Regulatory Report

PROOF

Highlights of the HIPAA Final Rule

Dental practices must be prepared to comply with these new regulations in order to effectively protect the privacy of their patients and secure the safety of health data.

By Charlene LaVoie, RDH, MPA, JD, and Joyce Ann Turcotte, RDH, MEd, FAADH

On January 25, 2013, the United States Department of Health and Human Services (HHS) published the long awaited final rule that modifies parts of the Health Insurance Portability and Accountability Act (HIPAA). Passed by Congress in 1996, HIPAA enables workers to transfer and continue health insurance coverage if they lose or change jobs, provides standards for the use of protected health information in electronic health records, and mandates the protection and confidentiality of protected health information.

The final rule applies to covered entities (medical/dental providers) and business associates (organizations that use and disclose protected health information to provide administrative services to medical/dental providers). The compliance date for most aspects of the final rule is September 23, 2013. Reportedly, HHS intends to more aggressively enforce HIPAA, making it crucial that every medical and dental practitioner—whether in large institutions or small practices—understand the new standards and the implications for health care delivery. Table 1 (page 18) lists the areas of focus for the final rule.

REVISED DEFINITION OF BREACH

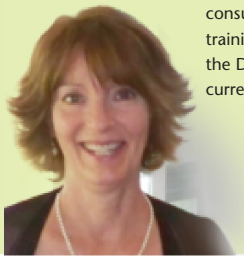
The final rule adopts most of the provisions of the interim rule regarding breach notification regulations, which require health care providers, health insurance providers, and other entities to alert individuals if their protected health information is compromised. However, it does change the subjective harm standard, which requires an analysis of the risk of financial, reputational, or other harm to an individual caused by a breach, with the presumption that a breach has occurred unless it is demonstrated through a risk assessment that the probability of such a compromise is unlikely. As a result, the burden of proof shifts to the medical/dental provider or business associate to demonstrate that this probability is low—a difficult standard to meet. The HHS will likely give less latitude in making internal determinations about what constitutes a breach, with the agency expected to report a majority of breaches to the affected individuals and the Office for Civil Rights.

Risk assessment must be performed after all impermissible uses and disclosures of protected health information. If a risk assessment is not performed, and none of the other exceptions apply, the incident is automatically presumed to be a breach. This increased burden on risk assessment analysis and notification means that medical/dental providers and business associates must update their policies and procedures to ensure they can detect and respond to potential data breaches in an appropriate and compliant manner.

EXCEPTIONS TO THE DEFINITION OF BREACH

The final rule eliminates the exception for protected health information that does not include dates of birth or zip codes from being labeled a breach. The following examples, however, remain exceptions and do *not* constitute a breach:

- Unintentional acquisition, access, or use of protected health information by a workforce member or individual acting under the authority of the medical/dental providers or business associate that is made in good faith, within the course or scope of employment or other professional relationship, and is not further used or disclosed in an unlawful manner under the HIPAA privacy rule



CHARLENE LaVOIE, RDH, MPA, JD, is a speaker on legal issues for Professional Learning Services, an educational and consulting service that provides continuing education, dental hygiene refresher programs, and cardiopulmonary resuscitation training. She is a former professor at the University of Bridgeport Fones School of Dental Hygiene in Bridgeport, Conn, and the Department of Dental Hygiene at Tunxis Community College in Farmington, Conn. LaVoie is a trial lawyer and currently serves as director of the Community Lawyer/Advocate Project, in Winsted, Conn.

JOYCE ANN TURCOTTE, RDH, MEd, FAADH, is the president of Professional Learning Services, and has 35 years of clinical practice and teaching experience. She is an adjunct faculty member in the Department of Periodontics at Nova Southeastern University in Fort Lauderdale-Davie, Fla, and a clinical instructor in the Department of Dental Hygiene at Tunxis Community College. Turcotte is past president of the Connecticut Dental Hygienists' Association and the American Academy of Dental Hygiene.

