OASIS Alert

HIPAA Compliance: 3 Tips to Safeguard Patient Data On Mobile Devices

Prevent unauthorized access or risk big fines.

Recent breaches underline the importance of keeping electronic protected health information on mobile devices secure. Is your agency taking proper precautions?

Watch out: With the Jan. 2 announcement of the very first HIPAA breach settlement affecting less than 500 patients, you should do everything possible to avoid being the next target. This HIPAA breach involved you guessed it ePHI stolen off of unencrypted laptops that the staff used for field work. The **Hospice of North Idaho** will pay $50,000 as part of the breach settlement.

Unfortunately, the growing trend of mobile-device use in healthcare is quickly outpacing adoption of appropriate HIPAA security measures. "Given the rapid adoption of mobile devices against the backdrop of the breach incidents reported, there's been a growing concern about the use of these devices in the health field because of their vulnerability," **Joy Pritts, JD**, Chief Privacy Officer for the **HHS Office of the National Coordinator for Health Information Technology**, says in a recent statement.

"Mobile devices are particularly vulnerable to loss and theft because of their small size and portability," writes **Catherine Barrett**, principal consultant with the Washington, D.C.-based **Federal Working Group**, in an article for the **American Bar Association's Health Law Section**. "Mobile devices are typically small, light and highly visible to would-be thieves looking for an opportunity to take a phone left behind in a public space, such as at a restaurant."

And theft is perhaps the biggest risk for compromised HIPAA privacy and security. A 2011 survey that the **Center for Democracy and Technology** conducted of 600 U.S. healthcare professionals and organizations found that theft accounted for 66 percent of reported data breaches during the preceding two-year period.

Bottom line: If you're allowing staff to use mobile devices to access, manipulate and store ePHI, you must have:

1. Physical Safeguards

2. Technical Safeguards

3. Administrative Safeguards

Heed 4 Physical Safeguards

"Unlike laptops and PCs, clinicians are far more likely to use their own personal mobile devices, rather than employer-issued mobile devices, to access and exchange ePHI," Barrett notes. She points to a **Health Research Institute** study that found about 81 percent of the more than 2,000 physicians surveyed used their personal mobile devices to access ePHI.

This is a particularly sticky problem, because you don't have control over the physical security of clinicians' personal mobile devices. Therefore, your staff policies regarding mobile devices, and how your staff will secure the device when not in use, are of the utmost importance, stresses **Jim Sheldon-Dean**, director of compliance services for **Lewis Creek Systems, LLC**. This is especially true when you're allowing staff to access health systems from their mobile devices.

Do this: Barrett points to the following examples of physical safeguards you should employ:

1. Keep an inventory of personal mobile devices that healthcare professionals use to access and transmit ePHI;

2. Store mobile devices in locked offices or lockers;

3. Install radio frequency identification (RFID) tags on mobile devices to help locate a lost or stolen mobile device; and

4. Use remote shutdown tools to prevent data breaches by remotely locking mobile devices.

Technical Safeguards: Start with 2-Factor Authentication

Most of all, you want to protect the data the ePHI stored on your mobile device. And you can begin with access controls and authentication. "Typically, data stored on personal mobile devices is not encrypted," Barrett points out. "Thus, ePHI stored on a mobile device could be retrieved and shared by anyone with access to the mobile device."

"The lack of authentication on mobile devices presents a risk that any user of the device could access ePHI stored on the device," Barrett warns. Authentication refers to the passwords, passcodes and other barriers you install on your device that prevent others from accessing any data.

Pay attention: But a simple password login is no longer enough. "A two-factor authentication is becoming the standard now," Sheldon-Dean says. This may involve, for example, a password entry and a PIN or even a more sophisticated method.

You should also encrypt any transmissions of data to and from mobile devices, Sheldon-Dean says. Doing this ensures that no unauthorized access occurs while sending or receiving ePHI.

"Mobile devices that use public Wi-Fi or unsecure cellular networks send and receive information risk exposing ePHI," Barrett cautions. "Unless mobile device users connect to a secure web site to transmit data or connect using a VPN ("virtual private networking"), which encrypts data to and from the mobile device, there is a risk of ePHI could be compromised."

Encrypting any ePHI stored on the mobile device is also essential, Sheldon-Dean adds. You'll also need to consider your backup methods for stored ePHI, especially if staff members are creating or altering patient records via their mobile devices. Proper data syncing can keep your patient records up-to-date in real time.

Best bet: According to Barrett, you can utilize the following specific technical safeguards:

Install and regularly update anti-malicious software (also called malware) on mobile devices;

Install firewalls where appropriate;

Apply encryption to ePHI and metadata;

Install IT backup capabilities, such as off-site data centers and/or private clouds, to provide redundancy and access to ePHI;

Adopt biometric authentication tools to verify the person using the mobile device is authorized to access the ePHI; and

Ensure mobile devices use secure, encrypted Hypertext Transfer Protocol Secure similar to those used in banking and financial transactions to provide encrypted communication and secure identification of a network web server.

Focus on Policies, Procedures, Training for Administrative Safeguards

Administrative measures mostly involve the policies and procedures you put into place for mobile-device use. Staff training is also crucial. You must train staff on the risks and costs of breaches, as well as how to secure their mobile devices in compliance with HIPAA security and privacy standards, Sheldon-Dean says.

Tips: Barrett highlights the following examples of administrative safeguards:

Conduct periodic risk assessments of mobile device use;

Establish an electronic process to ensure that an unauthorized third party does not destroy or alter the ePHI;

Establish processes and procedures to appropriately protect ePHI in a mobile device environment, including establishing encryption and security breach protocols for mobile device use; and

Train clinicians on the processes and procedures to use when accessing ePHI on mobile devices, and educate clinicians on the risks of data breaches, HIPAA violations and fines.