



MOBILE DEVICES: CONSIDERATIONS FOR HEALTH CARE PROVIDERS

Author: Mary Beth Schneider, CRNA

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was passed by the United States Congress and set national standards for the protection of individually identifiable health information by health care providers, health plans, and health care clearinghouses¹. As these standards include the electronic transmission of individually identifiable health information, health care professionals using their personal mobile devices to receive, transmit, and store protected health information (ePHI) are also obliged to conform with HIPAA rules. With a maximum fine of up to \$50,000 per violation, the potential financial impact is eye opening.

Since HIPAA was passed, the use of personal mobile electronic devices including smart phones, tablets, and laptop computers has increased exponentially². A recent survey conducted by Netwrix found that 56% of healthcare organizations believe that their employees are their greatest threat when it comes to their security and system availability³. To this end, proper education and vigilant use of mobile devices for ePHI can help reduce this threat.

Two particular concerns for health care providers regarding ePHI are possible loss of a mobile device and possible interception of data.

Device Loss: To protect against inadvertent access to ePHI, it is essential to secure the device. Biometric identification and passwords can be used to secure access to data. Without this two-factor authentication, anyone using the device could access secure information in violation of HIPAA. Additionally, the owner of the device should log out of the device when it is not being used and also have the remote ability to clear protected health information from the mobile device if it is lost or misplaced.

Data Interception: When using the Internet, a health care provider should be aware that data can be intercepted and ePHI exposed. To reduce this risk, the health care professional has a number of options such as using a secure cellular network instead of free public WiFi provided in coffee shops, hotels, and airports. Another option is the use of a Virtual

¹ <https://www.hhs.gov/hipaa/for-professionals/index.html>

² <https://www.ben-evans.com/benedictevans/2016/4/29/the-end-of-a-mobile-wave>

³ <http://www.hipaasecurenow.com/index.php/56-of-healthcare-organizations-see-employees-as-their-greatest-threat-to-it-security/>

Private Network (VPN). A VPN uses the Internet to connect remotely to a private internal network. Also, a health care provider can look for hypertext transfer protocol secure (HTTPS) in the address bar of their browser. HTTPS is the secure version of HTTP. It encrypts communications between a browser and the website the provider is connected to. Unsecured connections transmit the data in plain text which can be intercepted.

Another option to reduce the potential for exposure of ePHI is *Encryption*. Encryption scrambles data so that it is unintelligible without the correct access codes. Mobile devices can be encrypted. Encryption can also be used to protect the transmission of data between devices as both sender and receiver use a shared code to unscramble the data.

Best practice calls for vigilance with ePHI. New mobile devices may have default settings that are unsecure. Steps should be taken to ensure that mobile devices and the transmission of data are properly configured and secured before receiving, transmitting or storing ePHI.

ADDITIONAL INFORMATION

For additional information, please refer to a recent publication from the U.S. Department of Health and Human Services⁴. This article includes the following checklist to help health care providers safely access, store, and send ePHI.

- 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.

⁴ <https://www.hhs.gov/sites/default/files/october-2017-ocr-cybersecurity-newsletter.pdf>

ABOUT THE AUTHOR

Mary Beth Schneider has been a nurse for more than 25 years and a CRNA for greater than 12 years. Her experience ranges between both private practice and academic settings. Since 2014 she has been a member of the Injured Patients and Families Compensation Fund (IPFCF) Risk Management and Patient Safety Committee.

DISCLAIMER

Articles published contain the expressed opinions and experiences of the authors and do not necessarily represent the position of the Injured Patients and Families Compensation Fund. Authors are required to make disclosure of any relevant financial relationships, which may be related to the subject matter discussed. Authors have made proper disclosure and have no relevant financial relationships that exist now or in the past 12 months.