Keeping your Personal Health Information (PHI) safe on your mobile devices

WiFi SECURITY

Communications Security: 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.

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.

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.

DATA SECURITY

Install and enable Security Software: Install security software to protect against malicious applications, viruses, spyware, and malware-based attacks.

Remember to regularly update your security software for the latest tools to prevent unauthorized access to health information on or through your mobile device.

Disable and do not install or use file sharing applications: File sharing software or systems allow 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.

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.

MOBILE DEVICE PRIVACY

Use a Password, PIN or Passcode: 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 lock their screens after a set period of device inactivity to prevent unauthorized use.

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. Your password, PIN, or passcode field can be masked to prevent people from seeing it.

Remote disabling enables you to lock or completely erase stored data.

Delete all stored information before discarding or reusing the mobile device: Use software that thoroughly deletes (or wipes) stored data your device before discarding or reusing the device, to protect and secure health information from authorized 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.

Remote disabling enables you to lock or completely erase stored data.

Maintain Physical Control of your device: The portability, small size, and convenience of mobile devices also makes them easily lost or stolen. Once compromised, there is also a risk of unauthorized use and disclosure of patient health information. You can limit unauthorized access, tampering or theft of your mobile device when you physically secure the device.