Mobile Devices
Protecting "EPHI"
Electronic Protected Health Information

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.

Encryption of your Mobile Device: iOS: Understanding data protection

Learn how to enable and verify data protection.

Data protection is available for devices that offer hardware encryption, including iPhone 3GS and later, all iPad models, and iPod touch (3rd generation and later). Data protection enhances the built-in hardware encryption by protecting the hardware encryption keys with your passcode. This provides an additional layer of protection for your email messages attachments, and third-party applications.

A. Enable data protection by configuring a passcode for your device:

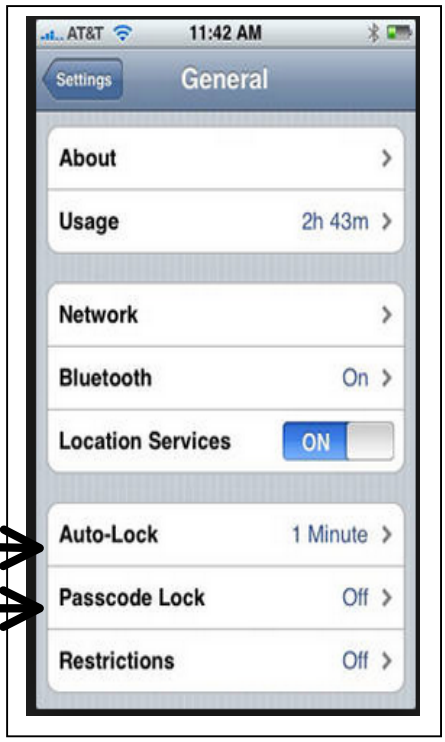
1. Tap **Settings**

   > General

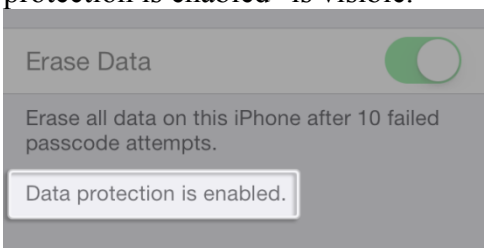
   > Passcode.

Since you are on this menu it is a good time to set the "Auto-Lock" on your phone. This sets a time- like 1 minute- that if you set your phone down without exiting by turning off an application then the phone will "Auto-Lock" and in order to use the phone you will need to reenter your password. This prevents an inadvertent EPHI breach by someone picking up your phone and having access to EPHI.

2. Follow the prompts to create a passcode.



3. After the passcode is set, scroll down to the bottom of the screen and verify that "Data protection is enabled" is visible.



2. Use a password or other user authentication.

Passcode tips: Use these passcode settings to maximize passcode security:

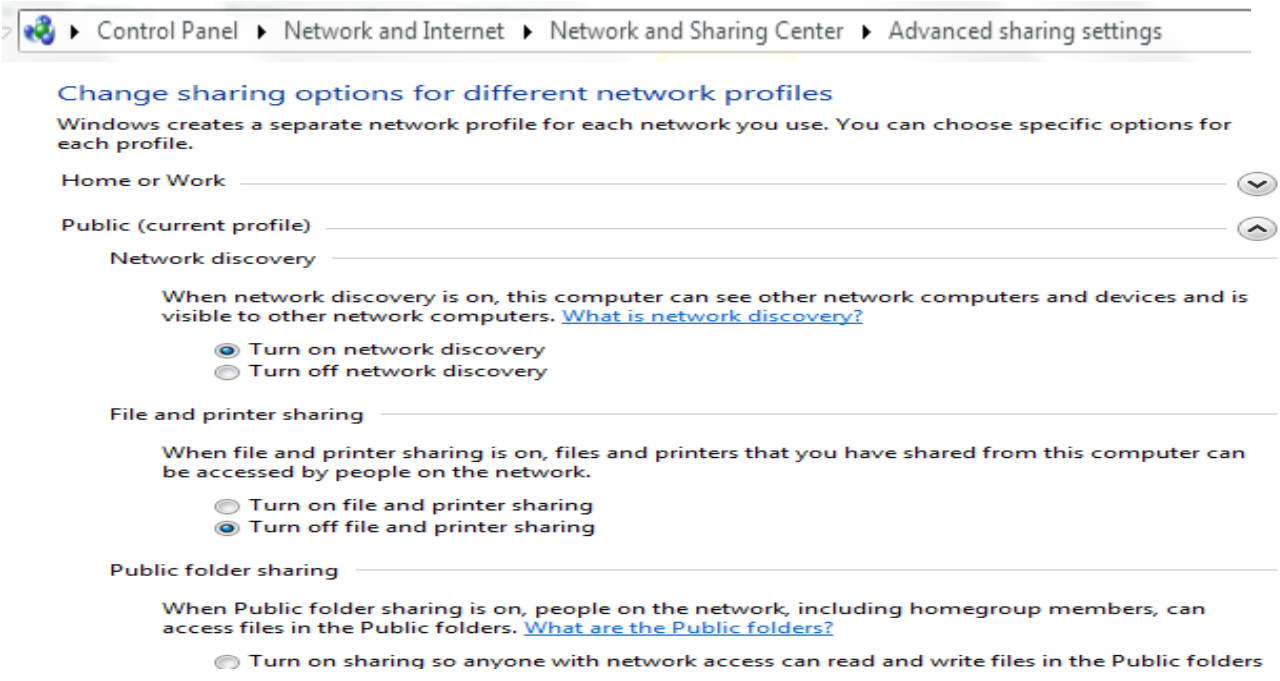
- Set Require Passcode to Immediately.
- Disable Simple Passcode to use longer, alphanumeric passcodes (if your device has this option)
- Enable Erase Data to automatically erase the device after ten failed passcode attempts.

