Getting Ready for HIPAA Privacy Rules

by Margret Amatayakul, MBA, RHIA, FHIMSS

What do the proposed privacy regulations mean to HIM professionals—and what can you do now to begin to prepare? The author takes an in-depth look at the proposed rules.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is bringing significant changes to the management of health information. While final rules have not yet been published, proposed rules make it clear that changes are in store for how we handle confidential health information. We should prepare now to educate our organizations, respond to consumers, and make the transition to new practices.

While many of the proposed rules related to HIPAA have been in circulation since 1998, the "Standards for Privacy of Individually Identifiable Health Information" are relative latecomers, published in November 1999 with a comment period that lasted until mid-February 2000. At this time, we don't know when the privacy standards will actually be implemented. But it's not too early for HIM professionals to become familiar with the proposed standards, understand what they mean, and identify some preliminary steps toward compliance.

Administrative Simplification 101

The privacy regulations are part of HIPAA's administrative simplification provisions. These provisions aim to improve the efficiency and effectiveness of the healthcare system. While adoption of the standards will likely entail expenditure of resources to ensure compliance, once in place they are expected to reduce current costly multiple proprietary systems. Processes and procedures will be streamlined and practices more uniform across states.

The security and privacy provisions aim to safeguard the confidentiality of private information and protect the integrity of health data while also ensuring its availability for care. It is important to understand, however, that the proposed security standards and the proposed privacy standards are two different things. The security standards deal with measures organizations need to take to keep their information safe. The privacy standards deal with things patients may expect from organizations in terms of the way their health information is used.

Although proposed rules for many of the HIPAA standards were published in 1998, the volume of comments generated on the proposals and the Department of Health and Human Services' (HHS) Y2K remediation efforts stalled issuance of final rules. Spring 2000 has now been targeted as the tentative schedule for publication of the first set of final rules. (Check the administrative simplification Web site at http://aspe.os.dhhs.gov/admnsimp/ for updated schedules.) Organizations must comply with new rules within the specified period after the effective date of the final rules. (The effective date of a final rule is generally 60 days after its publication, and compliance is generally required within two years of that.)

An Imperfect Measure?

To understand the proposed privacy regulations, it is important to appreciate their context. The regulations do not provide the sweeping privacy reform that federal privacy legislation could afford. Because Congress failed to pass privacy legislation within its self-imposed deadline under HIPAA, the secretary of HHS has had to promulgate regulations that are restricted to the scope of HIPAA.

This means that the privacy regulations only pertain to "covered entities," which include healthcare providers who transmit health information electronically, health plans, and healthcare clearinghouses. Covered entities are required to have contracts with their business partners, including auditors, consultants, claims clearinghouses, and other contractors, that would limit the

business partner's uses and disclosures of the protected health information to those permitted by the contract. Banks, employers, schools, other insurers, and others that are not a "covered entity" and do not have business arrangements with covered entities do not have to comply with the requirements.

Further, only "protected information"—individually identifiable health information that has been maintained or transmitted in electronic form—is covered. Electronic maintenance includes information stored on magnetic tape, disk, or CD, and electronic transmission may be via any means—Internet, extranet, leased or dial-up lines, and private networks. (Voice mail and fax-to-fax systems are excluded.)

When information becomes "protected" by being stored or transmitted electronically, the protections would apply even after it is printed, discussed orally, or otherwise changed in form. The protections also apply to the original paper version of information once it is transmitted electronically.

A provider who maintains a paper-only information system would not be subject to the privacy standards. Because the provisions of the privacy regulation pertain to information, not the record, providers who maintain certain information exclusively on paper and other information in electronic form would have "mixed records" and would theoretically be able to treat the two types of information differently.

Finally, the proposed privacy rule creates only a "floor," or basic set, of provisions. Organizations in states whose laws have more stringent requirements would still have to comply with those laws. As a result, organizations in some states will have to follow dual privacy practices. Vendors, enterprises that cross state boundaries, and potentially those exchanging information across states will have to address these issues as well.

