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

Instructions for Android 3.0 and above
NOTE: Earlier versions do not support encryption but do allow for Strong Password protections.

Before starting consider backing up the data on your device and make sure that the device is fully charged and plugged in. 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.

This process may very slightly for each device and carrier.
Under Settings, and Security configure the following options.

- Screen lock: select lock type as “Password” and enter a strong 8 character password. See below for tips on creating strong passwords.
- Automatically lock: Immediately or any timeframe less than 10 minutes.
- Power button instantly locks: Check This Box
- Data encryption: Storage, Check This Box
- Device Data: Check This Box (This will insure that all email, calendar and contacts are encrypted)
- Key protection: Check This Box
- Unknown sources: Uncheck This Box
- Tap ‘Apply’

Phone will reboot and the encryption process will start – this will take several minutes depending on how much data is stored on the phone and SIM card.

- Phone will reboot again after the encryption is complete
**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)