In order to enable the **"Erase Data"** function on the iPhone you must first turn on the **"Find My iPhone"** feature. This feature allows you to locate your phone on a map if it is lost or stolen. In addition it allows you to remotely "lock" your phone and to erase all of the data on your phone. That way you can protect any EPHI that is on your phone. This means that you want to also activate the **iCloud** feature on your phone so all of the data on your phone is automatically stored periodically and you can access the data from your computer after it is erased from your phone. It also sets up your phone to erase all data after 10 failed passcode attempts.

3. Install and activate wiping and/or remote disabling to erase the data on your mobile device if it is lost or stolen.

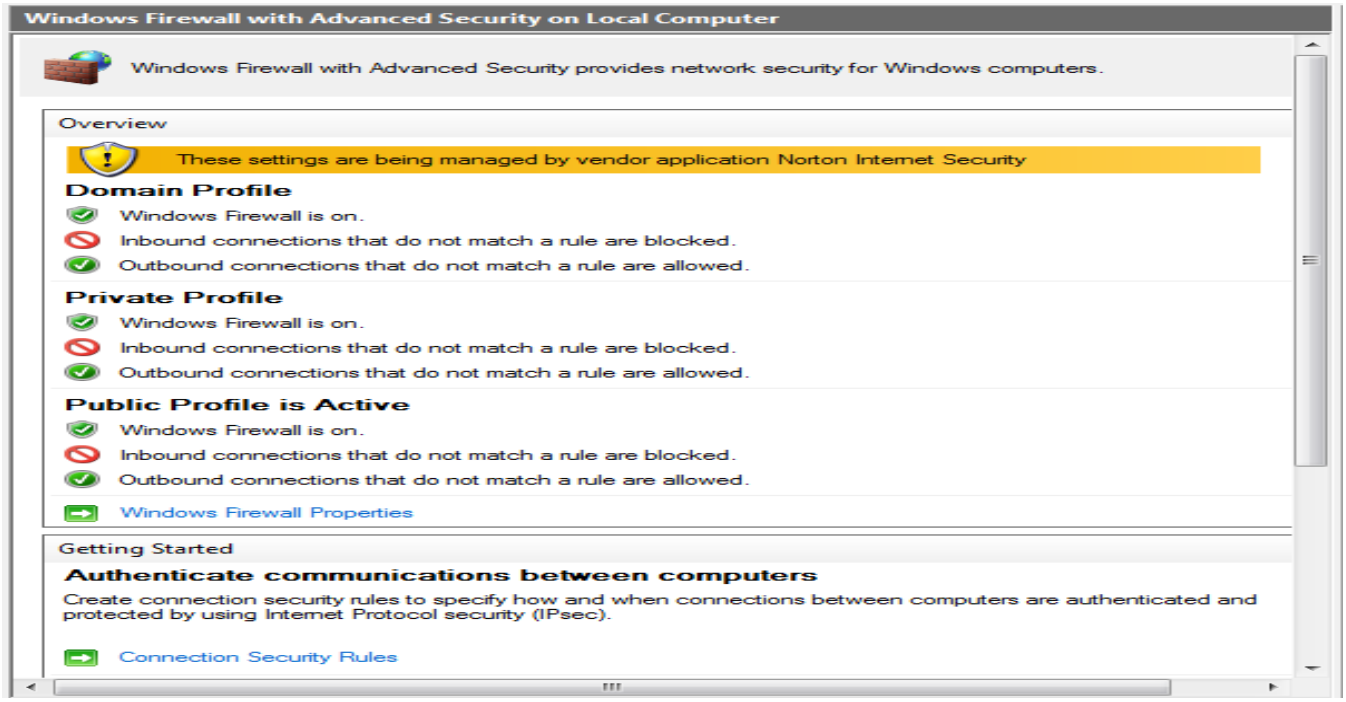
4. Disable and do not install or use file sharing applications.

