Do's and Don'ts for Mobile Computing for Medical Students

Don'ts
1. Don't store Protected Health Information (PHI) at DropBox, Google Docs or other Cloud vendors.
2. Don't store patient information or identified research subject information on unencrypted devices such as smart phone, thumb drives, laptops, iPad/tablet, etc.
3. Don't forward your Mednet email account to any other email accounts.
4. Don't send any unencrypted PHI to non-Mednet addresses.
5. Don't use anything but your Mednet email account for emailing PHI or research information to other Mednet email users.
6. Don't share your passwords with anyone.

Do's
1. Do enable the security pass code for your smart phone if you have one.
2. Do use encryption for smart phones and other devices.
3. Do enable the password-protected screen saver for your laptop, tablet, and smart phone.
4. Do logout of applications with patient information when you leave a workstation.
5. Do use strong passwords:
   a. Don't use the words "password" or "Password"; dictionary words or names in any language (monkey, Michael); sequences of numbers (123456, 123123, 121212); or sequences of keyboard characters (qwerty, asdfgh).
   b. Use passwords that are at least 8 characters in length with numbers and mixed upper and lower case. Use special characters ($%&@#, etc.) when possible.
      i. Note, the MITS RACF password used for cView and other applications has an 8-character maximum and does not allow special characters. If your preferred password is too long, just use the first 8 characters.
6. Do report lost/stolen devices with PHI ASAP to the Office of Compliance Services by phone at (310) 794-8638 or email PrivacyInfoSec@mednet.ucla.edu.