Complying with the HIPAA final Omnibus Rule

Many aspects of the law have changed since its initial enactment

Margie Satinsky, MBA, President, Satinsky Consulting, LLC

HIPAA has been with us for more than a decade, but the federal agencies responsible for writing and enforcing this complex law have only recently published final rules that reflect the current, official government position on how various aspects of this complex law should be interpreted and implemented. The Omnibus Final Rule was published in the Federal Register on in January 2013 and took effect March 23rd. "Covered entities" – including medical providers/practices, health plans and healthcare clearinghouses that transmit health information electronically, Business Associates, and subcontractors of Business Associates (i.e. Agents) are required to be in full compliance by September 23.

Ms. Satinsky

The Omnibus Final Rule modifies HIPAA Privacy, Security and Enforcement Rules, Breach Notification Rules under the HITECH Act of 2009, and the Genetic Information Nondiscrimination Act. It implements statutory amendments under the HITECH Act of 2009, strengthens privacy and security protection for individuals' health information, modifies the definition of a "breach", and strengthens privacy protections for genetic information, among other changes.

Durham practice management consultant Marjorie Satinsky tells *Forum* readers what they need to know.

Q&A

What is HIPAA?

In 1996, the federal government passed the Health Insurance Portability and Accountability Act (HIPAA). Its purpose was to provide assurances that the healthcare system would keep personal health information private. The Administrative Simplification portion of the law had five parts: the Privacy Rule, Transactions and Code Sets Standards, the Security Rule, the Employer Identifier Standard, and the National Provider Identifier Standards. The HITECH Act of 2009, part of the American Recovery and Reinvestment Act (ARRA), both modified some of the provisions of the Privacy and Security Rules and added requirements. Other relevant statutes are the Interim Final Regulations on implementation of Breach Notification; Federal Trade Commission (FTC) Final Regulations on implementation of Breach Notification; the Interim Final Rule addressing Breach Notification and monetary penalties; the 2010 Notice of Proposed Rule Making; and the Genetic Information Nondiscrimination Act of 2008. The intent of the Final Omnibus Rule is to eliminate inconsistencies among some of these statutes and bring everything together.

We're a small medical practice. Do we really have to bother with all the steps needed to comply with the Privacy and Security Rules?

Yes! When HIPAA first passed, the Department of Health and Human Services (DHHS), and its enforcement arm, the Office of Civil Rights (OCR), focused on education and voluntary compliance rather than on enforcement. That situation has changed, and an active enforcement audit program is now in effect. If you are a covered entity or Business Associate, small size does not mean you are under the radar screen. When I give presentations on HIPAA, the question I hear most often (usually from smaller practices) is whether practices really have to take HIPAA compliance seriously. Now that the federal government's HIPAA enforcement audit program has begun in earnest, many small entities have already faced stiff fines for incidents that meet the definition of a Breach. Here's an example: On January 2, 2013 DHHS announced its first HIPAA breach settlement involving fewer than 500 patients. The Hospice of North Idaho agreed to a settlement of $50,000. The agency had reported a theft of a laptop computer containing electronic PHI for 441 patients, and during the course of its investigation, OCR discovered that the Hospice had not conducted a risk analysis to safeguard PHI. Practices should understand that ignorance is not a valid defense and know that, if "willful neglect" is demonstrated, the financial penalties are even stiffer.

How has enforcement changed since HIPAA went into effect?

DHHS now does a preliminary investigation of every complaint. If the preliminary review indicates a possible violation of HIPAA rules due to willful neglect, the investigation automatically proceeds. If the preliminary review does not show willful neglect, DHHS has the option of trying to achieve voluntary corrective action.

A 30-day cure period factors into the determination of the size of the penalty. The clock starts running at the time the entity (i.e., Covered Entity, Business Associate, or Subcontractor) learns of or should reasonably know of the problem. DHHS

has a formal and proactive audit program in place in order to identify noncompliance with HIPAA. Practices and other covered entities should take heed and act now to ensure that they are meeting the requirements of the law. I am aware of several medical practices that attested to being HIPAA compliant when they applied for financial incentives under Meaningful Use and are now targets for audit. Questionable HIPAA compliance may jeopardize their receipt of the federal subsidy.

How does the Omnibus Final Rule enhance the rights of individuals with respect to PHI?

The Omnibus Final Rule strengthens limitations on the use and disclosure of PHI for marketing and fundraising purposes. Individuals can now request electronic copies of PHI, and Covered Entities must provide it in the form requested by the individual if readily producible, or in a readable form and format agreed to by the Covered Entity. Individuals can request transmission of a copy of PHI directly to a designated person. In such cases, the Covered Entity must verify the identity of the individual making the request and take reasonable steps to ensure that the email address of the recipient is correct. Individuals who pay out of pocket in full for a service can restrict disclosure of that information to a health plan. To help parents and guardians, Covered Entities now have an easier process for disclosing proof of immunization to schools in those states that have school entry and other similar laws. There's more clarity in the procedures for notifying individuals of a Breach. When individuals request PHI, Covered Entities must provide the requested information within 30 days, with a one-time 30-day extension.

How has the definition of a Breach changed, and what are the guidelines for determining and reporting a Breach?

