Using a Mobile Device: How to Protect and Secure Health Information

No Matter Your Location

If you are a health care provider or professional using smartphones, laptops, or tablets in your work, KNOW THE RISKS. Mobile device benefits—portability, size, and convenience—present a challenge when it comes to protecting and securing health information. Theft and loss of devices is one of the biggest issues.

Whether you use a personally owned mobile device or one provided to you by a health care organization, system, or private practice, you should understand how to protect health information when using a mobile device—no matter where you are.

For more tips and information on protecting and securing health information, visit:

www.HealthIT.gov/mobiledevices

Mobile Devices:
Know the RISKS.
Take the STEPS.

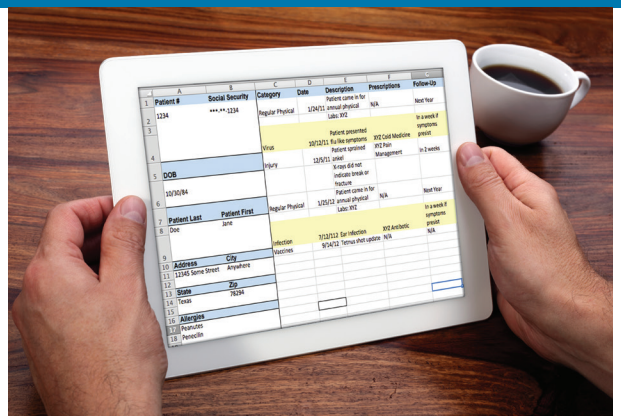
PROTECT and SECURE
Health Information.

HealthIT.gov

Tips for understanding how to protect health information when using a mobile device in a public space, home, office or health care facility.

HealthIT.gov

Using a mobile device in a public space, such as a coffee shop



- Don't let people around you see the numbers, letters, symbols, or pattern as you enter your password.
- Use a privacy screen shield or keep your back to a wall so others cannot see what is on your screen.
- Don't walk away from your mobile device in a public space—take it with you.
- Don't use an unsecured public Wi-Fi network to access, transmit, or receive health information. Use a virtual private network (VPN) or other secure connection to connect to an organization's private network or system with your mobile device.

Using a mobile device in a remote location, such as a home office

- Lock the screen of your mobile device and keep it in a secure location when you are not using it.
- Use a privacy screen shield or keep your back to a wall so others cannot see what is on your screen.
- Follow the instructions provided by the manufacturer to secure your home Wi-Fi network. Change the default administrator passwords and user names.
- Make sure your router's firewall is turned on. For extra protection, consider installing and running personal firewall software on each mobile device connected to the router.
- Use a VPN or other secure connection to connect to an organization's electronic health record EHR system or other private network.

Using your mobile device in a health care facility, hospital, or office

- Use a password or other user authentication to log on to the mobile device.
- Lock the screen of your mobile device when not in use.
- Set your mobile device preferences to automatically log you off or lock your screen after a short period of inactivity.
- Keep the mobile device with you.
- Protect the mobile device screen from others' view.

Mobile Devices: Know the RISKS. Take the STEPS.

PROTECT and SECURE Health Information.

HealthIT.gov