This applies more to your laptop, iPad or other notepad type of mobile device than your phone. on your device look for the below type of information on your control panel and make sure to "Turn off file and printer sharing" and in the public folder sharing also turn off sharing. Make sure you scroll to the end and click "save" settings.



5. Install and enable a firewall to block unauthorized access.

This applies more to your laptop, iPad or other notepad type of mobile device than your phone. On your device look for the below type of information and make sure that you have installed a firewall.



6. Install and enable security software to protect against malicious applications, viruses, spyware.

There are many software security products- Norton, Ad Aware, McAfee and others that you can purchase and install on your device.

7. Keep your security software up to date.

Hackers are constantly creating new viruses and malware that can harm your computer and risk an EPHI breach so it just makes sense to update your software periodically.

8. Research mobile applications (apps) before downloading.

One way to check to see if any application that you have on your iPhone is trying to access information on your phone is to click on Settings > Privacy > and then check each category: Contacts, Calendars, Photos and others.

9. Maintain physical control of your mobile device. Know where it is at all times to limit the risk of unauthorized use. It only takes a minute of inattention.

Another inadvertent disclosure can occur when you receive a text message and have not disabled the Short Message Service (SMS) on your phone. SMS displays the text message on your phone without you entering a passcode. If a client sent you a text message and your phone was sitting in plain view in public then an inadvertent EPHI breach could occur.

Turn off the SMS or MMS in order for the text message to not display without a passcode being entered.

10. Use adequate security to send or receive health information over public Wi-Fi networks.

To protect EPHI in this situation requires your device to have set up a Virtual Private Network (VPN). VPN actually creates encryption of your communication on your device. VPN may best be set up by the practice on their server. Below are some instructions to set up VPN but you may also need some IT consultation.

Step by Step: Connecting to a VPN (Outgoing)

Step 1 Click the Start button. In the search bar, type VPN and then select Set up a virtual private network (VPN) connection.
Step 2 Enter the IP address or domain name of the server to which you want to connect. If you're connecting to a work network, your IT administrator can provide the best address.
Step 3 If you want to set up the connection, but not connect, select Don't connect now; otherwise, leave it blank and click Next.
Step 4 On this next screen, you can either put in your username and password, or leave it blank. You'll be prompted for it again on the actual connection. Click Connect.
Step 5 To connect, click on the Windows network logo on the lower-right part of your screen; then select Connect under VPN Connection.
Step 6 In the Connect VPN Connection box, enter the appropriate domain and your log-in credentials; then click Connect.
Step 7 If you can't connect, the problem could be due to the server configuration. (There are different types of VPN.) Check with your network administrator to see what kind is in use--such as PPTP--then, on the Connect VPN Connection screen, select Properties.

Step 8 Navigate to the Security tab and select the specific Type of VPN from the drop-down list. You may also have to unselect Include Windows logon domain under the Options tab. Then click OK and Connect.

11. Delete all stored health information on your mobile device before discarding it.

The concern with this is to be really sure that all the EPHI has been deleted permanently and cannot be retrieved in any way. If you are using your own mobile device and it has EPHI on it (For example a client's phone number or email address) then the health care organization has a responsibility to collect information from you about your device in order to manage a HITEC breach of EPHI. That means the organization needs to collect identifying information about your device.