5

Tips for Securing your Mobile Device for Telehealth

The Health Insurance Portability and Accountability Act (HIPAA) requires that providers protect your information and not share it without your permission. Telehealth providers are required by law to secure medical information that can be shared electronically by encrypting messages and adding other safeguards into the software they use.

However, patients' devices on the receiving end of care often do not always have these safeguards while some medical devices have been shown to be vulnerable to hackers. It is therefore the responsibility of the patient to secure personal devices.

01 Use a PIN or Passcode to secure device

Securing your mobile device is important for ensuring that others do not have access to your confidential information and applications. To protect your iPad, iPhone, Android phone you need to set a passcode. It is a 4- to 6-digit PIN used to grant access to the device, like the code you use for an ATM bank card or a debit card.

Securing your Apple (iPhone and iPad) and Android devices

In addition to allowing you to secure your phone with a passcode, Newer Apple and Android devices also use biometrics called Touch ID and Face ID on Apple, and Face recognition, Irises, and Fingerprints on some Android devices. These tools use your Face, eyes, and fingerprints as unique identifiers to help secure your devices.

Face ID and Face recognition use your facial features in order to unlock your device. Touch ID, which is no longer being used on newer versions of iPhone and iPad, and Fingerprints on Android is a fingerprinting tool. Irises, sometimes used on Android devices, uses the unique features of your eye to do the same thing. If someone else tried to access your device that is protected using biometrics, the phone/tablet would not unlock.

Below are the steps for setting up your passcode, and Biometric features:

Setting Up your Passcode on iPhone or iPad (For iPhone X or later Versions)

1. Go to Settings then click on Face ID & Passcode. (On earlier iPhone models, go to Touch ID & Passcode. On devices without Touch ID, go to Settings > Passcode).
2. Tap Turn Passcode On.
3. Enter the six-digit passcode
4. Tap Turn Passcode On.
5. Enter your passcode again to confirm it and activate it.

01 Securing device continued

Setting Up your Face ID on iPhone or iPad (For iPhone X or later versions)

1. Go to Settings then tap on Face ID & Passcode. If asked, enter your passcode.
2. Tap Set Up Face ID.
3. Make sure that you're holding your device in portrait orientation, position your face in front of your device, and tap Get Started.
4. Position your face inside the frame and gently move your head to complete the circle. If you're unable to move your head, tap Accessibility Options.
5. When you finish the first Face ID scan, tap Continue.
6. Gently move your head to complete the circle for a second time.
7. Tap Done.

Setting Up Touch ID (For iPhones that preceded iPhone X)

Before you can set up Touch ID, you need to create a passcode for your device. Then follow these steps:

1. Make sure that the Touch ID sensor and your finger are clean and dry.
2. Tap Settings then tap Touch ID & Passcode, then enter your passcode.
3. Tap Add a Fingerprint and hold your device as you normally would when touching the Touch ID sensor.
4. Touch the Touch ID sensor with your finger—but do not press. Hold it there until you feel a quick vibration, or until you're asked to lift your finger.

Setting up your Android Device with Biometric functions:

1. Open your device's Settings
2. Tap Lock Screen
3. To pick a kind of screen lock, tap Screen lock type.
4. Tap the screen lock option you would like to use. There may be many options including:

- **Pattern:** Draw a simple pattern with your finger.
- **PIN:** Enter 4 or more numbers. Longer PINs tend to be more secure.
- **Password:** Enter 4 or more letters or numbers. A strong password is the most secure screen lock option

5. You'll also be able to select the Biometric options you'd like to enable.

- Turn the option on and your device will walk you through the process of setting each of these options up.
- You can also access these options by going to Settings
- Tapping Biometrics and security
- Tapping Face recognition, Irises, or Fingerprints

Securing your Android Device

1. Open your phone's Settings
2. Tap Security
3. To pick a kind of screen lock, tap Screen lock.
4. Tap the screen lock option you would like to use. There are 3 options for screen locks:

- **Pattern:** Draw a simple pattern with your finger.
- **PIN:** Enter 4 or more numbers. Longer PINs tend to be more secure.
- **Password:** Enter 4 or more letters or numbers. A strong password is the most secure screen lock option

02 Keep your Software Updates Current

Whenever an update is released for your device, download, and install it right away. These updates often include security fixes, vulnerability patches, and other necessary maintenance.

03 Turn off Wi-Fi when not in use

Most devices have a great feature that allows your phone to automatically connect to Wi-Fi hotspots. The issue with your phone being able to connect automatically to hotspots is that it may connect to a face wireless hotspot established for nefarious reasons without you knowing. To prevent your device from automatically joining networks:

To Stop iPhone or iPad from Automatically Joining Networks

a. Tap on Settings
b. Tap on Wi-Fi
c. Turn Ask to Join Network on

To Stop Android Phone from Automatically Joining Networks

a. Tap on Settings
b. Tap on Network & Internet then tap Wi-Fi preference
c. Turn off the Connect to open networks toggle switch to disable it.

04 Turn off Bluetooth when not in use

You need to keep your Bluetooth off whenever you are not using it in order to protect your device.

To Turn Off Bluetooth for iPhone and iPad

a. Tap on Settings
b. Tap on Bluetooth or the Bluetooth symbol in your settings and tap it.
c. Turn off Bluetooth by toggling switch to disable it

05 Download apps from reputable app stores

Use only the official app stores - Apple App Store if you have an iPhone or iPad, and Google Play store if you have an Android device. It is all too common for malware developers to create fake malicious apps and put them up on third-party sites, hoping someone will download them. Official app stores have a more stringent vetting process.