The manner of determining whether or not a Breach has occurred remains more subjective than many in the health industry would like it to be. Still, the Omnibus Rule modifies and clarifies the definition of Breach and the risk assessment approach. Under the Omnibus Final Rule, a Breach is defined as: an impermissible use or disclosure of PHI unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. Rather than focusing on potential harm to the individual, as in the HITECH Act of 2009, the new language speaks to the responsibility of a risk assessment, performed by the Covered Entity or Business Associate, to assess the nature and extent of the PHI, the unauthorized person who used the PHI or to whom it was disclosed, whether or not the PHI was actually acquired or viewed, and the extent to which the risk has been mitigated. A common example of a possible Breach is a lost or stolen laptop computer. The loss or theft itself does not necessarily mean a Breach. If the owner can retrieve the laptop

The price of noncompliance: a HIPAA penalties primer

Violations of the HIPAA Privacy and Security Rules have three types of associated penalties – civil monetary penalties, criminal penalties, and penalties for violation of the breach notification provision. It is possible to be "double dinged" – i.e., to receive both a civil penalty and a penalty related to Breach notification.

Improper use or disclosure of PHI can result in four categories of civil monetary penalties reflecting increasing levels of culpability by individuals, employees, and/or organizations. State attorneys general (AG) are authorized to pursue civil actions for HIPAA privacy and security violations that have threatened or adversely affected a resident of that AG's respective state. The state must notify DHHS of a suit before or as soon as feasible after filing.

Civil Penalties The following apply to covered entities, Business Associates, and to subcontractors (i.e., agents) of Business Associates.

- $100-$50,000 per violation for an unknowing privacy violation by a covered entity or Business Associate, with a $1.5 million maximum/calendar year penalty for violations of an identical provision.
- $1,000 - $50,000 per violation for a violation for which it is established that the violation was due to reasonable cause and not to willful neglect, with a $1.5 million maximum/calendar year penalty for violations of an identical provision.
- $10,000 - $50,000 per violation for which it is established that the violation was due to willful neglect and was corrected in a timely manner, with a $1.5 million maximum/calendar year penalty for violations of an identical provision.
- $50,000 per violation for a violation in which it is established that the violation was due to willful neglect and was not timely corrected, with a $1.5 million maximum/calendar year penalty for violations of an identical provision.

Criminal Penalties For the violation to be criminal, the individual who committed the violation must have done so willingly, knowing the implications of divulging the PHI. As with the civil penalties, there are different levels of severity for criminal violations.

- $50,000 per violation and up to one year in jail.
- For violations committed under false pretenses, $100,000 per violation and up to five years in jail.
- For violations where there was intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm, up to $250,000 per violation and up to 10 years in jail.

and forensically show that there was no Breach, then there's nothing to report. But if the laptop can't be retrieved, there is a Breach that must be reported to the individuals affected and possibly to the media and to the Centers for Medicare and Medicaid Services (CMS).

How does the Omnibus Rule modify the HIPAA Privacy Rule to protect genetic information as required by the Genetic Information Nondiscrimination Act (GINA) of 2008?

GINA prohibits discrimination based on an individual's genetic information in health coverage and employment contexts. Genetic information is defined as the genetic tests of an individual or an individual's family members and about diseases or disorders manifested in an individual's family members. A distinction is made between genetic tests and medical tests such as HIV tests, complete blood work, cholesterol testing, and liver function tests. This particular provision applies primarily to health plans.

Should my practice revise its (NPP) and redistribute it to patients?

The Notice of Privacy Practices (NPP) must be revised. There have been many changes since the initial passage of the HIPAA Privacy and Security Rules. For example, the NPP now must have language regarding patient authorization for most uses and disclosures of psychotherapy notes, uses and disclosures of PHI for marketing purposes, and disclosures regarding the sale of PHI. There must also be a statement regarding patient authorization for uses and disclosures not specifically described in the NPP. New language must mention an individual's right to opt out of fundraising communications. Healthcare providers must clearly acknowledge their obligation to restrict use and disclosure to a health plan upon request by an individual who has paid out-of-pocket in full for a specific service.

Healthcare providers are not required to print and distribute a hard copy of the revised NPP to every patient. However, within a year after the new NPP goes into effect, they must make the revised NPP available for patients to read. They can use a summary version, provided that the full NPP is readily available. As has been the case from the outset, providers must document the patient's acknowledgment of the right to review the NPP or refusal to exercise it. Providers should also post the new NPP in a clear and prominent location. Again, they can post a summary, provided that the full version is available. Providers should also post the new NPP on their websites. If patients have granted permission to receive practice information by email, the practice can send the revised NPP electronically.

What are good resources for additional information?

- The Final Omnibus Rule was published in the Federal Register on January 25, 2013. The link is *www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf*. The material identifies modifications and additions, citing both public comment and rationale for DHHS' final decisions.
- The North Carolina Healthcare Information and Communications Alliance (NCHICA) has already revised the sample Business Associate Agreement and is working to revise other sample tools. Go to *www.nchica.org* for additional information.
- The website of the Office of Civil Rights contains instructions for submitting a Breach form: *www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html*.

Has a Breach occurred?

One of the major changes in the 2013 Omnibus Final Rule applies to the definition of a "Breach" – i.e., the unauthorized use or disclosure of PHI. We're talking about "unsecured" PHI – PHI that is not secured through a technology or methodology specified by DHHS that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals (e.g., encryption). An impermissible use or disclosure of unsecured PHI is now considered to be a reportable breach unless the covered entity, Business Associate, or subcontractor (i.e. Agent) of a Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

The burden of proof regarding a Breach requires a four-part risk analysis. For example, a lost or stolen laptop computer isn't always a breach. The conclusion depends on answers to the following questions:

1. The nature and extent of the PHI, including the types of identification and the likelihood of re-identification
2. The unauthorized person who used the PHI or to whom a disclosure was made
3. Whether or not the PHI was acquired or viewed
4. The extent to which the risk to the PHI has been mitigated