Eli's Rehab Report

HIPAA Compliance: Follow These 'Official' 10 Steps To Protect PHI On Mobile Devices

Check out HHS' brand new web tools.

As you're trying to catch up with your HIPAA privacy and security compliance for mobile devices, the **U.S. Department of Health and Human Services** (HHS) is catching up, too. HHS recently launched a new online tool for protecting electronic protected health information (ePHI) on mobile devices (www.healthIT.gov/mobiledevices). Straight from HHS, here's your most essential to-do list for keeping ePHI safe and secure on your device.

1. Enable User Authentication:

ü Configure your mobile device to require passwords, personal identification numbers (PINs) and passcodes.

ü Set your mobile device so that it activates screen locking after a set period of inactivity -- this is the "time-out" or "automatic logoff" feature.

ü Mask the password, PIN or passcode fields so people cannot see it.

2. Use Encryption:

ü Encrypt data both stored locally ("at rest") and data sent by your mobile device ("in transit").

ü Encrypt data at rest by either utilizing your mobile device's built-in encryption, or by downloading an encryption app from a trusted source.

ü Encrypt data in transit by using a virtual private network (VPN) or secure browser connection.

3. Enable Remote Wiping/Disabling:

ü Enable "remote wiping" on your mobile device to remotely erase the data on the device if it's stolen or lost.

ü Enable "remote disabling" on your mobile device to remotely lock the device. (After you recover the mobile device, you can unlock it.)

4. Disable File-Sharing:

ü Disable any file-sharing feature on your mobile device to prevent others from accessing data on your device without your knowledge, as well as from placing viruses or malware on your system.

ü Do not download any file-sharing apps or programs to your mobile device.

5. Enable A Firewall:

ü Enable the firewall feature on your mobile device to block unauthorized connections.

ü Download and install a firewall on your mobile device if you don't have a built-in firewall.

6. Install Security Software:

ü Install security software to protect your mobile device from malware, spyware viruses and spam.

ü Ensure that you enable the security software if it's already installed on your mobile device.

ü Keep your security software up-to-date for optimal protection.

7. Beware of Mobile Apps:

ü Research mobile apps before you download and install them, and verify that they're from a trusted source.

ü Require management, HIPAA team or IT approval before staff can download any apps to mobile devices used to store, transmit or view ePHI.

8. Maintain Physical Control:

ü Whenever you can't keep your device with you physically, keep your mobile device in a secure location, such as a locked drawer or room, where nobody but you can access it.

ü Don't share your mobile device with others.

ü Lock your screen whenever you're not using your mobile device.

9. Beware of Public Wi-Fi Networks:

ü Use secure Wi-Fi connections that use encryption; don't use public Wi-Fi connections.

ü Use a virtual private network (VPN) and a secure browser connection.

10. Delete All ePHI Before Discarding the Device:

ü Use a software tool that thoroughly deletes, or "wipes," all the data stored on your mobile device before you discard or reuse it.

ü Follow the HHS Office for Civil Rights (OCR) guidance to wipe all PHI from devices: www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.