HIPAA Audits: Policies and Procedures

Targeted to Mobile Device Use

Critical considerations when conducting a risk analysis of mobile devices.

Who owns the device? A different level of control exists if the device is owned by an individual employee or if it is actually a device owned by an organization. If a mobile device is owned by an organization, the organization can control the nature and content of that device.

Are personal devices that are used at work registered? If personal devices can be used to access, store, or transmit PHI, the question should be asked as to whether employees should be required to register those devices. Many organizations have centralized security management to make sure mobile devices accessing their internal networks or resources are compliant with their security policies. Centralized security management includes: (1) configuration requirements, such as installing remote disabling on all mobile devices; and (2) management practices, such as setting policy for individual users or a class of users on specific mobile devices.

Is a virtual private network (VPN) used to exchange information so the information does not actually reside on the device? (Once the connection is broken, there is no information stored.) With a VPN, the connection between a mobile device and a server is encrypted, so information sent or received is protected due to the encrypted tunnel established by the VPN, even on an unsecured network. VPNs can reduce the risk of using a public Wi-Fi access point (hotspot) or public wired Internet connection such as at a hotel or airport. Otherwise, information can be intercepted between the mobile device and the system connection.

Is PHI from mobile devices saved onto servers? If PHI from mobile devices is saved onto servers, then a data backup would exist for any information saved on the mobile device even if it is lost or stolen.

Can mobile devices be remotely wiped or disabled if they are lost or compromised? If a mobile device is lost or stolen, there are two potential paths to reduce the risk that PHI can be compromised: remote wiping and remote disabling. Remote wiping is a feature for lost or stolen mobile devices that remotely erases all the data on the mobile device. Some mobile devices have built-in remote wipe capability that the organization or authorized user can enable. Remote disabling enables you to lock or completely erase data stored on a mobile device if it is lost or stolen. If the mobile device is recovered, it may be unlocked.

Is your workforce properly trained? Policies and procedures are not meant to be put into a binder and then hidden on a high shelf. They are intended to be used on a daily basis, and the OCR will take steps to see if your organization is doing what it said it would be doing in your policies and procedures with regard to mobile devices.

Best Practices for use of Mobile Devices

The direction that a company takes in response to the risk analysis questions above will require the development and implementation of best practices surrounding the use of mobile devices. Some best practices to consider are:

- Enabling or installing security software and with a process in place to ensure that the software is kept up-to-date
- Researching apps before downloading to ensure the apps are do not create security gaps
- Implementing policies that emphasize maintaining physical control of devices
- Training employees to use caution when using Wi-Fi – particularly free Wi-Fi – due to increase security risk and risk of casual exposure of PHI through onlookers
- Deleting all stored ePHI before reusing or discarding mobile device
- Establishing a policy and process for employees to use password protection or some authentication key to disable access if mobile device is lost or stolen
- Avoid storing data locally on mobile device
- Require encryption for mobile devices
- Disable file-sharing on mobile devices

Five Steps to Developing Policies and Procedures for Use of Mobile Devices

1. Decide how PHI will be accessed, received, transmitted, or stored via a mobile device, and how mobile devices will be used as part of your organization's internal networks and other systems
    - *For example, will ePHI be stored on a laptop? Will emails containing ePHI be accessible via a personal cell phone? How is that information stored on a network system?*
2. Conduct a risk analysis
    - *For example, will the mobile device be taken outside of the workplace? If so, what are the risks that the laptop will be lost or stolen?*
3. Determine risk management strategy, including privacy and security safeguards
    - *For example, will you require all employees who receive email containing PHI to password protect their cell phones?*
4. Develop reasonable and appropriate policies and procedures for mobile devices
    - *Your organization should have a mobile device management policy. That policy should address how to inventory those devices, what's on those devices, and what those devices are. That also means being aware, not only of the devices that you own, but the devices that your employees own, and on which device PHI may either be stored or pass through. This requires a decision as to whether to allow employees to utilize their own devices as part of handling PHI. Consider what restrictions to impose on mobile use and what security configurations and technical controls should be placed.*
5. Conduct training
    - *Train employees on how to physically secure the mobile devices so the chances of them being lost or stolen are reduced. Theft or loss is the most likely source of a breach.*