PHI is any information that links an individual with their physical or mental health condition such as:

- Name of individual or relative
- Any address smaller than state
- Telephone numbers
- Electronic mail address
- Social security numbers
- Medical record numbers
- Account numbers
- Health plan beneficiary number
- Dates such as birth, admission, or discharge
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

PHI Safeguards:

✓ Do not access PHI without authorization
✓ Access PHI using only authorized applications
✓ Report exposed data immediately to the UF Privacy Office
✓ Unless you have special permission, do not transmit PHI in email
✓ Never transmit PHI in instant messages
✓ Unless you have special permission, do not store PHI on:
  o A desktop computer
    ▪ Position screen so that it’s not viewable to others
  o A computer that is not professionally managed, such as your home computer
    ▪ Maintain current software updates
    ▪ Maintain current anti-virus updates
    ▪ Use a firewall
  o A laptop, PDA or smart phone or other portable devices
    ▪ Do not remove from campus without authorization
    ▪ Don’t synchronize with home computer.
    ▪ Protect device as you would a wallet or purse.
  o Removable media such as CDs, DVDs and USB thumb drives
    ▪ Protect media as you would a wallet or purse.

✓ Regardless of the use, practice the following safeguards
  o Obtain approval for all devices, media and software used with PHI
  o Use strong passwords to access PHI
  o Password-protected screensaver with a short time-out
  o Minimize the amount of data stored
  o Minimize the length of time data is stored
  o Encrypt stored data, preferably using whole-disk encryption
  o Only use applications that encrypt transmitted data
  o Encrypt backups and minimize backup retention time
  o Render all media unreadable prior to reuse or disposal