Rules of Spring: Reviewing the Upcoming Regulations on HIPAA Privacy Rule Modifications

By Kevin Heubusch

The American Recovery and Reinvestment Act came out with a bang in February 2009. The rules enacting its privacy and security provisions, however, have trickled out over the subsequent two years. Many of the provisions have the potential for significant impact on HIM operations, and the slow pace of the rulemaking process has drawn out the industry's uncertainty and, to some degree, apprehension.

This spring should resolve some of the uncertainty, if not the apprehension. It is expected that the rules will begin flowing again, perhaps even by the time this issue has been printed. Many of the provisions will have final rules and compliance dates behind them; others will be addressed in proposed rulemaking that offers the industry a first look at intended regulations and a chance for comment before proceeding further.

Expanded Access and Restrictions

Covered entities got their first look at a draft rule enacting the majority of the access and restriction modifications last summer. Things have been quiet ever since.

The Office for Civil Rights (OCR) published a notice of proposed rulemaking, or NPRM, in July 2010 titled "Modifications to the HIPAA Privacy, Security, and Enforcement Rules." The rule drafted regulations for HITECH provisions that:

- Require covered entities that maintain EHRs to provide individuals with copies of their protected health information in electronic format upon request or transmit the copy directly to an entity or person as directed
- Extend to business associates the same requirements and penalties as covered entities under HIPAA
- Convey business associate status to emerging entities such as health information exchanges and personal health record operators
- Extend a consumer's right to request restrictions on disclosure to health plans under certain conditions (e.g., the item or service has been paid out of pocket in full)
- Increase requirements and restrictions related to marketing and fund raising, such as prohibiting certain written marketing communications
- Prohibit the sale of an individual's protected health information unless covered by a valid authorization or limited exception

HITECH also requires the Department of Health and Human Services to provide guidance on what constitutes "minimum necessary" under HIPAA in an effort to clarify a data holder's responsibilities in releasing requested information. The NPRM asked for comments on what type of guidance would be helpful.

OCR also included in the NPRM modifications of its own based on issues it has been collecting since HIPAA was published. Two issues in particular relate to disclosure of decedent records that have at times frustrated individuals and challenged HIM departments. OCR's proposed rule would:

- Allow disclosure of decedent records to family members and others not named as personal representatives
- Remove protected health information status for a patient deceased more than 50 years

OCR will likely follow the NPRM with a final rule, unless it still requires feedback from the industry on aspects of the regulation. At the time this issue went to press, a rule was expected in April.

Accounting of Disclosure

OCR's NPRM did not address accounting of disclosure, one of the more daunting modifications that HITECH makes to HIPAA. Recognizing the administrative challenge this modification will require, OCR has proceeded more slowly with the AoD rulemaking.

HITECH revises HIPAA to require that covered entities that maintain an electronic health record system must account for all disclosures, including those related to treatment, payment, and operations-uses that HIPAA had excluded. HITECH also shortens the accounting period to three years.

In May 2010 the office published a request for information, in which it sought both general comments and answers to a list of nine questions. The information, OCR wrote, will help it "better understand the interests of individuals with respect to learning of such disclosures" as well as "the administrative burden on covered entities and business associates of accounting for such disclosures."

Meanwhile, the first HITECH deadline related to AoD has passed. HITECH had stipulated entities that purchased EHR systems on or after January 1, 2009, were due to begin providing the new accountings on January 1 of this year. In the absence of regulation, however, no reporting is expected. Entities with older systems, which presumably require more retrofitting to meet the requirements, have until 2014 to comply.

OCR's next step will be publication of an NPRM, which presents another opportunity for public comment. At press time, the rule was expected at any time.

NPRMs typically feature comment periods of 30 to 60 days, after which OCR will process the comments and proceed to either an interim final rule (if it still desires feedback) or to a final rule.

Depending on how prepared OCR believes covered entities are to meet the rule's requirements, it could choose to make the rule effective upon publication or at a later date.

Breach Notification

Covered entities and business associates have been reporting breaches of unsecured protected health information to the Department of Health and Human Services since September 2009, so it can be easy to forget that the rulemaking on breach notification is not over.

OCR published an interim final rule in August 2009, which took effect one month later. The first reported breaches involving 500 or more individuals were posted to the HHS Web site in February 2010. HITECH does not require HHS to publish reports of breaches involving fewer than 500 individuals.

It appeared a final rule was in the offing in May 2010, but OCR withdrew it for further consideration that summer. The office noted that the issues were "complex," but it did not specify what it would consider further.

Some speculated OCR was re-examining the so-called harm threshold, which was the most controversial feature of the interim rule. Under the provision, a covered entity may judge whether a discovered breach is likely to result in harm. If it judges the risk to be low, the entity is not required to notify the individuals affected.

This provision was not specified in HITECH. OCR introduced it to relieve administrative burden for covered entities and unnecessary alarm for individuals. However, consumer advocates and some Congressional members have objected, saying the allowance is counter to the intent of the law.

There also was speculation at the time that a more all-encompassing data breach law might be forthcoming from Congress. However, a final rule is now expected this spring.

HITECH also required that the Federal Trade Commission promulgate a breach notification rule for vendors of personal health records and other noncovered entities that provide PHR services. FTC published a final rule right out of the gate in August 2009. In broad terms, its provisions match those in the HHS breach notification rule.

Updates on all regulations discussed here are available on the *Journal* Web site, http://journal.ahima.org.

Audio Online http://journal.ahima.org

An Accounting of Accounting of Disclosure. An interview with AHIMA practice resources manager Diana Warner on AoD under HIPAA and HITECH.

Kevin Heubusch (kevin.heubusch@ahima.org) is editor-in-chief at the *Journal of AHIMA*.

Article citation:
Heubusch, Kevin. "Rules of Spring: Reviewing the Upcoming Regulations on HIPAA Privacy Rule Modifications" *Journal of AHIMA* 82, no.4 (April 2011): 34-35.