HIPAA and Your Mobile Devices

Not taking the appropriate precautions can be very costly.

BY MARK TERRY

Have you ever accessed patient data offsite using a laptop computer, tablet, or smartphone? It should come as no surprise that the trend is toward the use of mobile devices over desktop computers—anyone who's ever accessed their email, gone on Facebook, or watched TV or videos on a phone or tablet would be aware of this.

In fact, in November 2014 The Wall Street Journal ran an article by Christopher Mims with the provocative title, "The Web Is Dying; Apps Are Killing It." As he points out in the article, "All those little Chiclets on your screen are apps, not websites, and they work in ways that are fundamentally different from the way the Web does."

According to mobile analytics company Flurry, about 86% of phone Internet time is spent on apps and just 14% on the Web. More to the point, though, is how healthcare utilizes mobile devices and how HIPAA relates to it.

According to mobile analytics company Flurry, about 86% of phone Internet time is spent on apps and just 14% on the Web.

HIPAA 101

Although it seems unlikely that any reader is unaware of The Health Insurance Portability and Accountability Act of 1996 (HIPAA), let's go over a couple of points relevant to mobile devices. Title I of HIPAA protects health insurance coverage for workers and their families. It's not particularly relevant to this discussion.

Title II, however, which is known as the Administrative Simplification (AS) provisions, put in place national standards for electronic healthcare transactions. Within Title II there are many components, but the two that are most relevant to mobile security are the Privacy Rule and the Security Rule.

Privacy Rule

The Privacy Rule covers the use and disclosure of Protected Health Information (PHI) held by so-called "covered entities," which generally means insurers, medical service providers, and various healthcare clearinghouses and employer-sponsored health plans. It also extended the "covered entities" to business associates of those entities. People who feel that the Privacy Rule has been violated (i.e., someone leaked their private health information), can (and should) report it to the Department of Health and Human Services Office for Civil Rights (OCR).

Security Rule

The Security Rule complements the Privacy Rule, and unlike the Privacy Rule that relates to all PHI, both paper and electronic, the Security Rule applies specifically to Electronic Protected Health Information (EPHI). It describes three types of security safeguards: administrative, physical, and technical.

Continued on page 100

HIPAA (from page 99)

It is within these rules that HIPAA and mobile devices start to butt heads.

HIPAA and Mobile Devices

The Advisory Board Company published a daily briefing in June 2014 for healthcare executives, in which it interviews Stacy Cook of Barnes & Thornburg LLP, to discuss HIPAA and mobile devices. They wrote, "Mobile device users transmitting and receiving PHI via public Wi-Fi or email applications on mobile devices are using unsecure mobile networks, putting PHI at risk of interception. Most mobile devices can take and store photographs, which can be a compliance concern if the pictures violate their privacy. Also, any mobile device that is relatively small in size, providers must be concerned about misplacement and/or theft resulting in the unintended loss of PHI."

The briefing goes on to say that mobile devices pose problems with HIPAA due to storage challenges. That is to say, is any data on the mobile device stored on the device or in the cloud? "Cloud storage is popular among mobile device users, and users storing PHI in clouds may be putting the cloud provider at risk if a HIPAA business associate agreement is not signed." And as a recent headline-leading series of stories indicated when a number of celebrity photographs were hacked from a cloud storage service, the cloud isn't as secure as we all once thought.

Access via Portal?

For physicians, the key point is related to how you might be accessing patient information. If you're using a smartphone, tablet, or laptop to access your Electronic Health Record (EHR), or someone else's EHR, you're in good shape. "If you're interacting with your EHR or a hospital EHR, or somebody else's EHR through a secure web browser in an iPad environment or other tablet, that's okay," says Ron B. Sterling, CPA, MBA of Sterling Solutions, Ltd. (Silver Spring, MD), a consultant on the use of technology in healthcare and author of Keys to EHR Success. "But if you start saving screenshots of things on your iPad, that's a different story. As long as it's not identifiable PHI, then you really don't have to worry about it."

