Revisiting HIPAA Compliance

By **Margie Satinsky, M.B.A.**

The Health Insurance and Portability Act has required Covered Entities to comply with the requirements of the Privacy and Security Rules since 2001 and 2005, respectively.

Our experience includes training more than 100 medical practices and business associates on both rules. We're repeatedly struck by the inconsistencies that we see. Some organizations approach Health Insurance and Portability Act (HIPAA) compliance thoughtfully, carefully and correctly; others take the easiest and least expensive way out.

Let's start with three erroneous assumptions that we encounter most frequently:

1) Having a Notice of Privacy Practices (NPP) and Business Associate Agreements (BAA) constitutes HIPAA compliance.
2) Completing risk analyses for both the Privacy and Security Rules is all that needs to be done.
3) Compliance audits don't target small practices.

HIPAA compliance may be much more complex than what you have incorrectly assumed!

Changes in HIPAA Privacy and Security

HIPAA has evolved since the passage of the initial Privacy and Security Rules. One change occurred in 2009 with the passage of the HITECH Act, part of the Affordable Care Act (ACA). The most recent change occurred in 2013, with the passage of the Omnibus Final Rule. The Centers for Medicare and Medicaid Services (CMS) issued the rule in March 2013, requiring compliance by Sept. 23, 2014 (with some exceptions). Compliance with the original Privacy and Security requirements doesn't guarantee compliance with more current requirements.

We'll point out two of the major changes in HIPAA requirements. One is the definition of a "breach," i.e. the unauthorized use or disclosure of protected health information (PHI). The Omnibus Final Rule spells out four questions to ask to determine breach occurrence and sets forth the specific steps to be taken in the event of a breach.

A second change, issued in 2009 and clarified in 2013, has to do with patients' rights. Patients now have the right to pay in full for a service and ask that PHI not be disclosed to an insurer. They also have the right to request that a Covered Entity provide their PHI in electronic format.

Notice of Privacy Practices

The Notice of Privacy Practices (NBPP) that Covered Entities must make available to patients is a good place to start. If you created an NPP in 2001 and never updated it, you're non-compliant. If you have a new NPP and didn't inform patients about the changes, you're non-compliant.

There are efficient ways to notify patients about changes. You can send a letter by mail and/or by email. You can and should inform patients when they come to the office, giving them the opportunity to review the revised document.

Business Associate Agreement

The concept of the Business Associate has been part of HIPAA since the outset, but there have been major changes. A Business Associate is an organization that routinely uses PHI in order to carry out the services that it performs on behalf of a Covered Entity. Examples are your information technology software vendor or billing company.

Business Associates have much greater liability than they had when HIPAA went into effect, and they're now liable for most of the same civil and criminal penalties that apply to Covered Entities. Moreover, in 2013, CMS introduced a new concept, called "Agent" (i.e. subcontractor).

Depending on how work is done, some Business Associates outsource aspects of the work they do for Covered Entities to third parties, i.e. agents. Agents, too, are liable. If you put Business Association Agreements (BAAs) into effect in 2001 and never updated the language, you're non-compliant. If BAAs don't have agreements in place with agents, you're non-compliant.

Use of Risk Analyses to Determine Current Compliance Status

Both the Privacy and Security Rules require using a Risk Analysis (also called "gap" analysis) to determine what compliance requirements have been addressed and what

Margie Satinsky, MBA, is President of Satinsky Consulting, LLC, a Durham, NC consulting firm that specializes in medical practice management. She's provided HIPAA compliance consultation to more than 100 Covered Entities and Business Associates. Margie is the author of numerous books and articles, including Medical Practice Management in the 21st Century. For additional information, go to www.satinskyconsulting.com.

compliance requirements should be addressed going forward. We repeatedly see that Covered Entities and Business Associates assume that answering the questions constitutes compliance; it doesn't.

The questions are just a starting point. You need to keep going, listing what needs to be done, the responsible party and the timeframe. Most important, use the lists to take action steps.

HIPAA Privacy and Security Policies and Procedures

Both the Privacy and Security Rules require Covered Entities and Business Associates to have policies and procedures (P&Ps). Realistically, busy medical practices find it hard to devote time to the creation of P&Ps. We think it's not necessary to reinvent the wheel. A more reasonable approach is to customize a sample P&P to your particular situation.

Privacy and Security Rule Similarities and Differences

The Privacy and Security Rules have both similarities and differences. Both require a designated individual to take responsibility. In some organizations, the Privacy Official and the Security Official are different individuals; in other cases one person handles both Rules. Both Rules require a Risk Analysis, written P&Ps and annual workforce training.

Let's talk about differences. The Privacy Rule is administrative, and the requirements are straightforward. The Security Rule contains administrative, technical and physical components. There's a distinction between requirements that you must meet and items that you must "address."

The address approach gives you options, with the expectation that you will use good judgment. Here's an example. The Security Rule speaks to the security of your physical facility, but it doesn't require installation of a particular alarm system. The choice is up to you.

Next Steps for Enhancing Compliance

Here are suggestions for enhancing HIPAA Privacy and Security Rule compliance in your practice. Start with an honest assessment of what you have in place and where you'd like to be. Although compliance with the requirements of Meaningful Use (MU) are by no means the only reason to be HIPAA compliant, the connection between HIPAA and the MU requirements is real and important. More than one practice that thought it met the MU requirements found its financial incentive taken back because its attestation to HIPAA compliance wasn't valid.

Next, use your assessment to determine what needs to be done. Finally, get the job done in a way that recognizes your staff's competence and availability.

We have a strong opinion on what works best – i.e. collaboration between an individual within the practice designated with the responsibility for HIPAA compliance and an external expert.