Protection Detail
Protecting Against Breach of Electronic Protected Health Information

Our Winter 2010 JHIM article, “HIPAA Before and After HITECH—Will the HITECH Act Increase Compliance Activities,” along with our Spring 2010 article called “Pro-Active Audits of Information System Activity—Even More Important with HITECH” both have one underlying concern—the need to protect against a breach of protected health information (PHI).

The HITECH Act of 2009, with increased financial penalties, plus the potential for government audits and monitoring, and an expanded scope of information security requirements, along with the need to demonstrate compliance for the meaningful use information security requirements, should result in a common focus and framework for covered entities—to protect and secure electronic protected health information (ePHI). The time to focus is now, if not yesterday.

Back in “the day”, most healthcare organizations stored health information in a central database in a single data center. The users accessed the information via “dumb” terminals which could not store local health information. Electronic health information was much less vulnerable to unauthorized access.

Today, most HIPAA/HITECH covered entities that we have worked with or talked to have a much higher vulnerability for unauthorized access to confidential electronic data (both ePHI and business confidential data) due to the various and numerous locations where the data resides. For example, if user workstations are not locked down, confidential data could reside on hard drives, CD’s, and pen (USB) drives. Confidential data can reside on other portable devices such as laptops. Recent HHS breach reports indicate that the most common reason for breach is theft, including lost or stolen laptops. The fact that theft of laptops is a common reason for breach should and has made us all sit up and take notice. It should be no surprise that the HITECH Act requires encryption of vulnerable ePHI. It was what was left out of the HIPAA Security Rule!

So what comes first, the chicken or the egg? Do you encrypt all confidential data in vulnerable locations, or do you reduce the locations of your ePHI. We believe you do both. You need to encrypt vulnerable ePHI where it will continue to exist, such as on authorized laptops and pen drives. You also need to lock down user workstations for a large percentage of your users, and centralize user data on network servers that are technically and physically secure. By locking down the majority of user workstations, you will reduce the risk of unauthorized access to your confidential data significantly. In addition, by encrypting known authorized locations such as laptops and pen drives, you will reduce the risk even further.

The first step is to do an assessment of where your confidential data exists today. It will no doubt have changed from the first time you did a risk assessment under the HIPAA Security Rule. Then rate the risk of vulnerability for unauthorized access. Finally determine your mitigation plan based on risk. That process sounds familiar, right? So you need to do that in order to avoid major financial penalties for negligence under the HITECH Act, and in order to protect and secure your confidential data. Remember the HITECH Act has vastly upped the monetary penalties. The former ceiling is now the floor! The penalties can be as much as $1.5 million.

You also need to assess your software vendors that remotely host any your vulnerable ePHI. Are they SAS70 certified? Can they provide proof of their information security program, such as policies and procedures, workforce training, technical testing and results, mitigation of known vulnerabilities, physical security, disaster recovery and business continuity planning, monitoring and audits, and more. The fact that they host your confidential data means that they are in control of protecting and securing it and you should make sure that they do.
you do not have that control, you need to investigate what they are doing and make sure that they are doing what you would do if you had control.

Remember, if the software vendor has a breach, they have to report it to you. You have to report it to HHS. HHS then reports it as a breach for your organization. At that point you may want to change your software vendor, but that is usually not a fast or easy thing to do. So you need to make sure that software vendors who remotely host your ePHI are doing their job to prevent unauthorized access to your ePHI. And you need to do that sooner than later. If you are considering a change to a new remotely hosted software vendor, make sure you have information security requirements covered in the contract, and make sure that they sign a business associate agreement (BAA) that has been updated for the HITECH Act. If you already use a remotely hosted software vendor, consider contract amendments, if necessary, and make sure they sign an updated BAA immediately since that requirement is now being enforced under HITECH. Do the same for any business associate that houses your ePHI remotely for any reason.

**SUMMARY**

Covered entities need to conduct risk assessments that cover the requirements of HIPAA, HITECH and Meaningful use, and create a process for steady and consistent mitigation of known gaps and vulnerabilities based on risk. Reducing risk of vulnerabilities of unauthorized access to your ePHI can be done via safeguards and controls, plus audits and monitoring. When reducing risk is outside of a covered entities control, audits and monitoring are required in order to demonstrate due diligence.

Know where your ePHI is stored, where it is at risk, and take steps now to reduce or eliminate the risk. Encrypt vulnerable locations. Encrypt sensitive data. By doing so, you will be protecting your organization by reducing risk of breach of ePHI.

Finally, don’t forget what is sometimes considered to be the hardest part – documenting your compliance activities in order to demonstrate evidence of due diligence in and avoid major $$$ penalties for negligence under the HITECH Act of 2009. **JHIM**

**Gerry Blass** has more than 34 years of experience in healthcare IT and compliance. Gerry provides IT and compliance consulting services, and software that automates the management and documentation of healthcare compliance activities. Blass is the President & CEO of Blass Affiliates LLC (www.blassaffiliates.com).

**Susan A. Miller, JD**, has 35 years of professional leadership experience spanning teaching, biochemistry research and law. Since 2002, Miller has provided independent consultation and legal services to numerous healthcare entities including DHHS/CMS.