Audits and Breaches and Fines, Oh My!

It's time to make sure your HIPAA privacy and security compliance program has you covered

06.25.2010

Elizabeth H. Johnson

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 (followed by a discussion of what you can do to improve your program).

Meaningful use incentives. As part of its proposed rule to implement "meaningful use" incentives, the Centers for Medicare & Medicaid Services (CMS) dictated that 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 for "meaningful use."

Breach notification. You probably know by now that your organization is obligated to report breaches of protected health information (PHI) to both affected individuals and Health and Human Services (HHS) (and, in some cases, the media). Existing breach notification laws at the state level have taught us that sending the requisite notifications often prompts a government investigation of privacy and security compliance and sometimes spawns lawsuits by affected individuals. Ensuring compliance prior to one of these events can mitigate its 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, regulators have been taking enforcement actions against organizations that report security breaches. In the typical pattern, the regulators investigate, find the incident demonstrating inadequate security, and charge the organization with an unfair trade practice pursuant to federal or state law. A case in point was the HHS-FTC joint enforcement action against CVS Pharmacy. 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 to submit to audits of compliance with that plan biennially for 20 years.

Increased penalties. The HITECH Act was 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 compliance incentive, the HITECH Act also made periodic HIPAA audits by HHS mandatory and authorized state attorneys general to enforce HIPAA. The Connecticut attorney general has already brought such an action, and

Office for Civil Rights (OCR) has indicated that it intends to audit every covered entity that reports a breach affecting more than 500 people.

Threats to medicaid and medicare reimbursement. In case you were thinking that the worst-case scenario in a breach situation would be allegations of HIPAA violations and a potential fine, 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.

What to Do? Further Progress along the HIPAA Brick Road

With all these compelling reasons to revisit your HIPAA privacy and security compliance, you may be wondering where to start. Some suggestions:

Know your obligations. Your first step is to identify all legal requirements governing your organization. For privacy and security purposes, these are enumerated in the HIPAA Privacy, Security, and Breach Notification Rules. You need to identify each requirement that should lead to some "end product" or response by your organization. Depending on the requirement, that could mean a documented policy or procedure, a set of security reminders, training programs, a complaint process, an incident response plan, etc. If you've never asked a lawyer to review your program to determine whether each of these end products is addressed, this might be a good time to consider that step.

Identify and address gaps. Once you have identified all of the requirements that require an end product, it's time to review your program to see if it actually consists of all those pieces. Is anything missing? Where are your gaps? Once you have found the gaps, they need to be addressed, which may mean drafting a policy, conducting training, instituting a new procedure, or preparing some other "end product," depending on the requirement you are trying to address.

Test your program and consider lessons learned. Assuming you have all the pieces in place, it's time to consider how well they actually work. If you have a complaint process in place as is required, how effective is it? Has it ever been used? If not, should you test it to determine how well it would work? The same questions can be asked of your security incident response plan, your procedure to address individuals' requests for access and amendment of their information, your contingency or emergency mode operation plans, and other required aspects of the HIPAA rules. Your actual experiences using these procedures should inform your updates to them – what worked, and what did not? If you haven't had an actual situation requiring you to put the procedures into practice, reconsider them in light of operational changes and consider a "tabletop" test – a test run to determine whether and how they would work. If it comes up short, it's time for some modifications to the approach.

Security rule compliance. Security Rule compliance deserves some special consideration. Whereas Privacy Rule compliance is primarily administrative, such as implementation of policies and procedures, Security Rule compliance is one part administrative safeguards and two parts physical and technical safeguards. That means that covered entities have to take a multidisciplinary approach to compliance. When we assist clients in a Security Rule compliance review, we always ask to meet with their IT personnel or provider. You simply cannot assess compliance with this rule unless you ensure that the physical and technical security controls are in place. More than likely, you will have to explain the legal obligations to your IT staff and, through a series of discussions with them, determine whether their existing security measures, policies, and procedures meet the rule's requirements. Very often, an existing security measure is appropriate but has not been documented. In such cases, the requirements are not met, due to the lack of documentation.

Another important aspect of the Security Rule is dealing with "addressable" implementation specifications. Covered entities may have an option not to implement those specifications denoted as "addressable," but only after they complete and document an assessment to determine whether the specification was reasonable and appropriate for the organization in light of the size, complexity, and capabilities of the organization; the probability and criticality of the potential risks to information; the cost of implementation; and the organization's technical infrastructure. This process need not be daunting, and a legal review is often appropriate in order to complete the task.

Business associates. As a result of the HITECH Act, all your business associate agreements require an update. More important, you need to make sure that your business associates are complying fully with the Security Rule, another new obligation imposed by the HITECH Act. Previously, your business associates' security measures needed only to be "reasonable and appropriate," which is a far cry from complying fully with the more than 60 specific safeguards outlined in the Security Rule. If they aren't complying, your business associates are putting your protected health information at risk. That risk is now greatly exacerbated by the breach notice obligations, which require covered entities to provide notification letters when security incidents are caused by their business associates. In other words, your business associate's security lapse could result in substantial notification costs and enforcement risks for your organization. These costs and risks are further magnified by the increased HIPAA penalties, audits, and enforcement also implemented by the HITECH Act.

Paper the problem. When the Office of Inspector General audited Atlanta's Piedmont Hospital on Security Rule compliance in March 2007, it gave Piedmont 10 days to respond to a list of 42 questions and requests. To comply with a request like that, you want to have all your compliance paperwork pulled together in a single location, fully organized, and up to date in advance of receiving the inquiry. Once you determine that you have all the requisite pieces documented, you must get organized. At a minimum, that means collecting together all the following.

- All requisite HIPAA privacy policies and procedures

- All requisite HIPAA security policies, procedures, security plans, security reminders, documentation of access rights, etc.
- Requisite HITECH breach response procedures
- Notice of privacy practices
- Log of HIPAA training
- Accounting of disclosures for the past six years
- Hybrid entity designation (if applicable)
- Log of security incidents
- Your organization's business associate agreements

The new HITECH requirements have substantially increased the obligations of health care providers and their business associates, and the stakes are high. Now is an excellent time to review your HIPAA privacy and security compliance programs and their implementation.

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