- Inadvertent disclosure to another authorized person at the same medical/dental office, business associate's company, or organized health care arrangement, and the protected health information is not further used or disclosed in an unlawful manner under the HIPAA Privacy Rule

TABLE 1. Areas of Focus for the Final Rule of the Health Insurance Portability and Accountability Act (HIPAA)

- Expands individuals' rights to access their protected health information
- Limits the use and disclosure of protected health information for marketing and fundraising, and probits its sale without patient authorization
- The Department of Health and Human Services (HHS) is no longer required to reach resolution of a HIPAA violation through informal means, such as voluntary compliance. Rather, HHS must conduct an investigation of a HIPAA complaint where a preliminary review of the facts indicates a possible violation due to willful neglect
- Mandates changes to both the content and distribution of medical/dental providers' notice of privacy practices; the notice must inform individuals of their right to be notified following a breach involving their protected health information
- Makes business associates of medical/dental providers subject to many of the same rules as medical/dental providers; expands the definition of a business associate to include individuals receiving protected health information from a business associate to perform legal, actuarial, accounting, consulting, management, administrative, or financial services; also makes business associates liable for the acts of its agents, including its subcontractors

- Disclosure where the medical/dental provider or business associate believed that the unauthorized person to whom the information was disclosed would not reasonably be able to retain such information

UPDATE PROCEDURES

The breach notification rule requires medical/dental providers to develop and document policies and procedures; train employees; impose sanctions for failure to comply with these policies and procedures; permit individuals to file complaints regarding these policies and procedures or a failure to comply; and requires refrain from intimidating or retaliatory acts.

Medical/dental providers must notify affected individuals, the HHS Secretary, and, in certain circumstances, the media in light of a breach of protected health information. Medical/dental providers must notify affected individuals of a breach in writing or by email within 60 days of the discovered breach, if the affected individual has agreed to receive electronic notices. A description of the breach, steps individuals can take to protect themselves, covered entity activities to investigate and mitigate, and how to contact the covered entity must be included in the notice. If the medical/dental professional has insufficient or out-of-date contact information for 10 or more individuals, then a substitute notice must be provided by either posting the notice on the homepage of the health care/dental provider's website, or by providing the notice in print or broadcast media where the affected individuals reside. If the medical/dental provider has insufficient or out-of-date contact information for less than 10 individuals, a notice must be issued by other means, such as written letter or telephone call. For a breach affecting more than 500 individuals, in addition to notifying the affected individuals, the medical/dental provider is required to provide notice to area media outlets within 60 days.

The covered entity must notify HHS of breaches on its website breach report form. For breaches affecting more than 500 individuals, the HHS Secretary should be notified within 60 days. For breaches affecting fewer than 500 people, the Secretary should be contacted on an annual basis—no later than 60 days after the end of the calendar year in which the breach was discovered (vs occurred).

EXPANDED ENFORCEMENT

Under the prior rule, investigations or compliance reviews were not mandatory. HHS attempted to resolve violations informally by allowing a provider to implement a corrective action plan. The final rule gives HHS the discretion to attempt to resolve allegations through informal means. But mandatory investigations must be initiated when a preliminary review of the facts indicates the violation occurred due to willful neglect, or when brought to its attention through means other than a formal complaint (eg, media report or government agency).

Civil monetary penalties and annual limits on penalties for identical violations will be imposed, depending on the medical/dental provider's or business associate's culpability and knowledge. Correction of the violation within 30 days can reduce the penalty.

The HHS Secretary may consider factors in assessing penalties, including the number of individuals affected, the time period in which the violation occurred, the nature and extent of the harm, prior compliance, the medical/dental provider's or business associate's response to technical assistance from the HHS Secretary, past responses to complaints, and the financial condition and the size of the medical/dental provider's practice.

ENSURE COMPLIANCE

To ensure compliance with the final rule, medical/dental providers need to update their HIPAA privacy and security policies by:

- Revising breach notification policies to address the new low probability standard and required risk assessment analysis
- Addressing the expanded access right to permit individuals to receive an electronic copy of their health information
- Reviewing the limitations on marketing, fundraising, and the sale of protected health information
- Retraining workforce members on revised privacy, security, and breach notification policies; emphasis should be placed on training workforce members to identify and report breaches of unsecured protected health information in a timely manner
- Revising notice of privacy practices to include additional statements specified by the final rule, including a description of the types of uses and disclosures that require written authorization, and distribute them accordingly

In addition, business associates may need to implement more detailed policies, as they are now liable for violations of the HIPAA rules; this includes a subcontractor who creates, receives, maintains, or transmits protected health information on behalf of a business associate

Through compliance with the final rule and all HIPAA policies, dental practices will be able to effectively protect the privacy of their patients while avoiding costly penalties. For more information about the final rule, visit: archive.hhs.gov/ocr/hipaa.