LEGISLATION

Gerry Blass and Susan A. Miller, JD

HIPAA Breaches

Have You Conducted Your PHI Vulnerability Assessment?

By now we all know that PHI refers to electronic *protected* health information. Unfortunately, based on the number of breach notifications reported, it seems that PHI has been anything but protected. The authors continue to receive e-mails that report breaches on a regular basis. There are even questions being raised about the privacy and security controls or lack thereof applied to the federal health insurance exchange website (HealthCare.gov). It is difficult to imagine that the federal government's website for healthcare insurance exchange is not in compliance with the federal government's HIPAA (Health Insurance Portability and Accountability Act [of 1996]) Omnibus Rule.

As of the writing of this column, we are hearing preliminary concerns regarding the federal health insurance exchange website and hope that any privacy and security vulnerabilities that exist today will have been addressed by the time this column is published.

The overall concern, however, is the ongoing breaches of PHI and why they are occurring.

COMMON REASON FOR BREACH

The most common reported reason for breaches of electronic PHI (ePHI) has been lost or stolen unencrypted portable devices and other electronic media. We can easily identify how common this is by looking at the U.S. Department of Health and Human Services' (HHS) "Wall of Shame."

Typical portable devices and media include laptops, tablets, flash drives, compact discs (CDs), external hard drives, smartphones and more. The keyword here is *unencrypted*. If lost or stolen devices are encrypted according to HHS standards, there is no breach.

WILLFUL NEGLECT

So after four years of breach notifications (required by the Health Information Technology for Economic and Clinical Health [HITECH] Act, the Breach Notification Interim Final Rule and now Omnibus Rule requirement), if a breach event is the result of an unencrypted portable device, the conclusion is potentially going to be willful neglect and the resulting penalties will then be very costly, as in the millions of dollars for the larger entities and approaching one million dollars for smaller entities.

Add to that the potential for civil action lawsuits, cost of providing free credit report access to individuals involved in the breach, damage to reputation, potential for additional audits and corrective action plans and the overall negative impact can be very extensive. And all of this could simply be due to a copier hard drive or a flash drive.

BREACH EXAMPLES

The authors are certain that many, if not all of you have read news about breach events. But just in case, here are some examples:

The Office for Civil Rights (OCR) settled a case with Affinity Health Plan for $1.2 million that involved several photocopiers Affinity had rented. Affinity had surrendered the tools to the owner without erasing the data. The photocopiers were then sold to a national news network. which used the found ePHI as material for a TV expose.

In summer 2013, there was a major problem at a safety net organization about the release of 3,700 individuals' information in an e-mail. Families and caregivers spoke out after an inadvertent release of ePHI in an e-mail chain.

The OCR settled with the Massachusetts Eye and Ear Infirmary (MEEI) for

$1.5 million for the theft of an unencrypted laptop. MEEI also has a corrective action plan in place and was required to retain an independent monitor. The information on the laptop included patient prescriptions and clinical information. MEEI had self-reported this breach.

In 2012, BlueCross and BlueShield of Tennessee settled with OCR for $1.5 million when 57 unencrypted computer hard drives containing the PHI of over one million individuals had been stolen from a leased facility. This was also a self-reported breach.

TIP OF THE ICEBERG

One of your reporters writes a weekly healthcare information report and can state unequivocally that these reports are only the tip of the iceberg.

When the OCR reported that they were going to enact more aggressive enforcement, they really meant it. As example, Leon Rodrigues, OCR Director, stated in a September 2013 HIMSS Privacy and Security Forum that if the breach is by a Business Associate (BA), OCR will investigate both the Business Associate and its Covered Entity (CE).

BEYOND THE FIREWALL

In today's world, the security perimeter has changed dramatically; it no longer ends at the firewall. And the firewall is now very porous—often with our permission.

Many healthcare entities' perimeter is now so far beyond the edge that it is but a dim horizon. We may not even be able to predict the edge of the security perimeter as it encompasses cloud storage and use. Do you know where all your cloud vendor(s) servers are? Do you know if your cloud vendor owns all the servers or do they rent them? Do you know where your ePHI is stored? Is it stored within the United States' borders or *offshore*, where information privacy and security rules may be very different? Are you notified by your cloud vendor(s) when new servers are added and does the notification include the entity name and country?

Remember when you wanted no openings in your firewall that the IT shop did not approve of and control? Well, any and all security perimeters now have many openings, such as for more and more remote workers, portal access for patients and providers, mobile tools including laptops; tablets; and smart phones that travel with your workforce and websites and other social media.

ASSESS, ASSESS, ASSESS

To reduce risk of breach, covered entities and BAs first need to identify where they are vulnerable for breach, evaluate the risk and implement a mitigation plan. We call this kind of assessment a *PHI Vulnerability Assessment*. It should include considerations for hardcopy and electronic PHI.

GET STARTED!

First, make a list of all categories of locations where PHI can exist in your organization. Typical examples are portable devices (list them separately), multiuser workstations in public settings, single-user workstations, servers, remote access, remote hosts, Wi-Fi transmission, e-mail transmission, other transmission to the open network, copiers, fax machines, external hard drives, backup tapes, transporting of PHI, BYOD, BYOA, portals, hardcopy and electronic disposal and more. For each category or type of PHI location, examine current controls (policy, physical, technical) and future plans; gaps; risk likelihood; and impact, and whether risk mitigation is necessary. If so, assign risk mitigation tasks and manage them. If not, document why.

CONCLUSION

It is no mystery that the HITECH Omnibus Rule includes increased responsibilities and liabilities for BAs and more requirements for covered entities to know how their BAs are protecting their PHI; no mystery that encryption is considered to be a business requirement to protect vulnerable PHI; no mystery why penalties have skyrocketed, along with potential for civil action lawsuits and more; no mystery why the Office of Civil Rights audits are mandated for covered entities and BAs. Enough is enough! Yes, the technology revolution and the categories of locations of unprotected health information have increased tremendously over the years and that is why we keep reading about breaches. But that is no longer an excuse. CEs and BAs now know via the Omnibus Rule that they must put *Protected* back into their PHI. **JHIM**

Gerry Blass has more than 35 years of experience in health IT and compliance. Blass provides IT and compliance consulting services and software called ComplyAssistant that automates the management and documentation of healthcare compliance activities. Blass is the President & CEO of Blass Consulting and Compliance, LLC.

Susan A. Miller, JD, has 40 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 the National Institute of Standards and Technology (NIST) and HHS. She has co-authored two OCR audit protocol prep books, *HIPAA Security Audit Prep Book* and *HIPAA Breach & Privacy Audit Prep Book*.

Blass and Miller are co-founders of HIPAA 411, a Linked-in group.