Section 1: GENERAL PRIVACY RULES

1.9 Training and Education

POLICY

1. Training and Education.
    a. All members of the University of Florida (UF) Workforce will be trained on Privacy policies and procedures with respect to the protection and use of restricted information.
    b. Training must be conducted to the extent necessary and appropriate for the Workforce to carry out their job responsibilities.
2. Documentation.
    a. UF maintains electronic records of training provided to Workforce members for the retention period as prescribed in the applicable law or regulation.
3. Scope of Participation
    a. All members of the UF Workforce are required to complete appropriate Privacy training at hire and annually thereafter.
    b. Failure to comply with the training requirements may result in:
        i. Progressive sanctioning or disciplinary action;
        ii. Loss of access to information systems where training is a requirement for such access.
4. Workforce and Departmental Responsibilities.
    a. Each individual, as a member of the Workforce, is ultimately responsible for maintaining compliance with UF's Privacy training requirements.
    b. Supervisors in all units (e.g., colleges, departments, divisions, clinics, etc.) are responsible for maintaining records of training compliance for all Workforce members.
    c. Other supervisor responsibilities include:
        i. Incorporating unit specific training into new hire orientation and routinely providing supplemental or specialized training to members of the Workforce based on their position or responsibilities;
        ii. Informing and training Workforce members, whose functions are affected by a material change in policies or procedures, within a reasonable period of time after a change becomes effective;
        iii. Monitoring Workforce training to ensure all privacy training requirements are met and current.

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/
3. ***Restricted Data:*** Data (information) in any format collected, developed, maintained or managed by or on behalf of UF, or with the scope of UF activities that are subject to specific protections under federal or state law or regulations (HIPAA, FERPA, Red Flags Rule, etc.), or under applicable policies or contracts.

PRIVACY REQUIREMENTS

1. All members of the University of Florida (UF) Workforce will be trained on Privacy policies and procedures with respect to the protection and use of restricted information.
2. Privacy training must be completed at hire and then annually, or other specified time period, thereafter.
3. Training must be conducted to the extent necessary and appropriate for the Workforce members to carry out their job responsibilities.
4. Completion of Privacy training must be documented and retained as prescribed in the applicable law or regulation.
5. The UF Privacy Office will develop privacy training resources to facilitate the privacy training of Workforce members.

TRAINING AND EDUCATIONAL RESOURCES

1. The UF Privacy Office website provides an overview of current modules and resources under the 'Training' category.
2. Training modules and resources are described below.

HIPAA & Privacy: General Awareness (PRV800)

Availability: myTraining
Audience: Required for all Workforce members who have contact with patients or protected health information (PHI)
Frequency: At hire and annually thereafter

Health Information Confidentiality Statement

Availability: UF Privacy Office website (http://privacy.ufl.edu/)
Audience: Required for all Workforce members, as defined in this policy, who have contact with patients or PHI, or are involved in human subject research activities
Frequency: At hire and annually thereafter

Disclosure Tracking & Accounting

Availability: UF Privacy Office website (http://privacy.ufl.edu/uf-health-privacy/accounting-for-disclosures/)
Audience: Required for Workforce members designated to access either Epic or UF's Disclosure Tracking System to account (record) certain disclosures of PHI.
Frequency: Prior to receiving access to the Disclosure Tracking System (DTS) and as needed thereafter

FERPA Basics (PRV802)

Availability: myTraining
Audience: Recommended for Workforce with access to student records
Frequency: At hire and annually thereafter

FERPA for Faculty (PRV803)

Availability: myTraining
Audience: Recommended for faculty, instructors, including TAs, with access to student records
Frequency: At hire and annually thereafter

HIPAA for Fundraisers

Availability: myTraining
Audience: Recommended for personnel in the HSC Development Office and other persons involved in fundraising or donor relations with patients
Frequency: At hire and annually thereafter

Mobile Device Management

Availability: myTraining
Audience: Recommended for Workforce members who use mobile devices (smartphones, tablets, laptops) to communicate Restricted Data (i.e., PHI)
Frequency: At hire and as needed thereafter.

Privacy in Today's World of Higher Education (PRO331)

Availability: Instructor-led
Audience: Optional. Provides essential information about privacy application in academia; provides an understanding of responsibilities and obligations to assure UF compliance
Frequency: Periodic; see myTraining for next scheduled session

Protecting Social Security Numbers & Identity Theft Prevention (PRV804)

Availability: myTraining
Audience: Required for Workforce who collect or have access to SSNs, or who routinely work with payment card data, consumer reports or covered accounts
Frequency: At hire and annually thereafter

REFERENCES

1. HIPAA 45 CFR §164.308 (a)(5)(i) - Security Training, §164.530(b)(1) and (2) - Privacy Training
2. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
3. Florida Statute 119.071 (5) – Use and Collection of Social Security Numbers
4. Title 16 CFR – Commercial Practices: Part 681 Identity Theft Rules