SECTION 5: SECURITY OF PHI

5.2. Personal Portable Data Devices / Mobile Devices

A. POLICY

REV. 06/01/2015

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 personal portable data devices, also known as 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. **Devices** include, but are not limited to: wireless phones of all brands, wearable technology and personal data assistants of all types and brands, laptop/notebook computers, dictation equipment, cameras and video recorders of all types and brands, and any portable memory devices.
3. **Security** of PHI and other restricted data accessed, used, stored in, or transmitted through portable electronic devices is subject to the policies of the UF Information Security programs, UF Health Information Security programs, and the provisions of relevant state and federal laws. Disclosure of unsecured PHI or patient data, including images, via electronic devices is strictly prohibited. Unauthorized use or disclosure of PHI or other restricted data via any electronic device will be cause for disciplinary action.
   a. All devices used to communicate 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 and encrypted communication channels to transmit the information.
4. **Loss or theft** of portable data 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, whether the device is the property of UF or not.
5. **Use of Personal Devices and Cameras:** Use by workforce members of personal portable data devices that create, store, or transmit text, data, or still or moving images is generally prohibited for work-related purposes in patient care areas, except for the direct provision of patient care and/or during emergencies or disasters. Users are responsible for any activity originating from personal devices. Personal devices should not be used for image or video capture inside areas already wired to capture videos (i.e., operating rooms, certain procedure rooms).
   a. Users sharing and receiving photos of PHI must have a professional need to know the information used or shared for treatment purposes.

SECTION 5: SECURITY OF PHI

5.2. Personal Portable Data Devices / Mobile Devices (continued)

b. 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.

c. Examples of acceptable and unacceptable uses of Personal Devices

1) Acceptable Uses:

a) A resident physician photographs a patient's wound and sends the image to the patient's attending physician for consultation.

b) A nurse "texts" stat lab results to the ordering physician.

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

2) Unacceptable Uses:

a) Patient images recorded out of curiosity

b) 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.

c) PHI shared outside the ufl.edu domain under the assumption of "general healthcare education."

d) 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.

6. **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.

7. **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.

B. DEFINITIONS

1. **Breach (HIPAA):** The acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. (See APPENDIX A: *Glossary* for more details.)

2. **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).

SECTION 5: SECURITY OF PHI

5.2. Personal Portable Data Devices / Mobile Devices (continued)

3. **Health Information:** any information, including genetic information, whether spoken or recorded in any form that:
   a. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
   b. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
4. **Personal Portable Data Device:** Any easily mobile, hand-held or wearable device that provides creation, manipulation, transmission, storage, and/or retrieval capabilities for information, sound, text, or images for personal or business purposes.
5. **Restricted Data:** Data in any format collected, developed, maintained or managed by or on behalf of the university, or within the scope of university activities, that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to medical records, social security numbers, credit card numbers, Florida driver licenses, non-directory student records and export controlled technical data.
6. **Unsecured PHI:** PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary [of Health and Human Services].
7. **Workforce:** employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity (CE) or business associate, is under the direct control of such CE or business associate, whether or not they are paid by the CE or business associate.

C. PRIVACY REQUIREMENTS

1. **Security standards: General rules.** Covered entities and business associates must do the following:
   a. Ensure the confidentiality, integrity, and availability of all electronic PHI the CE or business associate creates, receives, maintains, or transmits.
   b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
   c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.
   d. Ensure compliance with the Security Rule by its workforce.
2. **Administrative safeguards:** Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the CE or business associate.

D. PROCEDURES

1. **Training:** Complete the Mobile Device Privacy and Security Training

SECTION 5: SECURITY OF PHI

5.2. Personal Portable Data Devices / Mobile Devices (continued)

2. **Protect Contents:** Use all available measures to protect data stored on or transmitted through portable data devices, including, but not limited to:
   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.
      1) Configure the Mobile Device to require a strong password, consistent with or exceeding UF password requirements and to allow no more than ten (10) failed password entry attempts before the device auto-locks.
      2) Configure the device with an inactivity timeout of not more than 10 minutes, which requires re-authentication before use.
   c. *Use Encryption Programming and Maintain It:* Download and use only approved software to communicate and protect PHI, PII, or other restricted data during transmission over any wireless network and any non-UF wired network.
      1) Contact the UF and/or AHC IT departments with any questions regarding approved software. Update virus protection and malicious software detection and removal products as often as recommended.
      2) An exception to this encryption requirement would only be for specific uses where no restricted data of any type will be stored and encryption would interfere with the device's intended use.
3. **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.
4. **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.
5. **Label Devices:** Place an engraved, electronic, or otherwise indelible label with the owner's name and contact information sufficient to facilitate return on all portable data devices.
6. **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 whenever possible.
   b. When not in use, turn the device off and store it in a locked or otherwise secure area.
   c. Do not leave data devices unattended in personal vehicles!
7. **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.

SECTION 5: SECURITY OF PHI

5.2. Personal Portable Data Devices / Mobile Devices (continued)

8. **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. UF or AHC IT Security Office
   c. UF Police Department

E. REFERENCES

HIPAA: 45 CFR §164.302 Security Standards, §164.308 Administrative safeguards; §164.312 Technical Safeguards; § 164.402 Definitions.

F. EXHIBITS

None

Back to Table of Contents