In other words, if your patients utilize the patient portal component of your EHR, you should be fine because it's designed with HIPAA security and network security in mind. But if you save data to your computer, tablet, or phone and those devices get stolen, be prepared to pay a penalty.

If you save data to your computer, tablet, or phone and those devices get stolen, be prepared to pay a penalty.

David J. Zetter, of Zetter Healthcare (Mechanicsburg, PA), says, "Physicians need to realize that the Security Rule encompasses all PHI that is electronic, of any type, over the Internet, within any hardware structure. They need to realize that whatever they're accessing their EHR with, it's incumbent upon them to use the same rules when accessing that information on any other devices."

Basic Security?

Sterling points out that pulling data via browsers is generally encrypted, especially when interacting with EHRs. The biggest problem is when physicians interact with patients via email. Although the email is probably secure via your Internet Service Provider (ISP), it doesn't provide the type of documentation that healthcare regulations require and which are automatic with the patient portals of EHRs.

"Let's suppose a patient sent you a clinical question or a photograph of something on their feet," says Sterling. "So you respond, they respond, you're going back and forth, and now you're giving clinical advice. And now that needs to go into the clinical record. How's that going to happen? And even if you do it two months later, and the patient sends you another email, they may have just taken your last email and responded back. All the previous emails are in the thread, but the topic is different." It's far better to utilize the patient portal.

Device Documentation

Far more complicated is what to do about the specific devices you and your staff use in your practices. Sterling points out that it goes back to the three components of HIPAA Security Rules: confidentiality, integrity and access. "The access issue is passwords," says Sterling, "and making sure you evaluate people who need access versus people who don't need access. You have to train your people."

Physical security and technological security basically involve encrypting patient information and monitor protection so people can't read confidential health information over your receptionist's shoulder. It also applies to physical security, meaning that the various devices are protected from random access.

"For example," says Sterling, "if I had a computer that had patient information on it, it's not a good idea to leave it on the front seat of your car. It would better to store it in the trunk and best yet to take it with you. When it comes to accessing devices, you want to make sure you don't store passwords on the devices. It's really a matter of following HIPAA guidelines. It's a process. It's not like you can do it once and forget about it. It's also very important because there are significant financial penalties for any violation."

Zetter underlines that point. "Most of our clients are starting to realize that they can't keep practicing medicine the way they used to and have their heads stuck in the sand concerning privacy and security. They have to be much more aware of what the requirements are because if

Continued on page 102

HIPAA (from page 100)

there's a breach, it could bring down the entire practice if they don't have certain precautions in place."

He suggests that for any device used in the practice, whether a tablet, laptop, PC, or even smartphone, "go through the process of documenting what the device is going to be used for, how it's going to be used, what types of communication are going to be done on it, and find out what needs to be done to make it compliant with all the rest of your hardware."

This may require hiring an expert on HIPAA compliance, not just an IT expert who isn't familiar with HIPAA security. "They have to be fully aware of it," says Zetter, "and aware of what the risk assessment is. The risk assessment is going to be performed on that piece of equipment as well as the other equipment, especially if you're seeing Medicare patients and are participating in 'meaningful use' requirements."

Staff & Devices

One question that comes up is employees and their own cell phones, especially smartphones with cameras built in. Zetter suggests the medical practice should have a policy in place regarding use of those cameras. "What can they use them for, where are they allowed to use them? Because anybody can snap a picture and accidentally have a patient in there and put it up on Facebook or wherever, and the next thing you know, the patient finds out they've been posted and you've got a breach. All these little things, people need to be aware that these are possibilities, things that can happen. They might not set out to do something wrong, but they need to be aware of these types of things to prevent them from happening."

Make sure you don't store passwords on your mobile devices.

Recommendations

HealthIT.gov offers a great deal of advice on protecting and securing health information. Here are recommendations.

