A Focus on HIPAA and Communications

Mandatory Safeguards
- There are two mandatory computer applications for all computers that access patient information. Check your computer today to make sure it has:
  1) Encryption to prevent unauthorized reading or changing of electronic data;
  2) Software to detect, contain or remove intruders-viruses, Trojans, worms, and other malicious attacks.

Security: PHI in Email
- Patient to Provider: If a patient wants to communicate by e-mail, provide an Alert For Email Correspondence - which includes a list of all the potentials for disclosure of their PHI.
- Then ask the patient to sign the Authorization for Email Correspondence. Patients and caregivers should both keep a copy of the authorization. (The caregiver should store the copy as an attachment in axiUm.)
- Patients can email you and include their PHI if they choose to but you should never include PHI in emails to patients without the patient’s written authorization.
- This applies to communications between research participants and researchers as well.

Security: PHI in Email among workforce members
Limited PHI can be included in emails between workforce members but only for work-related purposes, only within the ufl.edu system, and only for these limited purposes:
- Requesting consultations
- Making referrals (axiUm messenger is preferred)
- Prescription refills (axiUm messenger is preferred)
- Billing inquiries (when possible, axiUm messenger is preferred)
- Among researchers, staff and authorized third parties, PHI used for research can be attached as an encrypted file to emails.
- Need more information? You can access the UF policy here.

Security: Portable Data Devices
- Devices include, but are not limited to: pods, pads, “smart” and blackberry devices, PDAs, dictation devices, laptop or notebook computers, cell phones, digital cameras, video recorders, flash drives, memory cards, and any similar devices.
- Devices are subject to all applicable UF and HSC information security policies and relevant state and federal laws.
- Unauthorized use or disclosure of PHI via any electronic device will be cause for disciplinary action.
- Loss or theft of portable data devices on which restricted information is stored must be reported to the Privacy Office, the IT Security Office, and the University of Florida Police Department.

Security: Personal Cameras
- Unless specifically authorized by the department chair, use of personal cameras or video devices is prohibited for work-related purposes in patient care areas, unless needed for emergency treatment of a patient.
- Personal camera devices include, but are not limited to: digital cameras, camera phones, video recorders, blackberry devices, web cameras, and similar devices.
- Images of our patients taken as part of their care are the property of the UF College of Dentistry and must be stored in the patient’s record accordingly.