OCR Offers Tips for Securing PHI on Mobile Devices

Last month the U.S. Department of Health and Human Services Office for Civil Rights (OCR) published a newsletter dedicated to the important issue of protecting sensitive health information when mobile devices like tablets, cell phones, or laptops are in use ("Mobile Devices and Protected Health Information").

Theft, unsecure networks, malware among topics highlighted by OCR

One obvious risk discussed in the OCR's newsletter is theft of a mobile device containing protected health information (PHI). If that PHI is not secured, a breach can occur, leading to required HIPAA (Health Insurance Portability and Accountability Act) breach notifications kicking in. Healthcare organizations have been burdened with hefty penalties for not following those HIPAA regulations after a breach in electronic PHI is discovered, so awareness prior to an incident — and even better yet, measures to prevent security breaches altogether — can save providers headaches down the road.

The newsletter also discussed the issue of mobile device default settings that are potentially unsecure. For instance, device default settings might allow a connection between the device and unsecure file sharing, cloud storage, Bluetooth, or Wi-Fi. The OCR says that healthcare entities should anticipate this likelihood and configure devices that will collect or transmit PHI in such a way that they will only connect with secure networks. (And of course this will involve a degree of workforce training to ensure that when staff use the same mobile devices away from the secure network they do not allow connections to networks in public places.)

Another potential — and common — ePHI security pitfall can occur when the device is corrupted by a virus or malware. Naturally this can be an e-nightmare for any user, but when the device contains PHI, the stakes are substantially higher. And the OCR points out that the entry point for a PHI breach doesn't always come from an obvious place, like a virus: "A seemingly innocuous mobile app or game could access your contacts, pictures or other information on your mobile device and send such data to an external entity without your knowledge."

The OCR's Tips to help protect and secure PHI while using mobile devices

- Implement policies and procedures regarding the use of mobile devices in the work place – especially when used to create, receive, maintain, or transmit ePHI.
- Consider using Mobile Device Management (MDM) software to manage and secure mobile devices.
- Install or enable automatic lock/logoff functionality.
- Require authentication to use or unlock mobile devices.
- Regularly install security patches and updates.
- Install or enable encryption, anti-virus/anti-malware software, and remote wipe capabilities.
- Use a privacy screen to prevent people close by from reading information on your screen.
- Use only secure Wi-Fi connections.
- Use a secure Virtual Private Network (VPN).
- Reduce risks posed by third-party apps by prohibiting the downloading of third-party apps, using whitelisting to allow installation of only approved apps, securely separating ePHI from apps, and verifying that apps only have the minimum necessary permissions required.
- Securely delete all PHI stored on a mobile device before discarding or reusing the mobile device.
- Include training on how to securely use mobile devices in workforce training programs.

more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.

NELSON HARDIMAN
HEALTHCARE LAWYERS