Audits Breaches and Fines Part 2 - Further progress along the HIPAA brick road

Hospice EndNotes June 2010

06.03.2010

Elizabeth H. Johnson

In last month's issue of *Endnotes*, we covered the "why" of HIPAA compliance. Now let's consider the "how." How exactly do you review your HIPAA privacy and security compliance program and ensure that all the requisite bases have been covered?

Know Your Obligations

Your first step is to identify all your legal requirements. For privacy and security purposes, these are enumerated in the HIPAA Privacy, Security and Breach Notice Rules. You need to identify each requirement that must result in some "end product." 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 the requirements for 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, you'll need to address them, and this 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 (which is required), how well does it work? Has it ever been used? If not, should you test it to determine whether 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? What didn't? If you haven't had an actual experience putting 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 (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 I assist clients in a Security Rule compliance review, I 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 those 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 for completion of the task.

Business Associates

As a result of the HITECH Act, all your business associate agreements require an update (yes, it's required). More important, you need to make sure that your business associates are fully complying 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 full compliance 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, get organized. At a minimum, that means collecting together all the following:

- All the requisite HIPAA privacy policies and procedures
- All the requisite HIPAA security policies, procedures, security plans, security reminders, documentation of access rights, etc.
- The requisite HITECH breach response procedures
- Notice of Privacy Practices

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

- Log of HIPAA training
- Accounting of disclosures for the past six years
- Hybrid entity designation (if applicable)
- Log of security incidents
- All of your organization's business associate agreements

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