HIPAA Compliance with SecureShield™

HIPPA Guidance for Mobile Devices

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule establishes a set of security standards for the confidentiality, integrity and availability of electronic Protected Health Information (ePHI). Healthcare providers and related entities must comply with the requirements under the Rule to protect the privacy and security of ePHI.

While mobile devices provide many benefits for healthcare providers, due to their small size and portability, they are at a greater risk of being lost or stolen. A lost or stolen mobile device containing ePHI can lead to a breach of that ePHI, which could trigger HIPAA breach notification obligations.

Given the increasing risks associated with the use of mobile devices in the healthcare industry, the Office for Civil Rights and the Office of the National Coordinator for Health Information Technology have issued guidance on the use of mobile devices and tips for securing ePHI on mobile devices.[i]

Soliton SecureShield for HIPAA Compliance

This document introduces the ten recommendations of the HIPAA guidance for mobile devices and describes how Soliton's SecureShield helps healthcare providers and related entities adopt those recommendations.

Please note that the HIPAA Security Rule does not require specific types of technology, rather requires entities to conduct their own risk analysis to define and implement reasonable and appropriate safeguards.

1. Use a password or other user authentication.

Mobile devices should require a password, PIN, passcode and additional authentication methods to gain access to the device. Requiring an additional authentication step to access ePHI hosted on corporate networks and web-based apps from remote devices provides greater security to the ePHI.

SecureShield requires users to authenticate with a username and password to access corporate networks and web-based apps where ePHI resides. With AD/LDAP integration, a centrally managed AD/LDAP username and password can be used to grant or deny user access to the SecureShield workplace.

Soliton SecureShield

Reduced Attack Surface

- Secured container completely contains desktop-based attacks
- Cache is automatically erased upon closing the browser; upon reopening, data is reloaded, unaffected by malware, ransomware, etc.
- Data cannot be accessed by other apps

Cost Effective

- Eliminates the need to set-up and configure an expensive VPN or maintain a complicated infrastructure
- Delivers the same speed as other browsers
- Less than 30% total cost of ownership compared to VDI, RDP, and VPN solutions
- Includes two-factor authentication (2FA), single sign-on (SSO) and ID Federation (optional)

Reduced IT Administration

- Manage user access to corporate data via a single point of control
- Patch, deploy and upgrade user applications with simple web application settings
- Easily block and/or disable unauthorized BYOD devices to prevent data leakage

2. **Install and enable encryption.**
Encryption protects health information stored on and sent by mobile devices.
SecureShield's encrypted browser-based connection (SSL-VPN) provides safe, controlled access to the workspace.

3. **Install and activate remote wiping and/or remote disabling.**
Remote wiping enables you to erase data on a mobile device remotely. Remote disabling enables you to lock or completely erase data stored on a mobile device if it is lost or stolen.
With SecureShield, user sessions are executed in a virtual sandbox. All content is disposed along with the sandbox each time the user closes the workplace. This ensures that sensitive health information never remains on a mobile device after the browser is closed.

4. **Disable and do not install or use file sharing apps.**
Users may install third-party file sharing apps on their devices, but file sharing can also enable unauthorized users to access the devices without the users' knowledge.
SecureShield uses sandboxing to create a workplace that is completely isolated from the local environment. Even if a file sharing app is installed in the local environment, ePHI accessed via the SecureShield workplace is completely contained within the sandbox and is isolated from local apps.

5. **Install and enable a firewall.**
A personal firewall on a mobile device can protect against unauthorized connections.
With SecureShield, installation of secure gateway is required for IP access control. The secure gateway will enable the corporate firewall for internet access.

6. **Install and enable security software.**
While it is extremely important to install and frequently update anti-malware software on mobile devices, there is no way to absolutely keep devices malware-free.
SecureShield's workplace co-exists with anti-malware software installed on a mobile device. The SecureShield workplace completely contains malware within the sandbox, thus preventing malware from spreading to the corporate network. Malware is discarded by closing the workplace.

7. **Research mobile applications before downloading.**
The guideline recommends verification of apps to be used on devices before download and installation. Not only malicious software, but even a seemingly innocuous mobile app or game could access your information on your mobile device and send such data to an external entity without your knowledge.
SecureShield provisions a preconfigured corporate workplace that only allows access to apps that have been researched, approved and installed by IT administration. The isolated SecureShield workplace prevents data sharing to the local environment, where unverified apps may exist.

8. **Maintain physical control.**
Mobile devices are easily lost or stolen due to their portability. Implement appropriate policies and procedures to mitigate the risk of unauthorized access due to device loss.
SecureShield's administration features allow you to disable a username and password to immediately block access to the workplace. Disabling the username and password ensures that no ePHI remains on remote devices and prevents data from falling into the wrong hands.

9. **Use adequate security to send or receive health information over public Wi-Fi networks.**
Public Wi-Fi networks can be an easy way for unauthorized users to intercept information. Thus, it is important to send data through a secure connection on a public unsecured network.
SecureShield uses an encrypted SSL-VPN to provide secure access between each remote device and VPN gateway to ePHI on corporate networks and web-based apps, even in an unsecured environment.

10. **Delete all stored health information before discarding or reusing the mobile device.**
When a mobile device needs to be discarded or reused by another user, it is necessary to properly wipe all sensitive healthcare data.
SecureShield does not allow devices to keep any apps or data on the local environment. In addition, disabling the user name and password will reset the workplace immediately for reuse, thus providing additional security throughout the device use cycle.

[i] https://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device