MedPro Group
a Berkshire Hathaway company

Risk Tips

Securing Mobile Devices in Healthcare

Mobile devices are convenient, but using them also carries risks. Mobile data security and HIPAA compliance are ongoing concerns that healthcare organizations must address.

To address these issues, healthcare leaders should establish mobile device policies and procedures to safeguard protected health information (PHI). Additionally, they should ensure that all mobile device users are educated about these protocols and aware of ongoing privacy and security concerns. Healthcare organizations also should implement data breach incident response protocols.

The following tips provide guidance for healthcare organizations and mobile device users on best practices for device security and ways to avoid risk.[1]

---

1. Enable password/PIN protection or biometric authentication on mobile devices to restrict access to authorized users and safeguard PHI.

2. Require appropriate levels of password complexity and periodic password changes as well as multifactor authentication. Ensure passwords are masked when users enter them.

3. Install and enable encryption, firewall protection, and security software (including applications that help identify and prevent viruses, malware, spyware, phishing, etc.).

4

Install and activate remote wiping and/or remote disabling. Require users to immediately report lost/stolen mobile devices so data wiping can occur before exposure.

5

Research mobile applications before downloading. Download only HIPAA-compliant applications, and use secure messaging applications.

6

Ensure that operating systems, applications, and security software are configured for full functionality and maximum security.

7

Use a secure virtual private network when connecting mobile devices to residential wireless networks, and ensure that security features are properly configured and have up-to-date firmware/operating system software.

8

Update mobile devices and applications as soon as updates are available. Automatic update deployment and installation should be used when it does not interfere with device operations.

9

Establish mobile device policies and procedures, and train staff members on them as well as on HIPAA privacy and security awareness.

10

Reinforce that staff members should maintain physical control of their mobile devices at the healthcare organization, at their residences, and in transit. Establish requirements to secure passwords, health information, and other sensitive data.

11

Implement a policy that all mobile devices used to access PHI must be registered with the healthcare organization and authorized to add, modify, remove, and access PHI.

12

Strongly encourage staff members to report any security incidents resulting from using their mobile device.

13

Do not (a) install or use file-sharing applications, (b) share passwords or user authentication, (c) knowingly allow unauthorized access to mobile devices, (d) store or send unencrypted PHI, (e) download applications without verifying that they are from a trusted source, (f) leave mobile devices unattended, or (g) use unsecured Wi-Fi networks.

14

Delete all stored PHI and other proprietary information before discarding or reusing mobile devices. Be sure to use proper disposal techniques as delineated in organizational policy.

Resource

For more information related to this topic, see MedPro's *Risk Resources: Cybersecurity*.

Endnote

[1] The tips in this publication are based on information from the following sources: U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology. (n.d.). *Your mobile device and health information privacy and security*. HealthIT.gov. Retrieved from www.healthit.gov/topic/privacy-security-and-hipaa/your-mobile-device-and-health-information-privacy-and-security; U.S. Department of Health and Human Services Health Sector Cybersecurity Coordination Center (HC3). (2023, March 23). *HC3: HPH mobile device security checklist* (Report: 202303231700). Retrieved from www.hhs.gov/sites/default/files/hph-mobile-device-security-checklist-tlpclear.pdf; U.S. Department of Health and Human Services. (n.d.). *Mobile devices: Know the risks. Take the steps. Protect and secure health information*. Retrieved from www.healthit.gov/sites/default/files/mobile_devices_and_health_information_privacy_and_security.pdf; Clements, J. (2023, April 10). *10 tips for HIPAA compliance when using mobile devices*. MOS Medical Transcription Services. Retrieved from www.medicaltranscriptionservicecompany.com/blog/10-tips-for-hipaa-compliance-when-using-mobile-devices/