How the New HIPAA Regulations Affect Billing Companies and Their Subcontractors as Business Associates

By Robert A. Polisky, Esq.

DEVELOP AN ACTION PLAN FOR YOUR COMPANY AND SUBCONTRACTORS

On January 25, 2013, the Office for Civil Rights of the U.S. Department of Health & Human Services (OCR) published the anticipated final omnibus rule (the Final Rule). This rule created significant changes to the Privacy, Security, Breach Notification, and Enforcement Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), many of which are required by the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The Final Rule also implements changes to the Genetic Information Nondiscrimination Act of 2008.

The scope of the Final Rule is extensive, and enhances OCR's ability to enforce HIPAA. In the press release announcing the Final Rule, OCR Director Leon Rodriguez proclaimed that the Final Rule "marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented" and "strengthen[s] the ability of my office to vigorously enforce the HIPAA privacy and security protections...." Individuals and entities affected by the Final Rule must comply with most of its provisions by September 23, 2013.

This article addresses key provisions of the Final Rule applicable to billing companies and their subcontractors, enforcement changes, and recommended action items needed for compliance by billing companies and their subcontractors.

KEY PROVISIONS

BUSINESS ASSOCIATES AND THEIR SUBCONTRACTORS

Expanded Definition of "Business Associate"

The Final Rule expands the definition of a "business associate" to include any individual or entity that creates, receives, maintains, or transmits protected health information (PHI) on behalf of a covered entity. Companies that code, bill, and/or collect claims on behalf of a health care provider (i.e., a covered entity), are business associates under HIPAA. Notably, the Final Rule includes subcontractors that create, receive, maintain, or transmit PHI on behalf of a business associate as business associates themselves. Thus, any subcontractors that a billing company engages to assist in coding, billing, or collections, and any subcontractors that store or transmit any healthcare records on the billing company's behalf, are business associates of the billing company.

Direct Liability

As business associates, the Final Rule requires billing companies and their subcontractors to comply with the Security Rule's administrative, physical, and technical safeguard requirements as well as with the Security Rule's policies and procedures and documentation requirements. These requirements apply to business associates in the same manner as they apply to covered entities, such that billing companies and their subcontractors can be held civilly and criminally liable for violations of these requirements. Similarly, the Final Rule applies certain Privacy Rule requirements to business associates and establishes direct liability of business associates for violations of these requirements. A billing company does not need to provide a notice of privacy practices or designate a privacy official unless the covered entity designated such a responsibility in the billing company's business associate agreement.

Specifically, billing companies and their subcontractors, as business associates, have direct civil and criminal liability exposure for the following items.

1. impermissible uses and disclosures of PHI
2. failure to provide breach notification to the covered entity
3. failure to provide access to a copy of electronic PHI to either the covered entity, the individual, or the individual's designee (whichever is specified in the business associate agreement)
4. failure to disclose PHI to OCR where required by OCR

to investigate or determine the business associate's compliance with HIPAA

5. failure to provide an accounting of disclosures
6. failing to enter into business associate agreements with subcontractors that create or receive PHI on the business associate's behalf
7. failure to comply with the requirements of the Security Rule

Billing companies and their subcontractors also remain contractually liable for all other Privacy Rule obligations that are included in their business associate agreements.

Business Associate Agreements

The Final Rule clarifies that a covered entity is not required to enter into a business associate agreement with a billing company's subcontractor. Rather, the billing company that engaged a subcontractor to perform a function or service involving the use or disclosure of PHI is required to enter into a business associate agreement with the subcontractor. Each business associate agreement in the business associate chain needs to be at least as restrictive as the agreement above it in the chain with respect to permissible uses and disclosures of PHI.

The Final Rule expands the requirements of a business associate agreement by obligating a business associate to comply, where applicable, with the Security Rule with regard to electronic PHI; report breaches of unsecured PHI to the covered entity; and ensure that any subcontractors that create or receive PHI on its behalf agree to the same restrictions and conditions that apply to the business associate with respect to such information.

Transition Period

The Final Rule delays compliance until September 22, 2014 for a covered entity or business associate to enter into a business associate agreement with a business associate or subcontractor if, prior to January 25, 2013, the covered entity or business associate had a business associate agreement with the business associate or subcontractor, as applicable, that complied with HIPAA prior to the Final Rule (unless the business associate agreement was modified or actively renewed between March 26, 2013 and September 23, 2013). In all other cases, covered entities and business associates will need to execute business associate agreements with their business associates and subcontractors no later than September 23, 2013.

MODIFICATION TO THE BREACH NOTIFICATION RULE

Background

Under the HITECH Act, a covered entity is required to notify affected individuals and OCR following discovery of a breach of unsecured PHI; a covered entity also needs to notify the media of a breach involving more than 500 residents of a state or jurisdiction. A business associate, in turn, is required to notify a covered entity following discovery of a breach of unsecured PHI at or by the business associate.

