October 2017

Mobile Devices and Protected Health Information (PHI)

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Mobile devices, including cell phones, tablets, and laptops, are increasingly ubiquitous in many work environments – including healthcare organizations. The use of mobile devices in the workplace can be convenient and productive, but organizations should realize the risks associated with increased usage of mobile devices – especially when mobile devices are used to create, receive, maintain or transmit electronic PHI (ePHI). Entities regulated by the HIPAA Privacy, Security, and Breach Notification Rules (the HIPAA Rules) must be sure to include mobile devices in their enterprise-wide risk analysis and take action(s) to reduce risks identified with the use of mobile devices to a reasonable and appropriate level. See 45 C.F.R. § 164.308(a)(1)(ii)(A)–(B).

Risks when using mobile devices to store or access ePHI

Many threats are posed to electronic PHI (ePHI) stored or accessed on mobile devices. Due to their small size and portability, mobile devices are at a greater risk of being lost or stolen. A lost or stolen mobile device containing unsecured ePHI can lead to a breach of that ePHI which could trigger HIPAA breach notification obligations for a HIPAA covered entity or its business associate (the entity). Additional risks could arise when using personal mobile devices to store or access ePHI. If an entity does not permit the use of personal mobile devices for work activities, especially activities involving ePHI, policies should be in place and enforced that make such prohibitions clear. Entities permitting the use of personal mobile devices must include such devices in their enterprise-wide risk analysis and implement security measures sufficient to reduce those risks to a reasonable and appropriate level.

Mobile devices, similar to many other computer systems, may be delivered by the vendor with default settings which may be unsecure. Such default settings may enable connectivity to unsecure Wi-Fi, Bluetooth, cloud storage, or file sharing network services. Entities should take steps to ensure that mobile devices are properly configured and secured before allowing the device to create, receive, maintain, or transmit ePHI. Additionally, workforce members should be trained in the proper, secure use of mobile devices to store or access ePHI. Such training could include educating workforce members on the dangers of using unsecure Wi-Fi networks, such as public Wi-Fi offered in airports and coffee shops, as well as unsecure cloud storage and file sharing services.

Workforce members should also be trained on the risks of viruses and malware infecting mobile devices. Just as with other computer systems, malicious software that infects mobile devices could provide access to unauthorized individuals which could result in a breach of PHI. Access to information on mobile devices need not be limited to nefarious actions by malicious software, but could also originate from more mundane applications. 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.

As mobile devices are increasingly and consistently used by covered entities and business associate and their workforce members to store or access ePHI, it is important that the security of mobile devices is reviewed regularly, and modified when necessary, to ensure ePHI remains protected. See 45 C.F.R. § 164.306(e).

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.

For more information and tips, see:

- OCR's Cyber Security Guidance Materials, https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
- OCR's Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html
- NIST SP 800-124 Rev. 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
- ONC's Mobile Device and Health Information Privacy and Security Resources, https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security