Mobile Device Management (MDM)

- What is Mobile Device Management?
  - Mobile device management is the process of securing, managing and supporting mobile devices such as SmartPhones and tablets through the use of software. This is an important tool allowing UAB Health System employees to use their personal devices for business use.

- What software does UAB Health System use as their mobile device management tool?
  - MaaS360

- What devices are supported?
  - At present time we support iOS and Android devices. We are constantly reviewing other device types. Please check back often as supported device types may change.

- What security features does MaaS360 enable and/or offer?
  - Five (5) digit passcode on the device
  - Auto-configuration of email, contacts and calendar synchronized with the organizational email system
  - Full device encryption*
  - Access to UAB Health System mobile Wi-Fi
  - Ability to remotely “wipe” the device if lost or stolen
  - Ability to selectively “wipe” corporate data when employee leaves the organization without affecting any personal data
  - Access to UAB Health System supported mobile applications

- How do I enroll my device?
  - Visit the mobile device request page [here](#) and complete the enrollment request form.

- Can I register more than one device?
  - Yes, you can register as many devices as your department is willing to pay for.

- I am currently an existing MaaS360 subscriber and I recently received a new phone, what do I need to do?
  - Please fill out the on-line form located [here](#) and we can assist with your transition.
MDM Privacy Concerns

- Does the use of MaaS360 allow the organization to view/read my text messages or email messages?
  - No, this type of data continues to stay private and is not accessible to the organization.

- Does the use of MaaS360 allow real time tracking of my location?
  - No, only a “snapshot” of the location is available.

- Does the use of MaaS360 allow access to my personal passcodes and/or passwords on the device?
  - No, MaaS360 does not have access to this data. All information, including your iTunes password, is protected.

- Is device usage, such as web sites visited and software utilization, tracked by MaaS360?
  - No

- Can calls made on the mobile device be recorded or listened to?
  - No

- Does MaaS360 allow access to my call log?
  - No

- When I leave, is all the data on my personal device “wiped” and lost forever?
  - No, the advantage of MaaS360 is only the corporate data and applications are wiped from your device. Any personal information remains.

- I have lost my phone. It was either stolen or misplaced. Can you wipe all the data, including personal data?
  - Yes, not only can the corporate data be removed from the device remotely, upon the request of the owner, the device can be erased and setback to factory settings.