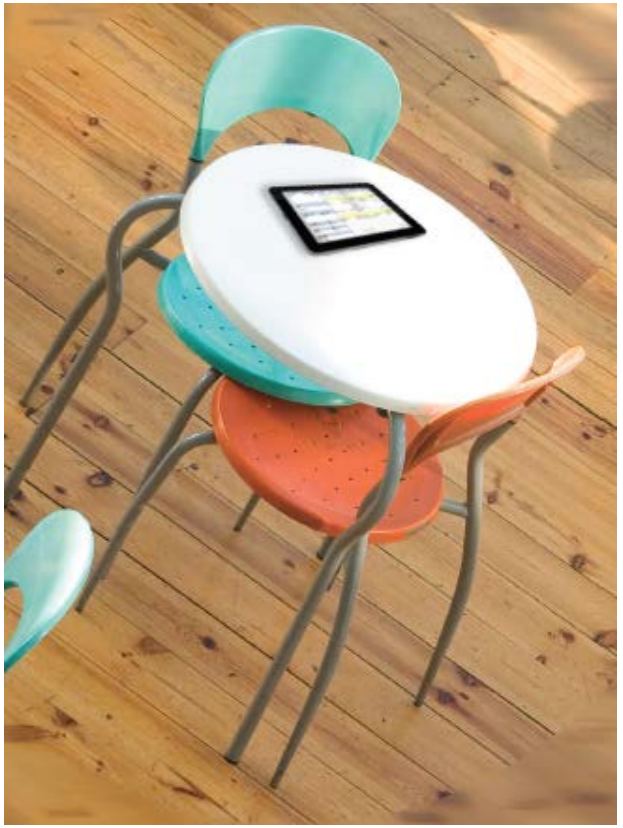
Mobile Devices:
Know the RISKS. Take the STEPS.
PROTECT AND SECURE
Health Information.

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



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: Tips to Protect and Secure Health Information

HealthIT.gov
Advancing America's Health Care

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.

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

Five Steps Organizations Can Take to Manage Mobile Devices

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.

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

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

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