HC3: HPH Mobile Device Security Checklist

March 23, 2023 TLP:CLEAR Report: 202303231700

HPH Mobile Device Security Checklist

Executive Summary

Mobile devices are prevalent in the health sector, and due to their storage and processing of private health information (PHI) as well as other sensitive data, these devices can be a critical part of healthcare operations. As such, their data and functionality must be protected. This document represents a basic checklist of recommended items for health sector mobile devices to maintain security, including data in motion and at rest, as well as the capabilities of the device itself.

Report

HC3 recommends the following considerations for any mobile device used within a healthcare environment:

☑ **Controlling wireless broadcasts** – Mobile devices can leverage various wireless communications protocols such as 802.11 (WiFi), Bluetooth and broadband cellular (currently 5th generation). These capabilities should be disabled and connection specifics should be deleted when not needed.

☑ **Limit connectivity** – Device owners should be cautious about which networks they connect to, especially public or other untrusted networks. Connection to residentail wireless networks should leverage the use of a VPN, should be through access points and modems that are of reputable brands, and have adequate security features properly configured and updated with the latest firmware/operating system software. Devices should ideally only be used to connect to corporate enterprise infrastructure via an approved and properly encrypted wireless network.

☑ **Application and software deployment limits** – The minimum number of applications required should be deployed to the device in order to reduce its attack surface. Applications that are used should be appropriate for the data (e.g. private health information) that they are storing and processing. The enterprise may choose to whitelist/blacklist applications as they see fit.

☑ **Operating system and software updates** – Ensure the device and all apps are updated as soon as possible. Automatic update deployment and installation should be implemented when it does not interfere with device operations.

☑ **Authentication** – Password requirements should be established and required by policy. Appropriate levels of password complexity and periodic password changes should be required for device operations, and passwords should be masked as they are being entered. Multi-factor authentication should be required as practical. Screen lock capabilities should be enabled after a set period of inactivity.

☑ **Encryption** – The Health Insurance Portability and Accountability Act requires encryption for any device that stores or processes any of the 18 categories of personal health information (PHI). End-to-end encryption is recommended for all mobile devices. Most devices have inherent encryption capabilities. Additional encryption software can be implemented as needed.

HC3: HPH Mobile Device Security Checklist

March 23, 2023 TLP:CLEAR Report: 202303231700

☑ **Data backup and cloud storage** – Data redundancy should be in practice for all sensitive information. HHS recommends the 3-2-1 rule for any healthcare organization as a data backup strategy. This applies to the most sensitive healthcare data, and requires that at least three copies of the data are maintained, stored on two different mediums, with at least one copy stored offline.

☑ **Endpoint Security software** – Security software should be installed as available. This includes anti-malware capabilities that can prevent viruses, spyware, and full-fledged cyberattacks.

☑ **Configuration management** – Operating systems, apps, and security software should all be configured for full functionality and then maximum security.

☑ **Content and conversations** – Users should periodically receive reminders (upon log-in, for example) that they are handling sensitive health data on the mobile device, and it is their responsibility to protect that data while it is stored on the device, as well as when transmitting it to/from the device.

☑ **Physical security** – Devices should be physically secured at all times, including at the enterprise facility, at the residence of the user, and in transit. Precautions should be taken by the user to ensure passwords, PHI and other sensitive data are always secure.

☑ **Remote wiping** – Mobile devices should include a remote wiping capability. Users should be required to immediately report lost/stolen devices so that data wiping can occur prior to exposure.

☑ **Inventory tracking** – Inventory tracking should include all mobile devices, including those owned by the enterprise, as well as any personally-owned devices that fall under a bring-your-own-device policy. Devices being taken out of service should be properly destroyed in such a way that data is completely irrecoverable.

References

National Security Agency: Mobile Device Best Practices
https://media.defense.gov/2021/Sep/16/2002855921/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF

HealthIT.gov: How Can You Protect and Secure Health Information When Using a Mobile Device?
https://www.healthit.gov/topic/privacy-security-and-hipaa/how-can-you-protect-and-secure-health-information-when-using-mobile-device

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback