

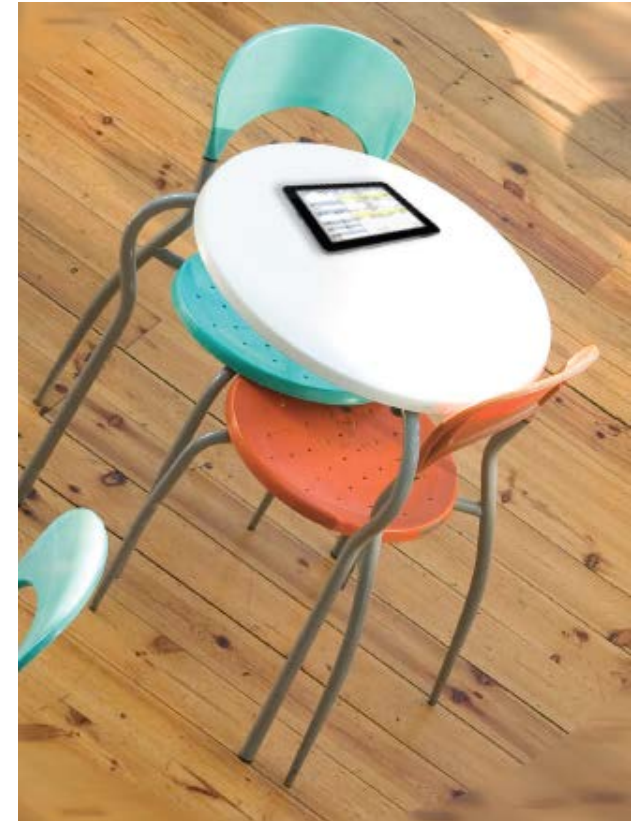


**Mobile Devices:**  
**Know the RISKS. Take the STEPS.**  
**PROTECT AND SECURE**  
**Health Information.**



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



**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 Policies 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

HealthIT.gov  
Advancing America's Health Care

Blog | Consumer Toolkit | Contact | Get Email Updates

in Partnership with the National Learning Consortium

Newsroom | Help Center | Multimedia | Search

Providers & Professionals | Patients & Families | Policy Researchers & Implementers

Benefits of EHRs | How to Implement EHRs | Privacy & Security | EHR Incentives & Certification | Health Information Exchange (HIE) | Case Studies & Data

HealthIT.gov > For Providers & Professionals > Privacy & Security > Mobile Device Privacy and Security > You, Your Organization, and Your Mobile Device

## Mobile Device Privacy and Security

### You, Your Organization, and Your Mobile Device

If you use a mobile device to access an organization's internal network or system, the owner of that network or system's policies and procedures apply to your use of the mobile device to gain such access. It is your responsibility to understand and follow the organization's policies and procedures.

Here are some questions to consider when using a mobile device to access an organization's network or system, such as an EHR:

- Does your organization have a mobile device use policy?
- Does your organization allow you to use your personally owned mobile device for work?
- Do you know who your organization's Privacy Officer and/or Security Officer are?
- Does your organization require you to register your mobile device with the organization?
- Does your organization have a Virtual Private Network?

# 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.



- 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.

HealthIT.gov

Blog Consumer Toolkit Contact Get Email Updates

in Partnership with the National Learning Consortium

Search

Newsroom Help Center Multimedia

Providers & Professionals Patients & Families Policy Researchers & Implementers

Benefits of EHRs How to Implement EHRs Privacy & Security EHR Incentives & Certification Health Information Exchange (HIE) Case Studies & Data

HealthIT.gov > For Providers & Professionals > Privacy & Security > Your Mobile Device and Health Information Privacy and Security

## Privacy & Security

### Your Mobile Device and Health Information Privacy and Security

 Physicians, health care providers and other health care professionals are using smartphones, laptops and tablets in their work. The U.S. Department of Health and Human Services has gathered these tips and information to help you protect and secure health information patients entrust to you when using mobile devices.



**Read and Learn**

- How can you protect and secure health information when using a mobile device?
- You, your organization and your mobile device
- Five steps organizations can take to manage mobile devices used by health care providers and professionals
- Frequently Asked Questions

**Watch and Learn**

- Securing Your Mobile Device is Important!
- Dr. Anderson's Office Identifies a Risk
- A Stolen Mobile Device
- Can You Protect Patients' Health Information When Using a Public Wi-Fi Network?

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