1) Use a password or other authentication. Any mobile device can be set up with a password, a personal identification number (PIN) or some sort of authentication. Many

Continued on page 103

HIPAA (from page 102)

smartphones are also being manufactured with fingerprint scanning to unlock the phone.

2) Install and enable encryption. Many devices do this automatically. It varies from device to device, but if you're utilizing mobile devices, do a little research to determine what, if any, encryption is being used. HealthIT.gov points out, "When you encrypt data in motion, you prevent unauthorized virtual access to the data while it is in transit (e.g., accessing an EHR system or lab test results using your mobile device). Consider carefully the risks associated with sending text messages containing protected health information. To improve the protection of information being sent in a text message, consider using secure messaging which is encrypted, instead of SMS (Short Message Service), which is not."

3) Install and activate remote wiping and/or remote disabling. If your device should be stolen or lost, this service allows you to erase the data on the device remotely. It's worth pointing out, of course, that you should regularly back up your data, so if you are forced to wipe your hard drive or memory, you haven't lost all the data.

4) Disable and do not install or use file-sharing applications. File sharing software lets individual users connect to each other and trade files. It basically lets other people access your device without your knowledge. Determine if this is on any of your devices and disable it.

5) Install and enable a firewall. A personal firewall protects against unauthorized connections. It intercepts incoming and outgoing attempts to access your device or network and sets up a series of rules that block or permit access. Many operating systems have built-in firewalls, but they don't work if you don't turn them on, i.e., enable them. You can also download and install a firewall on your mobile device.

6) Install and enable security software. This applies to antivirus software, spam filters, and anti-malware. Not as broadly used for mobile devices, there is some available or it may already be installed. If you are downloading security apps for your phone or mobile device, do a little research before purchasing.

7) Keep your security software up-to-date. As mentioned earlier, security is not a one-shot deal. You need to turn it into a process, where you're keeping security and privacy software and processes up-to-date and evaluated regularly.

8) Research mobile applications (apps) before downloading. Generally speaking, any app that is downloaded to your smartphone or device has access to everything else on your

Continued on page 104

HIPAA (from page 103)

device. HealthIT.gov states, "Before you download and install an app on your mobile device, verify that it will perform only functions you approve of. Use known websites or other trusted sources that you know will provide reputable reviews of the app. Understand the risks you are introducing to your mobile device."

9) Maintain physical control. In other words, lock devices in drawers or filing cabinets, lock your mobile device's screen when not in use. Don't leave them lying around, keep them with you. And don't share!

10) Use adequate security when sending or receiving health information over public Wi-Fi networks. HealthIT.gov says, "Regardless of whether you are using a public or private Wi-Fi connection (such as at your house), you can use a virtual private network, which encrypts the information you send. You can also use a secure browser connection. You will know if you have a secure browser connection if you see 'https' in the website address." They also recommend turning Wi-Fi off, as well as location services and Bluetooth functionality when not being used. That sounds completely inconvenient, but be aware of your locations and Wi-Fi networks when accessing PHI.

11) Delete all stored health information before discarding or reusing the mobile device. There are various ways of completely deleting data, often using specific software or products for it. In some cases, if you're intending to discard devices and need to delete any PHI on it, you may need to utilize a degaussing technology such as a powerful magnet, or physically destroy the hard drive.

The Buck Stops…

We live in an electronic world where privacy and security is more tenuous and fragile than ever before. It's important that physicians realize how important following HIPAA guidelines are for all the PHI that crosses through their practices. Zetter says, "The physician owners are ultimately accountable for anything that happens in their practice and outside their practice with their staff. So they need to be educated, which is already a requirement with HIPAA. They need policies and procedures in place." **PM**

Mark Terry is a freelance writer, editor, author and ghostwriter specializing in healthcare, medicine and biotechnology. He has written over 700 magazine and trade journal articles, 20 books, and dozens of white papers, market research reports and other materials. For more information, visit his websites: www.markterrywriter.com and www.markterrybooks.com.