are the Effective Dates?

Health plans would be required to comply with the security and electronic signature standards as follows:

- Each **health plan that is not a small health plan** would have to comply with the requirements of the proposed rule sections 142.306, 142.308, and 142.310 **no later than 24 months after publication of the final rule**

- Each **small health plan** would have to comply with the requirements of sections 142.306, 142.308, and 142.310 **no later than 36 months after the date of publication of the final rule**

- If the effective date for the electronic transaction standards is later than the effective date for the security standard, implementation of the security standard would not be delayed until the standard transactions are in use. The security standard would still be effective with respect to electronically stored or maintained data. Security of health information would not be solely tied to the standard transactions but would apply to all individual health information electronically stored, maintained, or transmitted

- Under this proposed rule, in some cases, a health plan could choose to convert from paper to standard EDI transactions prior to the effective date of the security standard. The authors of the proposed rule recommend that the security standard be implemented at that time in order to safeguard the data in those transactions

How Can I Learn More?

One of the best ways for HIM professionals to get informed is to obtain and read the full text of the HIPAA legislation and the *Federal Register*. Copies can be obtained by mail or via the Internet.

To obtain a copy of the original legislation which put HIPAA in motion, the Health Insurance Portability and Accountability Act of 1996, contact the Government Printing Office and ask for PL 104-191, Subtitle F.

Send requests to New Orders, Superintendent of Documents, PO Box 371954, Pittsburgh, PA 15250-7954. A check in the amount of eight dollars ($8) for each document, or your credit card number and expiration date, should be enclosed.

Credit card orders can be called to the order desk at (202) 512-1800 and orders can be faxed to (202) 512-2250.

Two more recent *Federal Registers* addressing HIPAA are:

- August 12, 1998, Part III, 45 CFR Part 142, Security and Electronic Signature Standards

- November 3, 1999, Part IV, 45 CFR parts 160 through 164, Standards for Privacy of Individually Identifiable Health Information

To use the Internet to locate the text of HIPAA, go to http://thomas.loc.gov and search under Legislation. To search the *Federal Register*, go to the US Government Printing Office site at www.access.gpo.gov/su_docs/index. html and follow the *Federal Register* links.

All about Digital Signatures

If digital signature is employed, the following three implementation features must be implemented: Message integrity, nonrepudiation, and user authentication.

Message integrity means ensuring (usually through technology) that what the sender types and sends out is received in the same form and format as the original message. Technology can "package" the message (through encryption or through some other mechanism) and unpack and check the message upon its arrival at the receiving location.

Nonrepudiation means the message must be "packaged" in some form so that the recipient has complete confidence and assurance that the message came from a particular sender and that the sender cannot claim he/she never sent the message.

Authentication ensures that users are who they say they are, and prevents unauthorized people from accessing data.

These implementation features are optional:

- Ability to add attributes
- Continuity of signature capability
- Countersignatures
- Independent verifiability
- Interoperability
- Multiple signatures
- Transportability

Selection Criteria

The developers of the proposed rule used certain general criteria to guide their choices for standards based on the specifications of HIPAA. In assessing security and electronic signatures, they noticed that the standards most strongly address certain criteria. Many of these criteria reflect issues HIM professionals are already well acquainted with. According to the proposed rule, Section F, these are:

1. **Improve the efficiency and effectiveness of the healthcare system**, particularly in regard to electronic health information.
2. **Be consistent and uniform with the other HIPAA standards and with other private and public sector health data standards.**
3. **Be technologically independent of computer platforms and transmission protocols.** The security and electronic signature standards have been defined in terms of requirements that would allow organizations to select the technology that best meets their business requirements while still allowing them to comply with the standards.
4. **Keep data collection and paperwork burdens on users as low as is feasible.** The standards would allow organizations to decide the level of security information techniques and controls they need while still meeting privacy and confidentiality goals. This would allow data collection and the paperwork burden to be as low as feasible.
5. **Incorporate flexibility to adapt more easily to changes in the healthcare infrastructure and information technology.** In other words, the standards is "technologically neutral and more adaptable to changes in infrastructure and information technology."

Bonnie Cassidy, *MPA, FHIMSS, RHIA, is a principal with the North Highland Company, Atlanta, GA. She can be reached at bcassidy@ north-highland.com.*

Article citation:
Cassidy, Bonnie S. "Get Ready for Digital Signatures (HIPAA on the Job series)." *Journal of AHIMA* 71, no.8 (2000): 16A-C.

Driving the Power of Knowledge