SECTION 5: SECURITY OF PHI AND OTHER RESTRICTED INFORMATION

5.1. Mobile Computing and Storage Devices

POLICY

1. Responsibility: All University of Florida (UF) faculty, staff, students, and volunteers are responsible for maintaining the confidentiality of all health information (not just protected health information (PHI)), personal identification information (PII), and other restricted data, stored on or transmitted through mobile devices, from improper use or disclosure.
   a. Persons violating this policy may be subject to disciplinary action by UF, up to and including, termination of their relationship with UF and/or denial of future access to a UF information system.
   b. Persons violating this policy may also be held personally liable for resulting damages and civil or criminal charges. When appropriate, law enforcement, the Department of Health & Human Services (HHS), and/or applicable licensing boards will be notified of incidents.

2. All mobile computing and storage devices that access, store, process, or transmit PHI or other restricted information must be compliant with UF Information Security Policies and Standards, and the provisions of relevant state and federal laws. These requirements apply to all devices used to restricted data. If your device cannot comply, then you need to be certain that you do not use it to access or store restricted data.

3. Minimum Device Requirements:
   a. All devices used to store PHI, PII, or other restricted data in any format must be encrypted using approved software that specifically offers HIPAA-compliant access to current electronic health record systems as well as HIPAA-compliant text, data, and image-sharing.
   b. All devices used to communicate PHI, PII, or other restricted data in any format must utilize approved communication channels to transmit the information.

4. Loss or theft of mobile devices on which PHI or other restricted data is stored must be reported to the Privacy Office as well as to the University Police Department or other local law enforcement agency where the theft or loss occurred, whether the device is the property of UF or not.

5. Use of Mobile Devices and Cameras:
   a. Users are responsible for any activity originating from personal devices.
   b. Mobile devices should not be used for image or video capture inside areas already wired to capture videos (i.e., operating rooms, certain procedure rooms).

6. Users sharing and receiving photos of PHI must have a professional need to know the information used or shared for treatment purposes.

7. Communications and/or images used for healthcare decision-making or to provision clinical treatment must become part of the patient’s health record and are subject to record creation and retention requirements.

8. Examples of acceptable and unacceptable uses of Mobile Devices
   a. Acceptable Uses:
i. A resident physician photographs a patient’s wound and sends the image to the patient’s attending physician for consultation.

ii. A nurse “texts” stat lab results to the ordering physician.

iii. A clinician photographs the placement of a healthcare device, excluding any patient identifiers, and sends the image to the device manufacturer for advice.

b. Unacceptable Uses:

i. Patient images recorded out of curiosity.

ii. Taking a picture with a patient, at the patient’s request, in a patient care area, and then forwarding the picture to the patient and/or posting the picture on a Facebook page.

iii. PHI shared outside the ufl.edu domain under the assumption of “general healthcare education.”

iv. Auto-forwarding e-mail to any e-mail system outside the ufl.edu domain, such as G-mail, Yahoo, Outlook, or similar external e-mail systems.

9. User Permissions for Communicating PHI

a. Clinicians and Employees: Use shall be consistent with the approved purposes of the direct provision of patient care and/or during emergencies or disasters.

b. Research: Images and videos recorded for research activities require Privacy Office approval during the IRB review/approval process.

c. Students: Use shall be consistent with supervised participation in a clinically affiliated educational program, either through a UF college, or another affiliated college (through an educational agreement) during on-site practicums.

d. User Protocols and Etiquette: Disruptive use of IT resources is not permitted. Occasional personal use of IT resources by employees is permitted when it does not consume a significant amount of those resources, is otherwise in compliance with this policy, and meets with the approval of the supervisor.

DEFINITIONS

1. **Encryption**: the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key (e.g., the translation of data into a secret code).

2. **Mobile Computing Devices**: Small devices intended primarily for the access to or processing of data, which can be easily carried by a single person and provide persistent storage. New products with these characteristics appear frequently. Current examples include laptops, notebooks, tablets, smartphones, and PDAs.

PROCEDURES

1. Training: Complete the Mobile Device Management module in myTraining.

2. Protect Contents: Use all available measures to protect data stored on or transmitted through mobile computing devices:

   a. Know your device: Equipment that only transmits data without storing needs a different level of protection than equipment that also stores data, which will require more security.

   b. Use Proper Authentication Practices and Password Protection: Use strong passwords; do not share passwords.
i. Configure the Mobile Device to require a strong password, consistent with or exceeding UF password requirements.

ii. Configure the device with an inactivity timeout of not more than 10 minutes, which requires re-authentication before use.

3. Encryption of data: Mobile computing or storage devices that store restricted data must be fully encrypted, regardless of ownership, including personally owned devices configured to access UF email. Exceptions to this encryption requirement are limited to those outlined in UF Information Security Mobile Computing and Storage Devices Standard.

4. Single User / Single Use: Limit use of the device to one person and one purpose, either work or personal, but not both. Do not allow friends, family members or children to use or play with a device designated for work purposes.

5. Limit Data: Store only the “minimum necessary” data on portable devices. Destroy stored data immediately when information is no longer needed; purge, overwrite, or degauss equipment when ownership changes.

6. Label Devices: Mobile computing devices must have durable physical or electronic label with contact information sufficient to facilitate return in the event that a lost device is found.

7. Secure Devices: Employ other reasonable safeguards as necessary to prevent theft of the device and/or unauthorized viewing of PHI.
   a. Use tracking and recovery software to facilitate return, or equip devices with the ability to remotely wipe stored data if the device is lost or stolen.
   b. When not in use, turn the device off and store it in a locked or otherwise secure area.
   c. Mobile computing and storage devices must be used and stored in a manner that deters theft. Do not leave data devices unattended in vehicles, hotel rooms or on aircraft!

8. Ensure Proper Disposal of Devices: Contact the UF or AHC IT Security Department or place a Computer-Related IT Service Request to prepare mobile computing and storage devices for disposal in compliance with Information Security Electronic Media Control, Disposal and Reuse policies.

9. Report Loss or Theft: Notify your immediate supervisor and the following units immediately concerning the loss or theft of a personal data device used for UF business that included PHI or other restricted data, whether it belonged to UF or not:
   a. UF Privacy Office
   b. U IT Security Office
   c. UF Police Department, or other local law enforcement agency, if applicable.

REFERENCES
2. UF Information Security Mobile Computing and Storage Devices Standard and Policy

EXHIBITS
1. UF ISO Mobile Computing and Storage Devices Policy at, [https://it.ufl.edu/policies/information-security/](https://it.ufl.edu/policies/information-security/)
2. UF IT training Mobile Device Help at, [https://training.it.ufl.edu/training/items/mobile-device-help.html](https://training.it.ufl.edu/training/items/mobile-device-help.html)