Codify
BY AAPC

Eli's Rehab Report

HIPAA: Are You Leaving PHI Vulnerable to Breaches?

Compliance review leads to startling settlement.

When the **Office of Civil Rights** (OCR) opened a compliance review after a physical therapy facility had a laptop stolen, it led to a $1.7 million HIPAA settlement. The message sent out to all healthcare providers and facilities was loud and clear: Risks need to be addressed immediately.

"OCR's investigation revealed that [the company] had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information (ePHI) was a critical risk," the **Department of Health and Human Services** (HHS) said in an April 22 news release on the case. "While steps were taken to begin encryption, [the company's] efforts were incomplete and inconsistent over time, leaving patient PHI vulnerable throughout the organization."

Following the investigation, the company agreed to pay $1,725,220 to the government to settle potential violations, and plans to create a corrective action plan to fix the issues that the OCR found.

How this impacts you: It's not practical for a medical practice or facility to have a pair of eyes on every mobile device at all times. Laptops, tablets, mobile phones and other devices can be left in examination rooms or at unattended desks, making your equipment vulnerable to thieves. Worse yet, if you have PHI on those devices and the information isn't encrypted, you're at risk of finding yourself in the same situation as the company in the case above. Consider the following tips to ensure that your PHI is safe on mobile devices, from the HealthIT.gov publication, Mobile Device Privacy and Security:

1. Always Use A Password. It may seem annoying to have to type in a password or PIN number every time you want to access your tablet or laptop, but if there's PHI on it, you have no choice. Make sure your password is at least six characters long and has a combination of uppercase and lowercase letters as well as a keyboard character (such as the "*" symbol). In addition, make sure your device requires the password after a specific period of inactivity. For example, if you leave your laptop on the table for five minutes without using it, you'd have to enter the password to use it again.

2. Install Encryption Software. One of the problems that the company had in the case profiled above was that the stolen laptop was not encrypted. In other words, anyone could read what was on it in plain English. If you add encryption to your mobile devices, the data cannot be converted into readable words without a decryption key or password. You should not only have encryption enabled for data stored on your device, but also for any information that you send which might contain PHI.

3. Activate Remote Disabling. It may sound like something out of Blade Runner, but the ability to erase your hard drive from a remote location is very much a realistic option. If you have this capability on your devices and the devices are stolen, you can wipe the data clean remotely, so the thief won't have access to any of the information on the laptops or tablets. Although many mobile phones already have this option built-in, you can often download remote disabling software after purchasing the device if you are interested in adding it to any of your products.

4. Disable File Sharing. You might think it's very convenient to allow your employees to "file share" with each other or outside billing companies, which means that you can trade computer files, but this type of application also leaves your device vulnerable to unauthorized users, and it's a bad idea.

5. Maintain a Firewall. If your device doesn't already have a firewall installed, it's time to get one. The term "firewall" simply means that you can block outsiders from getting into your server remotely and accessing your information.

6. Install Security Software. Most of us have security software installed on our laptops to ensure that no viruses can enter (which often can steal your information) □ but many of us don't keep it appropriately updated, which makes our computers vulnerable to attacks. Ensure that your security certificate is up to date and that you run software scans regularly.

7. Ensure That Apps Are Safe. Downloading an app to your phone, tablet or computer might seem harmless, but it may not always be. Some apps can copy your address book or other private information and then send it to another company. Always ensure that apps are trusted before adding them to your devices.

8. Avoid Public Wi-Fi Networks. Using a portable device over a public Wi-Fi connection makes you vulnerable to interception of your PHI. Always use a secured connection when you're on the internet using your mobile device.

9. Delete Stored PHI. You might think you're being "eco-friendly" by recycling your portable device or handing it to a warehouse when your practice gets new devices, but your PHI could still be on there, even if you think you've deleted it. Instead of simply sending your files to the "recycle bin," you should use software specifically designed to overwrite your computer with other data.

10. Keep It Near You. Although this step might seem obvious, most problems with stolen devices occur when the owner of the computers let them out of their sight, and then theft occurs. Keep your mobile products near you and use screen locks at all times to ensure that you're the only one who can get in.

Resource: To read more about the settlement, visit www.hhs.gov/news/press/2014pres/04/20140422b.html