FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

HIPAA Privacy and Security Rule Training # 1660.075

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 1, 2009	October 13, 2020	Office of Compliance and Integrity

POLICY STATEMENT

In accordance with the requirements of the regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which restrict Florida International University's (FIU) HIPAA Hybrid Designated Health Care Components (Components) ability to use and disclose patient Protected Health Information (PHI), FIU will comply with HIPAA's requirements. To that end, all FIU Component Workforce members and students (hereinafter Workforce members) as defined in this policy and procedure shall receive mandatory HIPAA Privacy and Security Rule training, as well as state law and/or regulation training in support of FIU's commitment to the proper use, disclosure, and safeguarding of PHI and electronic PHI (ePHI) from any intentional, unintentional or incidental use or disclosure to unauthorized individuals.

As a University-wide policy and procedure, this policy and procedure takes precedence over any Component-specific policies, procedures, or protocols that conflicts with this policy and procedure, unless prior approval is obtained from the Office of Compliance and Integrity. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

Components may maintain HIPAA documentation in either paper or electronic form, provided that any format is sufficiently protected to ensure it will be retrievable throughout the required retention period. Unless otherwise indicated in FIU Privacy or Security Rule Policy and Procedure, each Component Privacy Coordinator will be responsible for maintaining all HIPAA documentation relevant to his/her Component. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

Workforce members who fail to adhere to this policy and procedure may be subject to civil and criminal penalties as provided by law, and/or administrative and disciplinary action. (FIU Policy and Procedure #1660.085) (Sanctions)

Each Component must designate a HIPAA Privacy Coordinator and a HIPAA Security. (FIU Policy and Procedure #1660.070) (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)

FIU reserves the right to amend, change or terminate this policy and procedure at any time, either prospectively or retroactively, without notice. Any ambiguities between this policy and procedure and the other policies and procedures should be accordingly made consistent with the requirements of HIPAA and state law and regulation. (FIU Policy and Procedure #1660.080)

SCOPE

This policy applies to FIU's HIPAA Health Care Components that are contained within FIU's HIPAA Hybrid Designation (FIU Policy and Procedure #1610.005), its Workforce members and Business Associates as defined in this policy and FIU Policy and Procedure #1660.015 regarding Business Associate Agreements.

REASON FOR POLICY

To establish procedures necessary for the proper training of Workforce members involved in the access, creation, use and disclosure of patient PHI as described by HIPAA.

45 CFR §160.103 and 45 CFR §164.530(b) (Administrative Requirements - Training)

DEFINITIONS

TERM	DEFINITIONS
Access	Means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
Administrative Officer	Means the Component Workforce member responsible for financial management, human resources administration, management of facilities and equipment, and other administrative functions required to support the teaching and research missions of the FIU HIPAA Hybrid Designated Health Care Component. The Administrative Officer is the senior administrative staff position in the department, Division or Office and provides continuity as academic leadership changes.
Administrative Safeguards	Are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
Availability	Means the property that data or information is accessible and useable upon demand by an authorized person.

Business Associate	Generally an entity or person who performs a function involving the use or disclosure of Protected Health Information (PHI) on behalf of a covered entity (such as claims processing, case management, utilization review, quality assurance, billing) or provides services for a covered entity that require the disclosure of PHI (such as legal, actuarial, accounting, accreditation). **NOTE:** A business associate relationship exists when an individual or entity, acting on behalf of an FIU HIPAA Component(s), assists in the performance of a function or activity involving the creation, use, disclosure, or access of PHI. This includes, but not limited to, claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management or repricing. **NOTE:** A Business Associate may include any individual or entity that receives PHI from a HIPAA Component in the course of providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, software support, or financial services. A Business Associates does not, however, include HIPAA Component workforce members.
Business Associate Agreement	Means a contract or other written arrangement with a business associate which must describe the permitted and required uses of protected health information by the business associate; Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.
Breach	Means the unauthorized acquisition, access, use, or disclosure of Protected Health Information (PHI) that compromises the security or privacy of the data and poses a significant risk of financial, reputational, or other harm to the client.
Code of Federal Regulations	Also known as CFR
Component	Means a component or combination of components of a hybrid entity designated by the hybrid entity (Florida International University). Those programs designated by FIU that must comply with the requirements of the Health Insurance Portability and Accountability Act of 1996, hereinafter referred to as "Components". Components of FIU are required to comply with

	the Administrative Simplification provisions of HIPAA because the Components perform a covered function.
Confidentiality	Means data or information is not made available or disclosed to unauthorized persons or processes.
Covered Entity	An entity that is subject to HIPAA. 1. a health plan; 2. a health care clearinghouse; and/or 3. a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
Disclosure	Means the release, transfer, provision of access to, or divulging in any other manner of protected health information outside of the entity holding the information.
Electronic Protected Heath Information (ePHI)	PHI in electronic form. See also: PHI.
Florida Statutes	Also known as F.S.
Health Care	Means the care, services, or supplies related to the health of a patient, including: 1. preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of a patient or that affects the structure or function of the body; and 2. sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
Health Care Component	See "Component"
Health Care Operations	Means any of the following activities: 1. quality assessment and improvement activities, including case management and care coordination; 2. competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; 3. conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; 4. specified insurance functions, such as underwriting, risk rating, and reinsuring risk; 5. business planning, development, management, and administration; and 6. business management and general administrative activities of the entity, including but not limited to: a. de-identifying protected health information,

