HHS Publishes Notice of Proposed Rule Making for Security, Electronic Signature Standards

Save to myBoK

by Kathleen A. Frawley, JD, MS, RRA, and Donald D. Asmonga

On August 12, the Department of Health and Human Services (HHS) published the 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 are part of the requirements of the administrative simplification provision of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

This rule requires health plans, healthcare clearinghouses, and healthcare providers to have security standards in place. These standards would comply with the statutory requirement that healthcare information and individually identifiable health information be protected to ensure privacy and confidentiality for health information that is electronically stored, maintained, or transmitted. The proposed security standard does not require the use of an electronic signature but specifies the standard that must be followed if an electronic signature is used.

Electronic transmissions would include transactions involving all media, including information that is physically moved from one location to another via magnetic tape, disk, or compact disc. Also covered in the rule are transmissions via the Internet, Extranet, leased lines, dial up lines, and private networks.

The proposed security standard requires each healthcare entity engaged in electronic maintenance or transmission of health information to assess its own security needs and risks, then devise, implement, and maintain appropriate security to address its business requirements. These measures, which must be documented and maintained regularly, must meet four categories:

- Administrative procedures to guard data integrity, confidentiality and availability: Formal, documented practices to manage the selection and execution of security measures to protect data as well as the conduct of personnel in relation to the protection of data. These procedures including the following requirements:
    - certification
    - chain of trust partner agreement
    - contingency plan
    - formal mechanism for processing records
    - information access control
    - internal audit
    - personnel security
    - security configuration management
    - security incident procedures
    - security management process
    - termination procedures
    - training
- Physical safeguards: The protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. This category also covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities. Physical safeguards must include all of the following requirements and implementation features:
    - assigned security responsibility
    - media controls
    - physical access controls

    - policy/guideline on work station use
    - secure work station use
    - security awareness training
- Technical security services: The processes implemented to protect information and control and monitor individual access to information. These services include the following requirements:

    - access control
    - audit controls
    - authorization control
    - data authentication
    - entity authentication

- Technical security mechanisms: The processes implemented to prevent unauthorized access to data that is transmitted over a communications network.

Each of the requirements has implementation features that must be met to demonstrate compliance. Matrices that depict the requirement and implementation features can be found in the August 12, 1998, Federal Register. If the organization chooses to use the Internet to transmit or receive health information, some form of encryption must be used.

Electronic Signatures

If an entity elects to use an electronic signature in a HIPAA specified transaction, the entity must apply the electronic signature standard. The standard for electronic signature is a digital signature -- an electronic signature based upon cryptographic methods of originator authentication, computed with a set of rules and parameters that allow for the verification of the identity of the signer and the integrity of the data.

If an entity uses electronic signatures, the signature method must assure all of the following features:

- message integrity
- nonrepudiation
- user authentication

The entity may also use, among others, any of the following implementation features:

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

The notice in the August 12, 1998, Federal Register contains a detailed glossary of terms, bibliography, and chart listing the security requirements, implementation features, and mapped standards. Comments on the proposed requirements are due October 13.

Patient Protection Act Narrowly Passes in House

On July 24, Republicans pushed managed care quality legislation through the House of Representatives. Its chief sponsors are House Speaker Newt Gingrich (R-GA) and chair of the House Republican Health Quality Task Force, Rep. Dennis Hastert (R-IL). HR 4250, the Patient Protection Act of 1998, passed largely along partisan lines 216 to 210, lacking enough support to reach a majority of 218 votes. Upon passage, the Patient Protection Act was forwarded to the Senate for further consideration.

It is doubtful that the Senate will consider HR 4250 due to the Senate Republican Health Quality Task Force's own legislation, S 2330, the Patients' Bill of Rights Act. Sen. Don Nickles (R-OK) is the primary sponsor of S 2330. The bill, much less

comprehensive than the House's Patient Protection Act, will still face considerable hurdles in the Senate due to the Democrats' fairly united backing of their own proposal (S 1890) and the Senate's rules of procedure. At press time, the Senate did not anticipate that any action toward consideration of the legislation would take place until mid-September.

HR 4250, the Patient Protection Act of 1998, was introduced "to provide new patient protections under group health plans." The language of HR 4250's Title V addresses confidentiality of health information.

This title addresses requirements for inspection and copying of protected health information, supplementation of protected health information, notice of confidentiality practices, establishment of safeguards, and availability of protected health information for purposes of healthcare operations.

