Impact Security Information

Concerning Information Security:

- Do not use a portable device (thumb drive, laptop, PDA, cell phone) for storing ePHI. If absolutely necessary, check with your IT representatives for security safeguards.
- Do not email Protected Health Information unless you are within a closed network. If you have a question as to what constitutes a “closed network”, please ask.
- Do not FORWARD your UAB emails to outside email systems, i.e. AOL, Hotmail, Yahoo, Gmail.
- Do not use web-based personal file and backup media, i.e. Google docs, spreadsheets, personal backup sites, etc.
- Store sensitive data on a secure server, not on a workstation or laptop hard drive.

Should You Misplace or Forget Your IMPACT Code:

- Call the HSIS Help Desk (934-8888) to request your IMPACT code.
- Codes cannot be given out over the phone or mailed.
- Codes can be picked up from the HSIS receptionist’s desk (Room 401-General Services Building).
- The HSIS Receptionist office is open Mon-Fri, 8:00 a.m. – 4:30 p.m. (205) 934-6470
- Please provide a valid picture ID to obtain your code.
- Please contact the HSIS Help Desk (934-8888), after normal business hours.

By signing this form, you are acknowledging you have read and understand the above policy and the Use of Portable Devices within UABHS HIPAA Covered Entities

________________________________________
Your Signature

________________________________________
Please Print Legibly
Use of Portable Devices within UABHS HIPAA Covered Entities

What are Portable Devices?
Portable devices used for communicating and storing information are cause for both privacy and security concerns within the UABHS HIPAA Covered Entities. These portable devices include, but are not limited to the following:

- Laptop computers
- Notebook computers
- Cell phones, Smart phones, iPhones
- Android devices
- Personal digital assistants
- iPads
- Pagers
- CDs and DVDs
- Tapes
- USB flash or thumb drives

How to Appropriately Use Portable Devices if used to receive/send PHI:

- Each device MUST have the following:
  - Password protection and/or encryption using HSIS-approved encryption methods
  - UABHS software or security controls on the device, including a remote wipe capability
- Always use your UABHS email account and communicate with colleagues using only their UABHS email account.
- The device is not used as a storage unit for PHI. Electronic PHI should be stored only in secure UAB/UABHS server environments.

Inappropriate Uses of Portable Devices:

- Communicating with patients using email or text messaging
- Photographing or recording patients or fellow employees without obtaining appropriate written consent
- Documenting patient care or diagnosis
- Transmitting medical record information
- Capturing medical images
- Texting (or SMS messaging) information about a patient
- Forwarding messages containing PHI to off-campus email systems, i.e. gmail, Charter, hotmail, Yahoo
- Using cloud technologies, such as Dropbox and Google Docs, when transferring PHI
- Installing your own hubs, switches, routers, or wireless access points

Penalties for Noncompliance:

- Disciplinary action by the institution (up to and including termination of employment and/or medical staff privileges) and/or the licensing board
- Monetary fines applied to both the individual and the institution

Personally Owned Portable Devices:

You can not use your personally owned portable device for work-related purposes unless that use has been approved by senior management (dean, chair, or division or program director or their specific designate who is authorized to make executive decisions to accept risks for the administrative unit in the area of information security). If senior management approves the use of your personal device it must comply with the same security controls as provided by UABHS.