

Turn Awareness Into Action...

Keep Tabs On Your Mobile Devices & Protect The Data Stored On Them

Mobile devices include items such as **Laptop Computers, Personal Digital Assistants (PDAs), Smart Phones or Handheld Dictation Devices**. They help us perform our jobs while in and out of the office, but they also create privacy and security risks if they are not properly secured.

Nobody likes losing a mobile device or having one stolen, but the amount of pain caused to you and UCMC can be minimized if we use precaution. It is everyone's responsibility to protect mobile devices and the data/information (e.g. medical, financial, personnel, research) being stored on them.

These tips will help increase our success with mobile device security:

1. **Do not store data/information on the mobile devices.** However, if you must save data/information directly/locally on these devices, always password protect them and encrypt the files so unauthorized individuals can not access the data if the devices are stolen or lost.
2. **Keep the devices on your possession at all times. Do not lose sight of them for a second... *they can disappear in a flash.***
3. When leaving laptop computers unattended in a shared space, either physically secure them with a cable lock or keep them in a locked drawer or cabinet.

If you lose a device or have one stolen, please immediately contact your department management, the Chicago Biomedicine Information Services (CBIS) Help Desk at (773) 702-3456, or the HIPAA Program Office at (773) 834-9716 for assistance.

Do The "Smart" Thing...Protect Mobile Devices.