On August 24, 2009, OCR issued an interim final rule implementing the HITECH Act's breach notification provisions ("Breach Notification Interim Rule"). In the Breach Notification Interim Rule, a "breach" is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule that "compromises the security or privacy" of the PHI, with certain exceptions. Moreover, under the Breach Notification Interim Rule, "compromises the security or privacy" of the PHI is defined to mean that an impermissible use or disclosure of PHI poses a significant risk of financial, reputational, or other harm to the individual (the "harm standard").

Revised Definition of "Breach"

The Final Rule significantly revises the definition of "breach" to clarify that an impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. By replacing the "harm standard" with this "low probability" standard, it is more likely under the Final Rule than under the Breach Notification Interim Rule that covered entities and business associates will determine that an impermissible use or disclosure of PHI "compromises the security or privacy" of the PHI, resulting in many required breach notifications that would not have been required previously.

Modification of Risk Assessment

Under the Final Rule, to determine whether there is a low probability that PHI has been compromised, covered entities and business associates need to conduct a risk assessment that considers at least the following factors:

- the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- the unauthorized person who used the PHI or to whom the disclosure was made;
- whether the PHI was actually acquired or viewed; and
- the extent to which the risk to the PHI has been mitigated.

If an evaluation of the above factors, taken together, fails to demonstrate that there is a low probability that PHI has been compromised, breach notification will be required.

RIGHT TO RESTRICT DISCLOSURE TO A HEALTH PLAN

Under the Final Rule, health care providers, upon request from an individual, must agree to restrict disclosure of PHI about the individual to a health plan if the disclosure would be for the purpose of carrying out payment or healthcare operations, and is not otherwise required by law, or the PHI pertains solely to a healthcare item or service for which the individual, or person acting on the individual's behalf (other than the health plan), has paid the covered entity in full. To avoid payment issues, a health care provider may want to require payment in full at the time of the individual's request for a restriction. Health care providers may request assistance from billing companies to comply with this new restricted disclosure requirement.

ENFORCEMENT

Discretion

The Final Rule gives OCR discretion to use informal means to resolve HIPAA violations. However, OCR is permitted to impose a civil monetary penalty without exhausting informal resolution efforts, especially when the HIPAA violation is due to willful neglect. The Final Rule also allows OCR to coordinate with other law enforcement agencies, such as state attorneys general and the Federal Trade Commission, with respect to pursuing remedies against HIPAA violators.

Tiered Penalty Amounts

Under the HITECH Act, there are four tiers of increasing penalty amounts that correspond to the levels of culpability associated with a HIPAA violation. The minimum fines range between $100 and $50,000 per violation, and are capped at $1.5 million for all violations of the same HIPAA provision during any calendar year (see below table). The lowest category of violation covers situations where the covered entity or business associate did not know, and by exercising reasonable diligence would not have known, of the HIPAA violation. The second lowest category of violation applies to violations due to reasonable cause and not to willful neglect. The third category applies to situations where the violation was due to willful neglect and was corrected within 30 days of when the covered entity or business associate knew, or should have known, of the violation. The fourth category applies to situations where the violation was due to willful neglect and not corrected within 30 days of when the covered entity or business associate knew, or should have known, of the violation.

The Final Rule modifies the definition of "reasonable cause" to mean "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated [HIPAA], but in which the covered entity or business associate did not act with willful neglect." The Final Rule keeps the definition of "willful neglect" as the "conscious, intentional failure, or reckless indifference to the obligation to comply" with HIPAA.

Counting Violations

In the preamble to the Final Rule, OCR states that how it counts HIPAA violations for purposes of calculating a civil monetary penalty varies depending on the circumstances

Categories of HIPAA Violations and Corresponding Penalty Amounts

Violation Category	Penalty Per Violation	All such violations of an identical provision in a calendar year
Did not know	Between $100 and $50,000	$1.5 million
Reasonable cause	Between $1,000 and $50,000	$1.5 million
Willful neglect (timely corrected)	Between $10,000 and $50,000	$1.5 million
Willful neglect (not timely corrected)	$50,000	$1.5 million

surrounding the violation. OCR explains that where multiple individuals are affected by a HIPAA violation (e.g., a breach of unsecured PHI), it is anticipated that the number of identical HIPAA violations would be counted by the number of individuals affected. OCR also explained that, with respect to continuing violations (e.g., a lack of appropriate safeguards for a period of time), it is anticipated that the number of identical HIPAA violations would be counted on a per day basis (i.e., the number of days the covered entity or business associate did not have appropriate safeguards in place to protect the PHI). OCR notes that in many HIPAA breach cases, there would be an impermissible use or disclosure as well as a safeguards violation, for each of which OCR would be entitled to calculate a separate civil monetary penalty. Needless to say, the amount of civil monetary penalties that could be imposed against a billing company or one of its subcontractors for a HIPAA violation can be quite substantial.

Factors Used to Determine a Penalty

The Final Rule lists the following five factors that OCR will consider in determining the amount of a civil monetary penalty.

