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

Whether you use a personally owned mobile device or one provided to you by an entity such as a health care organization, system, or medical or private practice, you should understand how to protect health information.

Follow these tips to help you secure the health information your patients entrust to you:

1. Install and enable encryption to protect health information stored or sent by mobile devices.
2. Use a password or other user authentication.
3. Install and activate wiping and/or remote disabling to erase the data on your mobile device if it is lost or stolen.
4. Disable and do not install or use file-sharing applications.
5. Install and enable a firewall to block unauthorized access.
6. Install and enable security software to protect against malicious applications, viruses, spyware, and malware-based attacks.
7. Keep your security software up to date.
8. Research mobile applications (apps) before downloading.
9. Maintain physical control of your mobile device. Know where it is at all times to limit the risk of unauthorized use.
10. Use adequate security to send or receive health information over public Wi-Fi networks.
11. Delete all stored health information on your mobile device before discarding it.

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

Find out more at HealthIT.gov/mobiledevices**.**