Audits and Breaches and Fines, Oh My! — Part I

It's time to make sure your HIPAA privacy and security compliance program has a heart

05.01.2010

Elizabeth H. Johnson

Have you ever had that nagging feeling that you needed to take care of something, but you just didn't have time so you let it go, probably for too long? I usually feel that way about two things: exercise and yard work. Some HIPAA-covered entities feel that way about compliance with the HIPAA Privacy and Security Rules. They are cumbersome, dense, and difficult to fully implement. And even if you have implemented policies and procedures to address each requirement, your compliance program can't be a tin man. To effectively reduce risk of compliance problems and security incidents, you need to make sure the program actually functions, has been meaningfully implemented, and is refreshed periodically to address any compliance gaps created by changes in the law and your own operations. Breathing life into your compliance program takes real work, but doing so will have tangible rewards as the program becomes a living part of your organization's daily functions.

If you don't feel confident about your organization's HIPAA privacy and security compliance, now is a good time to undertake a refresher. Here are a few reasons why.

"Meaningful Use" Incentives

Let's start by discussing the carrot in this bunch. As part of the 2009 economic stimulus package, CMS was directed to provide incentive payments to eligible professionals and hospitals that make "meaningful use" of electronic health record technology and participate in Medicare and Medicaid. As part of their proposed rule to implement this requirement, CMS identified a series of "health outcome policy priorities" to be met, including "ensuring adequate privacy and security protections for personal health information." As a Stage 1 measure, eligible professionals and hospitals must "[c]onduct or review a security risk analysis…and implement security updates as necessary." If you comply with the HIPAA Security Rule, you will have met this Stage 1 requirement.

Breach Notification

If meaningful use incentives are the carrot, the rest of the motivators on this list are sticks. Breach notification is a very big stick. In August 2009, as directed by the HITECH Act, HHS issued an interim final rule requiring covered entities to notify affected patients when their protected health information is the subject of a security breach. Whether it's a lost laptop containing medical records, a misdirected fax or an intrusion by a hacker (or an unauthorized employee), these incidents may require that your organization send a letter to each person whose protected health information was affected, noting what happened, when it happened, and what you are doing to address it. You also have to notify HHS, and possibly the media. Existing notification laws at the state level have shown that sending these letters often prompts a government investigation of the organization's privacy and security compliance, and sometimes spawns lawsuits by affected individuals. Ensuring compliance prior to one of these events can mitigate

their impact, in part by minimizing the risk of a government enforcement action and as a defense to a potential lawsuit.

Government Enforcement

For several years now the Federal Trade Commission and state regulators have been taking enforcement actions against organizations that report security breaches. The pattern goes as follows:

1. Organization experiences a security incident affecting personal information
2. Organization sends a letter to affected individuals, as required by state law, describing what went wrong
3. Government regulator receives a similar notice (often required under state law) or reads about the incident in the press
4. Notice letter prompts regulator to investigate whether organization's security was adequate in light of the incident
5. Regulator alleges that incident demonstrates inadequate security, and charges organization with an unfair trade practice pursuant to the federal or state unfair and deceptive trade practices statute it enforces

In February 2009, HHS joined the party, taking a joint enforcement action with the FTC against CVS Pharmacy following multiple reports that employees disposed of prescription information in dumpsters. The result was a settlement with both agencies, including a $2.25 million payment by CVS and an agreement to implement a comprehensive, written information security program with oversight from HHS, as well as submitting to audits of compliance with that plan biennially for 20 years. This action predated the HITECH Act and HHS's breach notification rule, which now require covered entities to self-report the type of security incident that led to the action against CVS.

Increased Penalties

The HITECH Act was just full of motivators to compel HIPAA privacy and security compliance. The same statute that brought you breach notification and additional privacy and security obligations also increased the penalty amounts HHS can seek for noncompliance. Whereas penalties were previously capped at $25,000 for multiple violations of the same provision in a single calendar year, they are now capped at $1.5 million.

Mandatory Audits and State Enforcement

In case breach notification and increased penalty amounts were insufficient incentive to comply, the HITECH Act also made periodic HIPAA audits by HHS mandatory and authorized state attorneys general to enforce HIPAA. Wasting no time (and having announced days earlier his intention to seek the Senate seat soon to be vacated by Chris Dodd), Connecticut Attorney General Richard Blumenthal in January became the first state AG to exercise his newfound HIPAA enforcement authority. Blumenthal filed suit against Health Net, which allegedly lost a portable disk drive containing unencrypted protected health information, social security numbers and bank account numbers of

approximately 1.5 million past and present enrollees, including 446,000 Connecticut residents. The suit alleges that Health Net failed to notify affected individuals for approximately six months following discovery of the incident. Mr. Blumenthal already is engaged in a second HIPAA-related action, investigating an alleged breach of medical records at Griffin Hospital in Derby, Connecticut, where a radiologist allegedly accessed patient information and used it to promote his services offered at another medical facility.

Threats to Medicaid and Medicare Reimbursement

In case you were thinking that the worst-case scenario in a breach situation is allegations of HIPAA violations and a potential fine, let's consider the case of Wentworth-Douglass Hospital in Dover, New Hampshire. That facility has been the subject of an investigation by the New Hampshire attorney general following an alleged breach of patient medical records. What's different about this investigation is that CMS joined the investigation, sending surveyors from the New Hampshire Department of Health and Human Services to examine not only privacy and security issues, but also patients' rights and quality assurance in order to determine whether the facility meets the "conditions of participation" for reimbursement by Medicaid and Medicare.

With all these compelling reasons to revisit your HIPAA privacy and security compliance, you may be wondering where to start. In next month's issue of Shorts, we'll provide a road map to reevaluating HIPAA compliance. In the meantime, our attorneys frequently assist covered entities of all shapes and sizes in implementing HIPAA privacy and security compliance programs. If you have any questions about this article or need assistance with HIPAA or the new HITECH requirements, please contact us today.

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075