FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

University Community (faculty, staff, students)

SUBJECT (R*)	EFFECTIVE DATE (R*)	POLICY NUMBER (O*)
HIPAA PRIVACY AND SECURITY: REQUIRED EDUCATION OF COVERED WORKFORCE	December 31, 2017	1640.010

POLICY STATEMENT (R*)

In accordance with the requirements of the regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), all members of the University's workforce in each health care component or who otherwise have access to protected health information as part of their job responsibilities at Florida International University must receive education and training regarding the University's obligations under the HIPAA regulations and the University's policies and procedures.

All workforce members who have access to protected health information must receive this education and training as of the effective compliance date for Florida International University. Individuals who commence their employment with Florida International University after the effective compliance date, or those who transition to employment within the University to a unit or department where they will have access to protected health information as part of their job responsibilities, must receive education and training within a reasonable time (not to exceed thirty (30) days) from the time that they join the workforce or transfer to a University department or unit wherein they will have access to protected health information.

REASON FOR POLICY (O*)

To ensure that members of Florida International University's workforce complete required education and training regarding the privacy and confidentiality of protected health information in accordance with the requirements of the HIPAA regulations.

RELATED INFORMATION (O*)

HIPAA Privacy Rule, 45 C.F.R. § 164.530(b)
HIPAA Privacy Policy: Health Insurance Portability and Accountability Act Compliance
Administrative Safeguards, HIPAA Security Standards, 45 C.F.R. §164.308(a)(5)

DEFINITIONS (R*)

"Business associate" means, with respect to a covered entity, a person or entity who:

- Assists (other than as a member of the Covered Entity's workforce) in the performance of :
    1. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
    2. Any other function or activity regulated under the HIPAA regulations; or
    3. Provides, other than as a member of the Covered Entity's workforce, the following types of services: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, where the provision of such services involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

"Health care component" means a component or combination of components of a hybrid entity that has been specifically designated by the covered entity because it either performs covered functions; or activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

"HIPAA Security Administrator" is the individual designated by each health care component to assist in the implementation and maintenance of systems and processes for the creation, maintenance and transmission of protected health information via electronic means and to work in collaboration with the HIPAA Security Officer, HIPAA Privacy Officer and other designated University representatives to ensure that the University creates and maintains an information technology environment that is compliant with

applicable federal and state law governing health information privacy and confidentiality.

"HIPAA Security Officer" is the individual designated by the University to assist in the implementation of the HIPAA Security Standards, 45 C.F.R. Parts 160, 162 and 164, and to oversee and monitor the University's compliance with the required technical, administrative and physical safeguards as these relate to protected health information created, maintained or transmitted via electronic means. The University Information Technology Security Officer is designated as the HIPAA Security Officer.

"Individually identifiable health information" means information that is a subset of health information, including demographic information collected from an individual, and:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- 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; and
    1. That identifies the individual; or
    2. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Protected health information" or "PHI" means individually identifiable health information that is:

- Transmitted by electronic media;
- Maintained in electronic media;
- Transmitted or maintained in any other form or medium.
- Protected health information specifically excludes:
    1. Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g ("FERPA");
    2. Records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and
    3. Employment records held by a covered entity in its role as an employer.

"Workforce" or "workforce member" means part-time, full-time or temporary faculty and staff, students, volunteers, trainees, and other persons whose conduct, in the performance of work for the University, is under the direct command of the University (regardless of whether or not they are paid by the University).

PROCEDURES (O*)

Education and training to be provided to workforce members shall be appropriate to their ability to carry out their function on behalf of the health care component. Departments or units are responsible for ensuring that they identify those individuals who will be hired or transferred to a position in which the workforce member will have access to protected health information and will make such information available to the University Privacy Officer on a timely basis, in order for the education and training to take place in a timely manner.

To the extent that the workforce member will have access to electronic protected health information, the education and training will also include a security awareness which shall be provided by the HIPAA Security Officer, the HIPAA Security Administrator, or the HIPAA Privacy Officer, as shall be necessary or appropriate. The information technology security awareness education and training shall include, without limitation:

1. Protection from malicious software use (including virus protection)
2. Periodic security updates
3. Log-in
4. Password management
5. Appropriate retention and destruction of electronic protected health information

The department's or unit's designated HIPAA Security Administrator is responsible for ensuring that workforce members of the department or unit have received this training.

The department's or unit's designated HIPAA Security Administrator will periodically send out security reminders to make workforce members aware of security concerns and initiatives on an ongoing basis.

Successful completion of initial and periodically recurring training is a prerequisite for system access and a factor of job performance. Failure to successfully complete initial or recurring training will result in denial of system access. Documentation of completion of the security awareness training shall be maintained by the HIPAA Security Administrator. Training logs shall be made available to the HIPAA Security Officer, the HIPAA Privacy Officer, the Vice President of Human Resources or the Provost upon request.

HISTORY (R*)

Initial Effective Date: September 1, 2009; December 31, 2017

RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)	
Division of Academic Affairs Florida International University **RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)** University Compliance and Privacy Officer University Compliance Office PC 429 11200 S.W. 8th Street Miami, FL 33199 Telephone Number: (305) 348-2216	The University Policies and Procedures Library is updated regularly. In order to ensure a printed copy of this document is current, please access it online at www.policies.fiu.edu. For any questions or comments, the "Document Details" view for this policy online provides complete contact information.

***R = Required *O = Optional**