HITECH Final Rule Revises Privacy, Security and Breach Notification Rules

By Rick L. Hindmand and Dominic A. Paluzzi, McDonald Hopkins LLC

The Final Rule revises the Privacy, Security and Enforcement Rules that were previously issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the interim final Breach Notification Rule that was previously issued in accordance with the HITECH Act. The Final Rule was published in the Federal Register on January 25, 2013. This article provides an overview of some Final Rule provisions that are of particular relevance to physicians.

Action items for physicians prior to September 23, 2013 compliance date:

• Update policies and procedures, Notices of Privacy Practices and information security programs
• Workforce training
• Review business associate agreements, determine whether the agreements qualify for grandfathered status, and enter into new business associate agreements

Business Associates

The HIPAA Privacy and Security Rules allow covered entities to disclose protected health information (PHI) to business associates, and allow business associates to create and receive PHI on behalf of the covered entity, subject to the terms of a business associate agreement between the parties. For purposes of HIPAA and the HITECH Act, a “covered entity” is a health care provider (such as a hospital or physician practice) that transmits health information in electronic form, a health plan, or a health care clearinghouse (such as a medical billing company). In general, the HIPAA regulations define a “business associate” as a person (other than a member of the covered entity’s workforce) or entity who, on behalf of a covered entity, performs a function or activity involving the use or disclosure of PHI, such as the performance of financial, legal, actuarial, accounting, consulting, data aggregation, management, administrative, or accreditation services to or for a covered entity.

The Final Rule implements the HITECH Act’s expansion of business associates’ HIPAA obligations by applying the Privacy and Security Rules directly to business associates and by subjecting business associates to civil and criminal penalties for HIPAA violations. Furthermore, the Final Rule extends business associate status to direct or indirect subcontractors to whom a business associate delegates a function, activity or service involving the creation, receipt, maintenance or transmission of PHI. Each business associate that delegates any function involving the use or disclosure of PHI to a subcontractor will be required to enter into a business associate agreement with the subcontractor.

The Final Rule expands the potential liability of covered entities to include exposure for the acts and omissions of a business associate if the business associate is deemed to be an agent of the covered entity and the acts or omissions are within the scope of the agency. It will therefore be important for covered entities to structure their agreements and relationships with business associates to minimize the risk that a business associate could be viewed as an agent of the covered entity.

Breach Notification Rule

The Final Rule broadens the breach notification obligations of covered entities and business associates by modifying the definition of “breach” and the risk assessment process for determining whether notification will be required. The Final Rule replaces the “risk of harm” standard of the interim Breach Notification Rule with a standard based on the risk that PHI is compromised. The prior standard allowed covered entities and business associates to conduct a “risk of harm” analysis and a “breach” would only result if the impermissible use or disclosure posed significant risk of financial, reputational or other harm. Under this new standard, however, an acquisition, access, use or disclosure of unsecured PHI that is not permitted under the Privacy Rule is presumed to be a breach (and therefore requires notification to the individual, OCR and possibly the media) unless either the incident satisfies one of three relatively narrow exceptions, or the covered entity or business associate demonstrates a low probability that PHI has been compromised. This determination is now based on a risk assessment of at least the following four factors: (1) the nature and extent of the PHI, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used or accessed the PHI; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk is mitigated (for example, by obtaining reliable assurances by recipients of PHI that the information will be destroyed or will not be used or disclosed).

In its commentary, OCR expressed concern that the prior “harm to the individual” standard, has been misinterpreted to permit too many breaches to go unreported. OCR characterized the new standard as more objective than the “harm” standard.

It is also important to note that the Final Rule did not make any changes to the circumstances permitting preemption of state laws. HITECH notification is only the floor of notification obligations. Covered entities and business associates must still comply with the notification obligations set forth in the various state breach notification laws, which can often be more stringent than HITECH.

Additional provisions of the Final Rule

The Final Rule addresses a laundry list of issues, including provisions or commentary that:

• Require covered entities to modify their Notices of Privacy Practices
• Require covered entities to agree to an individual’s request to restrict disclosure of PHI about the individual to a health plan when the individual (or someone other than the health plan) pays for the item or service in full
• Permit compound authorizations for clinical research studies
• Revise the definition of PHI to exclude information regarding a person who has been deceased for more than 50 years
• Prohibit the sale of PHI without authorization from the individual, and add a requirement of authorization in order for a covered entity to receive remuneration for disclosing PHI
• Restrict marketing
• Allow individuals to obtain a copy of PHI in an electronic format if the covered entity uses an electronic health record
• Clarify OCR’s view that covered entities are allowed to send electronic PHI to

(Continued on page 6)
HITECH Final Rule Revises Privacy, Security and Breach Notification Rules (Continued from page 5)

- Prohibit health plans from using or disclosing genetic information for underwriting, as required by the Genetic Information Nondiscrimination Act of 2008 (GINA)
- Allow covered entities to disclose relevant PHI of a deceased individual to a family member, close friend or other person designated by the deceased, unless the disclosure is inconsistent with the deceased individual’s known prior expressed preference
- Allow disclosure of proof of immunization to schools if agreed by the parent, guardian or individual
- Revise the Enforcement Rule (which was previously revised in 2009 as an interim final rule) to expand mandatory investigations and compliance reviews, permit the sharing of PHI with other agencies for enforcement purposes, and revise standards for determining the levels of civil monetary penalties.

The Final Rule does not address the HITECH Act requirement that a covered entity provide an accounting for disclosures. Commentary from OCR notes that this requirement will be addressed in future regulations.

Effective and compliance dates
The Final Rule takes effect on March 26, 2013, with a compliance date of September 23, 2013. Covered entities and business associates, including subcontractors, therefore must comply with the Final Rule by September 23, 2013. The 180-day compliance period, however, does not apply to modifications of the Enforcement Rule, which will apply beginning on the March 26, 2013 effective date. Moreover, breach notification continues to be governed by the interim Breach Notification Rule until the September 23, 2013 compliance date.

If certain conditions are met, the Final Rule allows additional time (in addition to the 180-day compliance period) to revise business associate agreements to bring them into compliance with the HITECH requirements. In particular, transition provisions will allow covered entities and business associates to continue to operate under existing business associate agreements for up to one year beyond the compliance date (until September 22, 2014) if the business associate agreement:
1. is in writing,
2. is in place prior to January 25, 2013 (the publication date of the Final Rule),
3. complies with the Privacy and Security Rules as in effect immediately prior to January 25, 2013, and
4. is not modified or renewed.

This additional time for grandfathered business associate agreements applies only to the written documentation requirement. Covered entities, business associates and subcontractors will be required to comply with all other HIPAA requirements beginning on the compliance date, even if the business associate agreement qualifies for grandfathered status.

In light of the issuance of the Final Rule it will be crucial for all covered entities and business associates to review and update their HIPAA-related policies and arrangements prior to the September 23, 2013 compliance date.