A glaring weakness of the language in Title V is that it does not contain any restrictions on the use and disclosure of individually identifiable health information. Also absent is language concerning authorizations for disclosure of protected health information for treatment, payment, healthcare operations, and authorizations for the disclosure outside the rubric of treatment, payment, and healthcare operations. "Section 1185, Availability of Protected Health Information for Purposes of Health Care Operations" permits:

- Disclosure -- A person who maintains protected health information to disclose the information to a healthcare provider or a health plan in order to permit the provider or plan to conduct healthcare operations
- Use -- A healthcare provider or a health plan that maintains protected health information for use in conducting healthcare operations

The language does prohibit healthcare providers or health plans from selling or bartering protected health information as part of conducting healthcare operations. Healthcare operations is defined as "services, provided directly by or on behalf of a health plan or a healthcare provider or by its agent, for any of the following purposes: (a) coordinating healthcare, including healthcare management of the individual through risk assessment, case management, and disease management; (b) conducting quality assessment and improvement activities, including outcomes evaluation, clinical guideline development and improvement, and health promotion; (c) carrying out utilization review activities, including precertification and preauthorization of services, and health plan rating activities, including underwriting and experience rating; or (d) conducting or arranging for auditing services."

Another area of contention concerns the preemption of state law. AHIMA has long sought confidentiality legislation that comprehensively preempts state law and treats all health information at an equally high standard, in part to do away with the patchwork of laws and regulations that currently exist. Section 1186 of Title V preempts state law but creates exceptions for "confidentiality of medical records maintained by a licensed mental health professional" and "condition-specific limitations on disclosure."

Finally, the bill fails to establish criminal penalties for the illegal use and disclosure of individually identifiable health information. Civil penalties in the legislation, determined by the Secretary of HHS, apply to those who fail to comply with various sections of Title V. Penalties would be applied in the following manner:

- For violations of Section 1181, Inspection and Copying of Protected Health Information, and Section 1182, Supplementation of Protected Health Information, penalties would start at $500 for each violation but not exceed $5000 for all identical violations during a calendar year
- For violations of Section 1183, Notice of Confidentiality Practices; Section 1184, Establishment of Safeguards; and Section 1185, Availability of Protected Health Information for Purposes of Health Care Operations, the penalties would begin at $10,000 for each violation but not exceed $50,000 for all identical violations during a calendar year
- The penalty for violations that the Secretary of HHS determines occur with such frequency that they constitute a business practice will not exceed $100,000

The bill removes the authority of the Secretary of HHS to promulgate a unique health identifier for individuals that was originally mandated in HIPAA. The secretary may not adopt a final standard until legislation is enacted to specifically approve the standard or contain provisions consistent with the standard.

The bill also requires two reports from the Government Accounting Office's Comptroller General of the US. The first, a study and report on the effect of state law on health-related research, is due one year from enactment of the bill. The second, a study and report on state law on protected health information, is due nine months from enactment. In addition, the language

changes the August 1999 deadline set by Congress to pass confidentiality legislation that was established by HIPAA. The new deadline would be six months after the submission of the report on protected health information.

Aside from health information confidentiality, HR 4250 deals with many other aspects of healthcare. Managed care quality reform has focused on the issue of access to emergency medical care. The Patient Protection Act establishes the prudent layperson standard for the authorization of initial coverage of emergency medical care.

In addition, HR 4250 prohibits managed care "gag rules," provides for direct access to gynecological and obstetrical care for women if the plan covers such care, and provides for direct access to pediatric care if the plan covers pediatric care. The legislation sets a malpractice damages cap, establishes internal and external appeals guidelines, and expands access to medical savings accounts. Finally, the bill contains a number of provisions to increase the bargaining power of health plan purchasers. For small businesses, HR 4250 creates a "healthmart" concept, in which purchasing pools can be developed between small businesses, healthcare providers, and insurers. Similar provisions exist for association health plans such as church, trade, and business organizations.

Prior to the passage of HR 4250, an alternative offered by Reps. John Dingell (D-MI) and Greg Ganske (R-IA) was narrowly defeated 212 to 217. The alternative consisted of the HR 3605 text -- the Democrats' Patients' Bill of Rights Act. HR 3605 was more comprehensive with regard to establishing federal mandates for access to medical care, patients' rights, and enforcement procedures.

As Congress approaches the end of the 105th Congress, legislative activity will increase rapidly. If the Senate does consider health quality legislation, a second chance for the Democratic party's language may arise. Identical language to HR 3605 (S 1890) is expected to be the alternative language offered by Sens. Tom Daschle (D-SD) and Edward M. Kennedy (D-MA) during Senate debate.

Kathleen A. Frawley *is AHIMA's vice president, legislative and public policy services, and* ***Donald D. Asmonga*** *is AHIMA's government relations representative.*

Article citation:
Frawley, Kathleen A., and Donald D. Asmonga. "HHS Publishes Notice of Proposed Rule Making for Security, Electronic Signature Standards." *Journal of AHIMA* 69, no.9 (1998): 14-20.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.