In a practical sense, any provider who has mixed records—probably most providers today—would probably not want to treat information maintained solely on paper differently than that maintained in electronic form, if only to avoid uncertainty about when information is considered electronic.

The risk to privacy protection in the standards as proposed is more in relation to noncovered entities, to providers who maintain paper-only records, and, in the view of some, to those in states with less stringent privacy requirements. There is no federal "ceiling" that would protect all information in all states equally.

In issuing the proposed rules, HHS noted that this situation is not ideal and called for comments on the scope of its authority.

Knowing the Standards

The proposed privacy standards cover several important principles, including use, disclosure, minimum requirements, reasonableness, deidentification, and individual rights.

Use: The proposed privacy standards would allow health information to be used and shared easily for treatment, payment, and healthcare operations. (The latter includes activities such as quality assurance, utilization review, credentialing, insurance rating for individuals enrolled in a health plan, and others. It does not include marketing or the sale of protected health information.) The proposed privacy regulations explicitly prohibit covered entities from seeking individual authorizations for uses and disclosures for treatment, payment, and healthcare operations unless required by state or other applicable law, in which case they must use separate forms.

The reason for this prohibition is the belief that obtaining such an authorization at the time an individual presents for healthcare is generally not an informed consent and could cultivate erroneous understandings of individual's rights and protections. Covered entities are not allowed to make treatment or payment conditional to the patient's agreeing to disclose information.

Disclosure: The proposed privacy standards would also allow health information to be disclosed without an individual's authorization for certain national priority purposes (such as research, public health, and oversight), but only under defined circumstances. A written authorization for use and disclosure of health information for other purposes would be required.

Minimum necessary, reasonableness, and deidentification: The amount of information for any use or disclosures would be restricted to the minimum necessary to accomplish the relevant purpose, taking into consideration practical and

technological limitations. Covered entities would be given latitude in making reasonable efforts to limit use and disclosure and deidentify protected information. Covered entities are encouraged to deidentify information when it is possible to do so.

Individual rights: Finally, the proposed privacy rule includes a number of individual rights. It would create a set of fair information practices to inform people of how their information is used and disclosed, ensure that they have access to information about themselves, and require health plans and providers to maintain administrative and physical safeguards to protect the confidentiality of health information and protect against unauthorized access.

Detailed provisions of the proposed privacy standard were reported in the January 2000 issue of the *Journal of AHIMA*.[1] The full text of the proposed rule may be downloaded from the HHS Web site (http://aspe.os.dhhs.gov/admnsimp/) or from the Government Printing Office link to the November 3, 1999, *Federal Register* at www.access.gpo.gov/su_docs/aces/aces140.html. The Federal Register is also available in many public libraries or by purchase from the Government Printing Office.

The proposed privacy regulations are intended to be flexible and scalable. Each covered entity needs to assess its own needs and implement privacy policies appropriate to its information practices and business requirements. Following the steps noted in "Twelve Things You Can Do Now to Prepare for HIPAA" is a good way to begin. In the meantime, keep your eyes on the legislative horizon for more developments.

Note

1. Frawley, Kathleen, and Don Asmonga. "HHS Proposes HIPAA Privacy Standards." *Journal of AHIMA*, 71, no. 1 (2000): 16-18.

Twelve Things You Can Do Now To Prepare For HIPAA

HIM professionals should fully understand the requirements of the proposed standards, monitor the legislative and regulatory scene for any initiatives that Congress may yet consider and for issuance of the final rule, and begin addressing compliance in their own organizations. Some steps to take to prepare for compliance include:

- **Determine whether you are working for a covered entity or an organization that would have a contract with a covered entity.** Providers who transmit health information electronically are covered. Health plans and clearinghouses are covered because they must accept health information electronically. Information systems vendors, consulting firms, transcription services, and other potential business partner of a covered entity are required to comply with contractual terms to ensure that protected health information disclosed in the course of business remains confidential. Many businesses are taking proactive stands on HIPAA to ensure that their services will continue without disruption. Help your colleagues develop and use contracts that will protect privacy of individually identifiable health information.

