Securing and Encrypting iOS
Department of Medicine IT Services
Updated 1/28/2015

iOS devices have built-in hardware encryption. Additional 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 and attachments. You can also enable ‘Find my iPhone’ to do secure erases remotely when your phone is lost.

Instructions:
Before starting consider backing up the data on your device and make sure that the device is fully charged and plugged in because if the device runs out of power during this process it is possible your data will be lost. Most carriers provide a backup application as part of their standard service if the device has cellular service.

Enable data protection by configuring a passcode for your device:
1. Tap Settings > General > Passcode Lock.
2. Follow the prompts to create a passcode.
   Use these passcode settings to maximize passcode security:
   a) Set Require Passcode to Immediately or any timeframe less than 10 minutes.
   b) Disable Simple Passcode to allow the use of longer, alphanumeric, passcodes. See below for tips on creating strong passwords.
   c) Enable Erase Data to automatically erase the device after ten failed passcode attempts
   d) See below for extra tips on creating strong passwords.
3. After the passcode is set, scroll down to the bottom of the screen and verify that the text “Data protection is enabled” is visible.
**Tips for creating a strong Password/Passcode:**
A strong password is an important protection to help you have safer online transactions and a more secure device. Here are steps you can take to create a strong password/passcodes. Some or all might help protect your online transactions:

- **Length.** Make your passwords long with eight or more characters.
- **Complexity.** Include letters, punctuation, symbols, and numbers. Use the entire keyboard, not just the letters and characters you use or see most often. The greater the variety of characters in your password, the better. However, password hacking software automatically checks for common letter-to-symbol conversions, such as changing "and" to "&" or "to" to "2."
- **Variation.** To keep strong passwords effective, change them often, about every three months is considered optimal.
- **Variety.** Don't use the same password for everything. Cybercriminals steal passwords on websites that have very little security, and then they use that same password and user name in more secure environments.

Here is a link to allow you to test your password/passcode for strength; [https://www.microsoft.com/security/pc-security/password-checker.aspx](https://www.microsoft.com/security/pc-security/password-checker.aspx)

**Turning on Find my iPhone**
This enables the Find My iPhone feature of the iCloud service. Please note that there is also an App called Find My iPhone, using that App from another iPhone or iPad will only allow you to track lost devices.

1. Settings> iCloud.
2. Change ‘Find My iPhone” to on.
3. Now if your iPhone is lost you can go to [https://www.icloud.com/](https://www.icloud.com/) and log in with your Apple account. From there you can locate your phone and have the option of an alarm, locking it, or erasing the phone and all its contents.