Policy:  Privacy Training & Education
Effective: 9/1/2018

Section 1: GENERAL PRIVACY RULES

1.9 Training and Education

POLICY

1. Training and Education regarding Privacy and Security of Health Information is required for all members of the University of Florida (UF) workforce in health care components. Training is provided by UF as follows:

   a. HIPAA Privacy: General Awareness Training
      i. For each new member of the workforce, to be completed within the first 30 days after the person joins the workforce;
      ii. Required annually by all workforce members.
   b. Supplemental Role-based HIPAA and Privacy Training for workforce members based on their position and/or responsibilities, including:
      i. Policies and Procedures Training for faculty, staff, students, and volunteers.
      ii. HIPAA for Researchers for all members of human subject research teams.
   c. Focused HIPAA Privacy and Security Training for members of the workforce whose functions are specialized, requiring more narrow or in-depth training.
   d. Update HIPAA Privacy and Security Training for members of the workforce whose functions are affected by a material policy or procedure change, within a reasonable period of time after the change becomes effective.

2. Documentation: UF maintains electronic records of training provided to all workforce members for the retention period prescribed in the HIPAA Privacy regulations.

3. Scope of Participation: All members of the UF workforce in health care components are required to complete an appropriate training module, review the Health Information Policy and sign the Confidentiality Statement at orientation and annually.

   a. Failure to comply with the training requirements is a Level Two (2) Privacy violation.
   b. Failure to complete the requirements within 60 days after joining the workforce or the annual renewal due dates will result in:
      i. Loss of access to hospital and other computer systems for those who have such access. Access will not be reinstated until the required training has been completed and the training certificate hand-delivered to the Privacy Office.
      ii. For those who do not have computer access, a mandatory meeting with the Chief Privacy Officer and the employee’s immediate supervisor.
      iii. Disenrollment or suspension from classes for students.
      iv. Other sanctions as prescribed by policy may also be imposed.

4. Personal and Departmental Responsibilities: Each individual, as a member of the workforce, is ultimately responsible for maintaining personal compliance with UF’s Privacy training requirements. Supervisors in all
colleges, departments, divisions, and clinics are responsible for maintaining records of training compliance for all workforce members. Other responsibilities include:

a. Incorporating appropriate training into interviewing, hiring and orientation procedures for new staff, students, and volunteers,

b. Making all workforce members aware of any changes in Information Privacy and Security training requirements, and

c. Ascertaining that workforce members have completed all training requirements.

DEFINITIONS:

1. **Workforce:** employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by such entities. At UF, this includes UF faculty, staff, students, volunteers, trainees, and any other person, including, but not limited to, visiting and associate clinicians, visiting faculty, Business Associates, and other persons performing services for UF, whether temporary or permanent, full-time and part-time, whose conduct, in the performance of work with or for UF, is under UF’s direct control, regardless of whether the person is paid for their services or not.

2. **myTraining:** an integrated training-management system available for UF’s workforce; a one-stop location where faculty and staff can manage training records, view training schedules, register for professional and required classes and complete online training. myTraining Registration link: [http://mytraining.hr.ufl.edu/](http://mytraining.hr.ufl.edu/)

PRIVACY REQUIREMENTS:

1. **Security awareness and training.** A covered entity (CE) or business associate must implement a security awareness and training program for all members of the workforce (including management).

2. **Privacy Standard training:** A CE must train all members of its workforce on the policies and procedures with respect to PHI required by the Privacy Rule, as necessary and appropriate for the members of the workforce to carry out their functions.

   a. A CE must provide training to each new member of the workforce within a reasonable period of time after the person joins the CE’s workforce; and to each member of the CE’s workforce whose functions are affected by a material change in the policies or procedures within a reasonable period of time after the material change becomes effective.

   b. A CE must document that the training has been provided.

