HIPAA—Before and After HITECH

Will the HITECH Act Increase Compliance Activities?

I visited a physician’s office last year and the waiting room was full. The receptionist asked, in a loud voice, “Why do you need to see the doctor today, Gerry?” I looked around the waiting room and observed a number of patients waiting to hear my response.

When I use that example during HIPAA training sessions, my clients laugh and acknowledge similar experiences.

In a number of small physician practices it appears that the main—and possibly only—HIPAA privacy compliance activity is providing the Notice of Privacy Practices and attaining a written acknowledgement of receipt by the patient, along with any restrictions on disclosure. These offices may have a book of policy templates, but it likely has not been reviewed or customized based on organizational reasonability to comply. In other words, the policies document that they do things that they actually do not do. The odds are that few or no HIPAA security compliance activities have been performed or documented.

**GENERAL COMPLIANCE RESPONSE**

Will the HITECH Act influence how covered entities comply with HIPAA? On paper it appears that it should, due to the promise of increased penalties which will be used to fund increased monitoring/audits. In order to understand future response to compliance with HIPAA due to the HITECH Act, we need to understand response up to now.

Compliance with any rule appears relatively simple at a high level, but it is more complicated at a detailed level. When you examine the standards and the implementation specifications and determine your gaps, risk and mitigation plan, the amount of activity and impact on resources can be substantial.

Whether we are talking about compliance with HIPAA, HITECH or the highway speed limit, monitoring and penalties play an important role with response. If we are late to a meeting and need to get there on time we tend to break the speed limit. As soon as we see a police officer, we slow down. We comply with the speed limit because we want to prevent a ticket, points, fines and further delay. With HIPAA, covered entities are motivated to comply when there is a fear of fines and organizational embarrassment, or both. In addition, there is a direct correlation between the amount of human and monetary resources and the level of compliance with HIPAA.

An organization’s response to federal, state and local laws depends upon real or perceived risk of monetary penalties or embarrassment or both, and available human and monetary resources. For example, if the risk of “non-compliance” is high and human and monetary resources are available, a functional organization will normally mandate a comprehensive compliance program. If any of these variables are reduced, it is likely that the compliance program will be less comprehensive. As a result, large organizations tend to respond more. Medium-sized organizations tend to respond less. Small organizations tend to respond the least.

In small organizations, there are fewer human and monetary resources and the perceived risk is low. In small and sometimes medium-sized organizations, the HIPAA Privacy and Security Officers already have a full-time job. How can they find the time to address HIPAA?

The best chance to observe a formally documented, comprehensive HIPAA privacy and security compliance program is in large, functional organizations. The perceived risk is higher; more human and monetary resources are available; and there is a good chance that an executive mandate has been formally established.

**THE HITECH FACTOR**

So will the HITECH Act influence the variables at play? That remains to be seen. Initial perceived risk has increased due to the promise of increased monitoring and penalties from the HIPAA/HITECH police. Increased perceived risk will likely result in a general increase in HIPAA compliance activities. Over time the perceived risk must become real in order to sustain increased compliance activity levels.
The HITECH Act also increases the scope of compliance responsibilities for business associates. As a result, business associates have the same requirements for compliance as covered entities. It seems likely that business associates will perceive risk of monetary penalties and/or embarrassment or both to be high and will therefore implement an executive mandate for compliance and provide adequate human and monetary resources. While an incident at a covered entity could result in monetary fines and or embarrassment or both, a serious incident for a Business Associate is more likely to have a negative impact on current and future business. That is high risk.

In addition to the overall risk, monetary and human resource variables at play, the HITECH impact on HIPAA should increase compliance activities given the requirements and timeframes to get them done. The first step for any covered entity or business associate is to review and update their policies and procedures against the regulations, guidance documents and studies that affect privacy and security that will be released through 2012. For example, under the HIPAA security requirements you must have security incident procedures policies and procedures. Under the HITECH Act there is a related new requirement that mandates you to notify patients and members of a breach of their unsecured protected information. There is also a requirement to implement encryption of PHI. Your organization was required to do this administrative (e.g. new Breach Notification Policy and Procedure) and technology work by last Sept. 18, 2009. Thus, this was your first giant step into the new national privacy and security policy and procedures environment.

The next giant step will come by February 2010, when new regulations, guidance, and studies for the following areas will be released:
- Regulations to modify the HIPAA Enforcement Rule to implement revised penalty structure.
- Regulations to extend certain HIPAA Security Rule provisions to business associates.
- Guidance on technical safeguards to carry out security.
- Regulations to extend certain HIPAA Privacy Rule provisions to business associates.
- Regulations to modify the HIPAA Privacy Rule’s provisions regarding right to request restrictions, minimum necessary and access.
- Regulations to modify the HIPAA Privacy Rule’s provisions regarding marketing and fundraising.
- Regulations to clarify that certain entities are HIPAA business associates.
- Guidance on the HIPAA Privacy Rule’s requirements for de-identification.
- A study of the HIPAA Privacy Rule’s definition of “psychotherapy notes” to including certain test data and mental health evaluations.

After that, the next giant step happens In June 2010 when the new accounting for disclosures requirement will be in place. A patient or member will now be able to ask for an accounting of all treatment, payment, and health care operations disclosures from any and all your electronic records. Under HIPAA a covered entity needs to account for the unusual disclosures such as sharing with law enforcement or report any misdirected confidential information. Under the HITECH Act, a covered entity must report each and every disclosure of its ePHI related to treatment, payment and health care operations.

Another giant step happens in August 2010 when the following regulations and guidance are released:
- Guidance on what constitutes ‘minimum necessary’ for purposes of the HIPAA Privacy Rule.
- Regulations to modify the HIPAA Enforcement Rule to implement willful neglect provisions.
- Regulations to modify the HIPAA Privacy Rule to generally prohibit selling health information without patient or member authorization.

The final giant step is scheduled for Feb. 18, 2012, when regulations to modify the HIPAA Enforcement rule to implement provisions for sharing civil money penalties or settlements with harmed individuals will be published. This is the last of three changes to HIPAA enforcement.

CONCLUSION

In the short term the HITECH Act will increase HIPAA compliance activities given the requirements and timeframes to get them done. For the long term, the impact of the HITECH ACT on HIPAA covered entities and Business Associates compliance activities remains to be seen based on the risk, human and monetary resource variables at play. The bottom line is that an organization (covered entity or business associate) can not properly address and document HIPAA/HITECH compliance activities based on risk without adequate human and monetary resources.

Susan A Miller, JD, has 35 years of professional leadership experience spanning teaching, biochemistry research and law. Since 2002, Susan has provided independent consultation and legal services to hospitals, clearinghouses, accrediting agencies, the Massachusetts Medical Society and the Department of Health and Human Services, Centers for Medicare and Medicaid in health care regulations and has written content for manuals and technology tools.

Gerry Blass is President and CEO of Blass Consulting LLC and has 34 years of experience in healthcare information technology and compliance. Gerry formed Blass Consulting in 2002 to provide Healthcare IT professional consulting services, including HIPAA, IT management, strategic planning and project management; along with software that automates the management and documentation of healthcare compliance activities. Gerry is a member of HFMA and HIMSS.