1. the nature and extent of the HIPAA violation, including the number of individuals affected and the duration of the violation
2. the nature and extent of the harm resulting from the violation, including physical, financial, and reputational harm, and any hindrance to an individual's ability to obtain healthcare
3. the history of prior compliance with HIPAA, including whether the current violation is the same/similar to prior indications of noncompliance by the covered entity or business associate and their attempts to correct that noncompliance
4. the financial condition of the covered entity or business associate, including any financial difficulties that could have affected compliance and whether a civil monetary penalty could jeopardize the future provision of healthcare
5. such other matters as justice may require

Agency Liability

The Final Rule makes covered entities and business associates liable for the acts of their business associate agents, regardless of whether the covered entity or business associate knew of the violation or had a compliant business associate agreement in place. According to OCR, the key factor in determining whether an agency relationship exists between a covered entity and its business associate, or between a business associate and its subcontractor, is the principal's right to control the agent's conduct in the course of performing a service on behalf of the principal. OCR observes that a business associate agent's conduct generally is within the scope of agency when its conduct occurs during the performance of the assigned work or incident to such work, regardless of whether the work was done carelessly, a mistake was made in the performance, or the business associate disregarded a covered entity's specific instruction. OCR further observes that, in contrast, a business associate agent's conduct generally is outside the scope of agency when its conduct is solely for its own benefit (or that of a third party), or it pursues a course of conduct not intended to serve any purpose of the covered entity. To protect itself, a billing company's services agreement with a subcontractor should specify that the subcontractor is engaged as an independent contractor, not as an agent, and the billing company does not have the right to control the subcontractor's performance.

In the press release announcing the Final Rule, OCR Director Leon Rodriguez proclaimed that the Final Rule "marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented."

RECOMMENDED ACTION ITEMS

Although billing companies and their subcontractors have until September 23, 2013 to fully comply with the Final Rule, they should begin preparing soon in light of the significant number of new or modified compliance obligations. In particular:

- Covered entities will need to revise, negotiate, and execute business associate agreements with billing companies compliant with the Final Rule by September 23, 2013 to the extent they did not have business associate agreements in place as of January 25, 2013 that were HIPAA compliant. They have until September 22, 2014 to do so to the extent they had business associate agreements in place as of January 25, 2013 that were HIPAA compliant. OCR gives a fair amount of latitude in the content of business associate agreements, so it is important for billing companies to ensure that they are not overcommitting to responsibilities or deadlines that are not required under HIPAA.
- Billing companies that use subcontractors that create, receive, maintain, or transmit PHI on their behalf will need to draft, negotiate, and execute business associate agreements with them by September 23, 2013. Billing companies will need to ensure that these business associate agreements are at least as stringent as their business associate agreements with covered entities, and enable billing companies to meet deadlines in their business associate agreements with covered entities.
- Billing companies, including subcontractors, will need to conduct a security risk assessment, implement a written HIPAA security plan, designate a security official, and create certain written HIPAA privacy policies by September 23, 2013 to the extent they have not already done so. OCR has posted guidance on compliance with the HIPAA Security Rule found at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule that may be helpful to billing companies and their subcontractors and facilitate their compliance efforts.
- Billing companies and their subcontractors will need to perform a gap analysis to determine what HIPAA policies and procedures need to be revised to comply with the Final Rule, and then will need to revise them by September 23, 2013 based on the gap analysis.
- Billing companies and their subcontractors will need to update by September 23, 2013 their breach notification policies and any tools concerning how to conduct a risk assessment to determine whether breach notification is required.

- Healthcare providers may ask billing companies to implement by September 23, 2013 a method to flag or make a notation in the record with respect to PHI concerning an item or service paid in full by an individual – or person acting on the individual's behalf (other than a health plan) – to ensure that such information is not inadvertently sent to or made accessible to a health plan for payment or healthcare operations purposes, such as audits by the health plan.
- Billing companies and their subcontractors will need to update their HIPAA training materials and then train their workforce members (i.e., employees, volunteers, trainees, and other persons under their direct control) by September 23, 2013 to comply with HIPAA.

Given the breadth and potential penalties under the Final Rule, billing companies and their subcontractors should review their data flows (i.e., the complete lifecycle of PHI that they create, receive, maintain, or transmit) and then perform an updated risk analysis based on that review, including a risk analysis of mobile devices. Billing companies and their subcontractors will need to determine whether to encrypt these devices in light of the increasing prevalence of large penalties imposed by OCR on entities whose mobile devices, such as laptop computers and smartphones, containing unencrypted PHI have been lost or stolen. Further, covered entities and business associates should consider whether it would be cost-effective for them to purchase HIPAA liability insurance given the risk of substantial penalties for HIPAA violations. ■

Robert A. Polisky, principal of the Law Offices of Robert A. Polisky (www.rphealthlaw.com), is a healthcare attorney based in Los Angeles. Robert represents healthcare providers and companies, including billing companies and their subcontractors, in healthcare transactions, healthcare regulatory (including HIPAA, Medicare enrollment and reimbursement, and fraud and abuse), and general business law. Robert opened his law firm last April after spending over 8 years in-house at Alliance HealthCare Services and, for several years before that, working at healthcare law firms, clerking for a federal judge, and interning at the U.S. Department of Justice.