How Can You Protect and Secure Health Information When Using a Mobile Device?

1. Use a password or other user authentication

Authentication is the process of verifying the identity of a user, process, or device. Mobile devices can be configured to require passwords, personal identification numbers (PINs), or passcodes to gain access to it. The password, PIN, or passcode field can be masked to prevent people from seeing it. Mobile devices can also activate their screen locking after a set period of device inactivity to prevent an unauthorized user from accessing it.

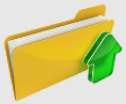
2. Install and enable encryption

Encryption protects health information stored on and sent by mobile devices. Mobile devices can have built-in encryption capabilities, or you can buy and install an encryption tool on your device.

3. Install and activate remote wiping and/or remote disabling

Remote wiping enables you to erase data on a mobile device remotely. If you enable the remote wipe feature, you can permanently delete data stored on a lost or stolen mobile device.

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, you can unlock it.



4. Disable and do not install or use file sharing applications

File sharing is software or a system that allows Internet users to connect to each other and trade computer files. But file sharing can also enable unauthorized users to access your laptop without your knowledge. By disabling or not using file sharing applications, you reduce a known risk to data on your mobile device.

5. Install and enable a firewall

A personal firewall on a mobile device can protect against unauthorized connections. Firewalls intercept incoming and outgoing connection attempts and block or permit them based on a set of rules.

6. Install and enable security software

Security software can be installed to protect against malicious applications, viruses, spyware, and malware-based attacks.

7. Keep your security software up to date

When you regularly update your security software, you have the latest tools to prevent unauthorized access to health information on or through your mobile device.

8. Research mobile applications (apps) before downloading

A mobile app is a software program that performs one or more specific functions. Before you download and install an app on your mobile device, verify that the app will perform only functions you approve of. Use known websites or other trusted sources that you know will give reputable reviews of the app.

9. Maintain physical control

The benefits of mobile devices - portability, small size, and convenience - are also their challenges for protecting and securing health information. Mobile devices are easily lost or stolen. There is also a risk of unauthorized use and disclosure of patient health information. You can limit an unauthorized users' access, tampering or theft of your mobile device when you physically secure the device.

10. 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. You can protect and secure health information by not sending or receiving it when connected to a public Wi-Fi network, unless you use secure, encrypted connections.

11. Delete all stored health information before discarding or reusing the mobile device

When you use software tools that thoroughly delete (or wipe) data stored on a mobile device before discarding or reusing the device, you can protect and secure health information from unauthorized access. HHS OCR has issued guidance that discusses the proper steps to take to remove health information and other sensitive data stored on your mobile device before you dispose or reuse the device.

Source: http://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device

Mobile Devices:
Know the RISKS. Take the STEPS.
PROTECT AND SECURE
Health Information.

Learn more at http://www.HealthIT.gov/mobiledevices

Mobile Devices and Health Information: What to Avoid

- Sharing your mobile device password or user authentication
- Allowing the use of your mobile device by unauthorized users
- Storing or sending unencrypted health information with your mobile device
- Ignoring mobile device security software updates
- Downloading applications (apps) without verifying they are from a trusted source
- Leaving your mobile device unattended
- Using an unsecured Wi-Fi network
- Discarding your mobile device without first deleting all stored information
- Ignoring your organization's mobile device policies and procedures

Five Steps Organizations Can Take to Manage Mobile Devices

1 Decide | 2 Assess | 3 Identify | 4 Develop, Document, and Implement | 5 Train

1.) DECIDE
Decide whether mobile devices will be used to access, receive, transmit, or store patients' health information or be used as part of the organization's internal networks or systems (e.g., your EHR system).

2.) ASSESS
Consider how mobile devices affect the risks (threats and vulnerabilities) to the health information the organization holds.

3.) IDENTIFY
Identify the organization's mobile device risk management strategy, including privacy and security safeguards.

4.) DEVELOP, DOCUMENT, and IMPLEMENT
Develop, document, and implement the organization's mobile device policies and procedures to safeguard health information

5.) TRAIN
Conduct mobile device privacy and security awareness and training for providers and professionals.

Understanding and Following Organizational Polices and Procedures

Health care providers and professionals are responsible for learning and understanding their health care organization's mobile device policies including:

Policies and procedures on:
- Bring your own device (BYOD)
- Mobile device registration
- Mobile device information storage
- Backup information stored on mobile devices
- Remote wiping and/or disabling

Professionals and providers should also be aware of the:
- Organization's privacy and security officer(s)
- Virtual private network (VPN)
- Mobile device privacy and security awareness and training

Mobile Devices: Tips to Protect and Secure Health Information

- Use a password or other user authentication.
- Install and enable encryption.
- Install and activate wiping and/or remote disabling.
- Disable and do not install file- sharing applications.
- Install and enable a firewall.
- Install and enable security software.
- Keep security software up to date.
- Research mobile applications (apps) before downloading.
- Maintain physical control of your mobile device.
- Use adequate security to send or receive health information over public Wi-Fi networks.
- Delete all stored health information before discarding or reusing the mobile device.

Take the Steps to Protect and Secure Health Information When Using a Mobile Device

The resource center http://www.HealthIT.gov/mobiledevices was created to help providers and professionals:

Protect and secure health information when using mobile devices
- In a public space
- On site
- At a remote location

Regardless of whether the mobile device is
- Personally owned, bring their own device (BYOD)
- Provided by an organization



Mobile Devices: Risks to Health Information

Risks vary based on the mobile device and its use. Some risks include:

- A lost mobile device
- A stolen mobile device
- Inadvertently downloading viruses or other malware
- Unintentional disclosure to unauthorized users
- Using an unsecured Wi-Fi network

Mobile Devices:
Know the RISKS. Take the STEPS.
PROTECT AND SECURE
Health Information.