Office of Institutional Integrity
East Carolina University
HIPAA Privacy and Security Best Practices

- Disclosure of Protected Health Information (PHI)
  - Make every effort to speak to a patient directly. Verify who you are talking to.
  - Never leave specific health information for patients on voicemail.
  - Avoid discussions about patients in hallways, elevators, or other public places where others may overhear your conversation.

- Appropriate Safeguards of PHI
  - Never share passwords.
  - Never leave patient information unattended.
  - Never access any medical record or other PHI unless you have a legitimate business or patient care purpose.

- Electronic Transmission of PHI
  - Limit e-mail transmissions of PHI when necessary.
  - Take proper precautions when sending PHI electronically:
    - Encrypt emails containing PHI when emailing outside of the institution (other than ecu.edu).
    - Refer to ECU’s ITCS website for instructions on encrypting email.

- Photography/Social Media
  - Do not post sensitive patients’ or other care providers’ information online.
  - Maintain appropriate boundaries of the patient-clinician relationship.
  - Report unprofessional postings to your supervisor.

- Portable Devices
  - Portable devices storing PHI should be encrypted, must have a passcode, and always be physically and technically secure.
  - Any loss, theft, or unauthorized use must be reported immediately to ITCS and/or OII.

- Concerns
  - When there is a privacy complaint and/or concern, report to your supervisor, or contact the HIPAA Privacy Office.
  - Complaints and/or concerns are taken very seriously. They are investigated in detail in order to comply with regulatory requirements.

- Violations/Sanctions
  - ECU is required to have and apply internal sanctions against employees who fail to comply with policies and procedures.

- Where to get more information
  - Website: https://hipaa.ecu.edu
  - Email: HEALTHCAREPRIVACY@ecu.edu
  - Phone: Office 252-744-5200 Hotline 1-866-515-4587