3. Overview of available myTraining modules is below.

   - HIPAA & Privacy – General Awareness (PRV800)
   - HIPAA & Privacy – Research (PRV801)
   - HIPAA for Fundraisers
   - FERPA Basics (PRV802)
   - FERPA for Faculty (PRV803)
   - Protecting Social Security Numbers (PRV804)
   - Identity Theft and Red Flags Rule (PRV805)

TRAINING PROGRAMS:

**Level One Training:** General Awareness
1. **HIPAA & Privacy: General Awareness** (may be replaced by HIPAA for Researchers)
   a. Participants include, but are not limited to the following, whether they have contact with patients or PHI or not:
      - All members of the workforce as defined in this policy;
      - Visiting and associate faculty, students, and other persons performing services for UF;
      - Business associates, as needed.
   b. Frequency:
      - At orientation or other entry into the UF workforce.
      - Annually thereafter.

2. **Research and Information Privacy:** HIPAA for Researchers
   a. Participants: All personnel involved in human subject research activities; including, but not limited to:
      - Principal investigators, co-principals and sub-investigators,
      - All research coordinators,
      - All staff with access to research-related PHI.
   b. Frequency:
      - Prior to submitting new research protocols, and annually thereafter as long as the participants are involved in human subject research.
      - Failure to maintain current training certification may be cause for rejection, suspension, or significant delay of a research protocol under review.

**Level Two Training: Health Information Privacy Policies and Procedures**

1. Participants: Administrative and Management Clinical and Non-Clinical Personnel who may have contact with PHI, or who supervise persons who have contact with patients and/or PHI.
2. Frequency: At orientation, and as needed thereafter, relative to changes in policies and/or changes in roles or job descriptions.
3. Content:
   a. Reporting and Responding to Privacy Complaints and Violations
   b. Health Information and Record Management Policies
   c. Patient’s Rights Procedures & Verification of Identity and Authority
   d. Uses and Disclosures of PHI & Minimum Necessary Rule
   e. Accounting for Disclosures

**Level Three Training: Role-Specific Tutorials**

1. **Notice of Privacy Practices:** Optional training
   a. Participants: All personnel who have first contact with patients
   b. Frequency: At orientation, and as needed thereafter, relative to changes in policies and/or changes in roles or job descriptions.
2. **Disclosure Tracking & Accounting**: Mandatory training for designated staff
   a. Participants: Only designated personnel authorized to enter data in UF’s On-Line Disclosure Tracking System.
   b. Frequency: Prior to receiving access to the system, annually, and as needed thereafter, relative to changes in policies and/or changes in roles or job descriptions.

3. **HIPAA for Fundraisers**: Mandatory training for designated staff
   a. Participants: Personnel in HSC development offices involved in fundraising and donor relations with patients.
   b. Frequency: During new-hire orientation, annually, and as needed thereafter, relative to changes in policies and/or changes in roles or job descriptions.

4. **Mobile Device Management**: Optional training
   a. Participants: All personnel who use mobile devices to communicate PHI.
   b. Frequency: At orientation, and as needed thereafter, relative to changes in policies and/or changes in roles or job descriptions.
   c. Content: Describes possible risks, acceptable use standards and safeguards, and approved software if you use a smartphone, laptop, or tablet (collectively called “Mobile Devices”) to communicate PHI.

**Training Procedures**

1. **Online Self-Directed Training Modules**
   a. Access and enroll in the appropriate on-line Training Program through the myUFL web site: https://my.ufl.edu/ps/signon.html, My Self-Service, Training and Development.
   b. Successfully complete the training module and obtain a passing score on the quiz.
   c. Print the Certificate of Completion, if provided (not all training modules provide a certificate).

2. **Face-to-Face Health Information Privacy Policies and Procedures Training**: Include in orientation to any new position; repeat as and when needed. Supervisors should:
   a. Present or coordinate the employee’s attendance at, or completion of, necessary Level Two Privacy and Security training, either as on-the-job, self-directed, or classroom instruction, as appropriate.
   b. Document the amount of training presented and include the record in the individual’s personnel file.

**REFERENCES:**

1. HIPAA: 45 CFR §164.308 (a)(5)(i) - Security Training, §164.530(b)(1) and (2) - Privacy Training

**EXHIBITS:**

None