

Policies and Procedures for Portable Devices

The UTHSCH HIPAA policy states the following:

"PHI (protected health information) should be stored on the secure servers in Zone 100"

Zone 100 is a protected area in our network where the Medical School's File server (NAS) resides. All MS employees should have a drive mapped to the NAS on their PCs, and they should be saving all of their data (especially PHI data) to that drive, and not to their local PCs or laptops or flash drives. (The NAS is also backed up every 3 hours, which would preserve such data from being lost.)

"Portable computing devices (laptops, PDAs) should be kept secure by remaining in the department or by password protection; All portable devices should be encrypted."

If transient PHI data needs to be stored on portable computing devices like laptops, PDAs and flash drives, then the data needs to be also encrypted, and the device needs to be password protected.

We recommend that no PHI data gets saved to laptops and PDAs. Flash (thumb) drives should be used instead. **As a new MSIT policy, we are recommending that only encryptable flash drives be purchased.** (We recommend the Data Traveler Elite flash drives from Kingston, which are encryptable). This way, even if the flash drive is lost, no one can have access to the data (keep in mind, though, that the data would be lost if it is not backed up on a regular basis).

Also, please remember that any email that contains identifiable patient information needs to be digitally encrypted before it is sent. Digital IDs are necessary in order to encrypt emails.

Finally, UTHSCH policy regarding laptop physical security, effective as of 3/31/2006, states that all unattended UT laptops on the UTHSCH campus should be physically secured by a locking device. To that effect, we have changed all laptop models on our leasing page to include a locking device.

LAST NAME _____

FIRST NAME _____

DEPARTMENT _____

ROOM # _____

SIGNATURE _____

DATE _____