- **Begin a HIPAA awareness program to acquaint top management with the proposed rules.** Encourage your employer to designate a privacy official now—someone who would create a comprehensive compliance plan, assist in developing policies and procedures, conduct education and training programs, maintain documentation of policies and procedures for complying with the privacy regulations, and monitor ongoing compliance. Frequently, HIM professionals are most familiar with their organizational requirements and are in the best position to serve as privacy officials.

- **Propose and obtain approval for an appropriate policy relative to what information will be protected beyond the scope of the standards.** If your organization limits the scope of its privacy practices to protected health information as defined in the rule, develop a procedure that identifies information that will be subject to protection. Most providers will treat all health information as protected. Develop methods for disclosing only the minimum amount of protected information necessary to accomplish any intended purpose. Determine when and how information will be deidentified to further afford protection.

- **Review present state statutes to determine if authorization is required for treatment, payment, and healthcare operations.** If so, this must be physically separate from authorization for disclosure of protected health information required under the proposed rule. Information about laws in different states may be obtained from the Attorney Internet Services (AIS) Web site. To find laws, go to www.alllaw.com/state_resources/, type in your search term (e.g., confidentiality), select the appropriate state, and then click the search button.

- **Revise authorization forms for release of information for all purposes other than treatment, payment, and healthcare operations.** Authorizations initiated by a covered entity include more requirements than authorizations initiated by an individual. The notice of proposed rulemaking provides a model that covers both types of requests. Be prepared to respond to requests for protected health information uses that do not require consent, such as for public health, health oversight, and judicial activities. Entities must have reasonable procedures for verifying the identity and authority of persons requesting such disclosures.

- **Draft and obtain approval for a notice of information practices** that states the uses and disclosures the covered entity intends to make with health information. Any use or disclosure not included becomes unlawful, so the statement should be made as broad as possible while still being specific. Providers must give this notice to each patient at the first service after the effective date of the rule and post a copy of the notice. Health plans would have to provide the notice at enrollment and at least every three years after. Any modifications made to the practices would also have to be distributed. Establish a means for individuals to lodge complaints about your organization's information practices and possible violations of privacy.

- **Propose and obtain approval for appropriate policies relative to restrictions on disclosure.** Individuals must be informed of their right to ask a covered entity to restrict further use and disclosure of protected health information, with the exception of uses or disclosures required by law. The covered entity, however, would not be required to agree to such a request; but if it does, it would be bound by the agreement.

- **Develop a mechanism for accounting for all disclosures of protected health information for purposes other than treatment, payment, and healthcare operations** (subject to a certain time-limited exceptions for disclosures to law enforcement and oversight agencies).

- **Develop a procedure that allows individuals to inspect and copy their protected health information.** Determine and apply reasonable cost-based fees for copying.

- **Propose and obtain approval for an appropriate policy for your organization with respect to the covered entity's response to individuals who request amendment or correction of protected health information that is inaccurate or incomplete.** Covered entities do not have to comply with the request, but you should have formal procedures for whatever policy is adopted.

- **Develop a privacy training program for employees and work with human resources to develop a system of sanctions for employees, ranging from retraining to reprimand to termination, for employees who are in violation of the organization's privacy policies.** Work with the medical staff to incorporate appropriate sanctions in their bylaws, rules, and regulations. Work with the appropriate members of your organization to develop a system of sanctions for business partners found to be in violation of contractual agreements.

- **Work with your security officer** (if different from the privacy official) to establish administrative, technical, and physical safeguards to protect identifiable health information from unauthorized access or use.

Margret Amatayakul *is president of Margret\A Consulting, LLC, in Schaumburg, IL. She is active in healthcare informatics standards development organizations that have contributed standards under HIPAA proposed regulations. She can be reached at MargretCPR@aol.com.*

Article citation:
Amatayakul, Margret. "Getting Ready for HIPAA Privacy Rules." *Journal of AHIMA* 71, no.4 (2000): 34-36.