LEGISLATION

By Gerry Blass and Susan A. Miller, JD

Security Risks

Mobile Devices Are Here to Stay, But Challenges Remain

THOSE OF US WHO experienced the implementation of healthcare applications during the 1990s know that for the most part, physicians did not want to use them. There was a simple reason why: It was easier to write an order on a paper pad and make a note in a paper chart than it was to remember a sign-on, enter a password and navigate a series of screens to enter an order. Let's face it, when something is not easy to do, the natural thing is to avoid doing it.

Since the 1990s, a number of factors have changed. For starters, the kids of the 1990s grew up using computer technology. It is second nature to them to use new technology. Secondly, the technology of today has simplified the use of tools like electronic medical records (EMR). So the young interns and physicians of today love to use what they have always used, and the older physicians finally have technology that may actually be easier to use than the pen and a pad of paper. Those two strong motivational factors could explain the current explosion in the use of technology in healthcare today.

THE iDOC WILL SEE YOU NOW

The use of portable devices—especially smartphones and tablets—are turning physicians into iDocs. These consumer tools are moving into the healthcare environment at break-neck speed. We have seen increased usability—that is good. But, we also have seen increased security risks—that is bad.

We have learned over the past 20 years that new technology cycles can initially increase the risk of unauthorized access to data due to new vulnerabilities. Portable devices such as laptops and flash drives are some examples of tools vulnerable to breach. We have seen that the majority of breaches of ePHI have been caused by lost or stolen portable devices.

Cycles begin when new technologies become available and are implemented. Vulnerabilities are exploited, and then controls are implemented. We have recently seen the same cycle with physicians' use of text messaging ePHI. Physicians love the ease of use, but in many cases, there is a still a need to implement controls to prevent unauthorized access.

We have recently seen the evolution of the HIPAA rule with the HITECH Act over the past three years in an effort to keep up with advances in technology. In the federal agency arena we have seen updated guidance from the National Institute for Standards in Technology (NIST) and in the private arena the HITRUST CSF (Common Security Framework).

So now that the physicians are on board with technology (for the most part), we should begin to see more and more information organizational, administrative, physical and technical controls to protect unauthorized access to ePHI. It is the next natural step in the cycle.

Here are some examples:

Administrative. Strong policies and procedures around the use of portable devices. For example, should personal devices be allowed in the work environment? They can currently distract physicians with personal information, such as a text from a friend during a patient visit, never mind in the surgery suite. Not good. And, they may not have the technical control standards required by the healthcare organization. Ah, but there are apps for that, no doubt. Workforce training should cover the risks and vulnerabilities and sanctions for violations including those involving improper use of mobile devices.

Physical and technical. ePHI will either not be stored on personal devices or the devices will be protected by strong authentication, encryption (including text messages) and a GPS location app that also has the capability to wipe the media. These controls are available today and will continue to improve. And, why not store all data on a secure server rather than on the device itself?

Legal framework. With all of the above said, let's take a look at the current legal and regulatory framework for mHealth devices, which includes six of the federal alphabet soup agencies: the FCC, FTC, FDA, NIST, OCR and ONC. Each of these agencies has one or more direct or indirect controls mobile devices.

- The FCC regulates communications including all private users; they manage all the federal frequency bands.
- The FTC works in the area of consumer protections especially privacy and identity protections; they have a new consumer privacy protection report out on their web site.
- The FDA has regulatory authority over all mobile medical devices, possibly including EHRs.
- NIST writes security guidance for the federal departments and agencies including Special Publication (SP) 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, and other SP 800 documents to assist with security such as risk assessment, various types of encryption, security controls, plus a freely downloadable NIST HIPAA Security

We have learned over the past 20 years that new technology cycles can initially increase the risk of unauthorized access to data due to new vulnerabilities.

Toolkit that can be used in audit and risk analysis.

- OCR writes and enforces the HIPAA Privacy, Security, Breach and Enforcement rules and guidance.
- ONC is partnering with OCR to determine the privacy and security needs of mobile devices.

It is important for Covered Entities to stay current with the latest rules and guidance from these agencies.

CONCLUSION

The use of mobile devices in healthcare is here to stay and will continue to advance into the healthcare environment. We have witnessed a revolution that has been fueled by the government-sponsored expansion of EHRs and tremendous advances in mobile-device engineering, making technology easier to use.

Like any revolution, there is good and bad. The "bad" has been ePHI breaches due to lost or stolen mobile devices. There are solutions: as we witnessed with computer viruses, the solution was virus protection software. Today we have several different types of controls, such as encryption to protect against unauthorized access of ePHI on mobile devices. The cycle of new technology, new opportunities, new vulnerabilities and new controls to offset the vulnerabilities continues. The key is to know where your vulnerabilities exist, prioritize risk and mitigate risk via controls and monitoring.

It is really the same thing that healthcare organizations have been doing since the dawn of electronic computing. What makes it more challenging today is the speed of technology advances and the need to keep up with the implementation of controls and to comply with the regulations from various federal agencies. **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 President & CEO of Blass Consulting and Compliance LLC.

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 NIST and HHS. Blass and Miller are co-founders of HIPAA 411, a linked-in group.