	b. creating a limited data set, and c. certain fundraising for the benefit of the covered entity.
Health Care Provider	Means a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
U.S. Department of Health and Human Services	Also known as HHS.
Health Information	Means any information, whether oral or recorded in any form or medium, that 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 relates to the past, present, or future physical or mental health or condition of an patient; the provision of health care to an patient; or the past, present, or future payment for the provision of health care to an patient.
HIPAA	Means the Health Insurance Portability and Accountability Act of 1996.
Hybrid Covered Entity	Means a single legal entity that performs both covered and non-covered functions. The entity has a defined health care component that engages in HIPAA electronic transactions.
Individually Identifiable Health Information	Means information that is a subset of health information, including demographic information collected from an individual, and 1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and 2. 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 a. That identifies the individual; or b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Integrity	Means the property that data or information have not been altered or destroyed in an unauthorized manner.
Patient	The person who is the subject of the PHI.
Physical safeguards	The physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Privacy Coordinator	Means an FIU Workforce member, appointed by the director, manager, or supervisor of a HIPAA Designated Component to conduct and/or coordinate with necessary and appropriate Workforce members all HIPAA Privacy Rule activities and actions within the Component, including but not limited to tracking HIPAA training activities; coordinating HIPAA Privacy Rule implementation; participating in HIPAA Privacy and Security Rule violation investigations, as necessary and appropriate, communicating with the Director of Compliance and Privacy for Health Affairs, the HIPAA Security Officer, and the Office of General Counsel, as necessary and appropriate, regarding HIPAA Privacy and Security Rule activities and concerns; conducting and reporting monitoring activities; participate in assessments; and responding to, tracking and documenting HIPAA Privacy Rule activities. Maintain ongoing communication with the Director of Compliance and Privacy for Health Affairs and the HIPAA Security Officer.
Protected Health Information (PHI)	Means any individually identifiable health information collected or created in the course of the provision of health care services by a covered entity, in any form (written, verbal or electronic). PHI relates to the past, present, or future physical or mental health or condition of an individual or the past, present, or future payment for the provision of health care to an individual. Protected Health Information however 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.
Privacy Rule	The regulations at 45 CFR 160 and 164, which detail the requirements for complying with the standards for privacy under the administrative simplification provisions of HIPAA.
Student	Means an individual who is a student and has access to PHI in their role as a participant in a clinical health professional training program within a Component of the FIU HIPAA Hybrid Designation. For example, medical students who are assigned to a clinical experience in FIU Practice as part of their educational program would be considered a student for purposes of this policy and procedure. Additionally, students would also be defined as a "Workforce" member during the clinical experience.

Subcontractor	Means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
Technical safeguards	Means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
Secretary	Means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.
Standard	Means a rule, condition, or requirement: 1. Describing the following information for products, systems, services, or practices: a. Classification of components; b. Specification of materials, performance, or operations; or c. Delineation of procedures; or 2. With respect to the privacy of protected health information.
Treatment, payment, and healthcare operations	(TPO)
Treatment	Means the provision, coordination, or management of health care and related services among health care providers or by a healthcare provider with a third party, or consultative services among providers regarding a patient.
Use	With respect to patient identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
Workforce	Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity (FIU HIPAA Component) or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

ROLES AND RESPONSIBILITIES

1. **Compliance Oversight:** The Office of University Compliance and Integrity (University Compliance)
    - Evaluates all federal and state healthcare privacy laws, regulations, rules and ordinances (Rules) to ensure compliance with the Rules.
    - Develops and maintains all required University-wide Privacy Rule policies, procedures and associate forms.
    - Develops and maintains HIPAA health care Privacy Rule training modules and ensures appropriate Workforce members complete the required training.

- Performs audits and assessments of the Components to ensure their compliance with the Privacy Rules and associated FIU Policies and Procedures.
- Partners with the Division of Information Technology HIPAA Security Officer to ensure compliance with all federal and state healthcare privacy and security laws, regulations rules, and ordinances.

2. HIPAA Components:

- Each FIU HIPAA Hybrid Designated Component must designate a Privacy Coordinator responsible for overseeing and ensuring the Component's implementation and compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable state laws and/or regulations governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to ensuring Component Workforce members have received required HIPAA Privacy Rule and Associated FIU Privacy Policy and Procedure training.

RELATED RESOURCES

References

- 45 CFR §164.308
- 45 CFR §164.502
- 45 CFR §164.504
- 45 CFR §164.524
- 45 CFR §164.526
- 45 CFR §164.528
- F.S. §95.11

Related Policies

- FIU Policy # 1610.005 (Designated Health care Components of FIU Community)
- FIU Policy and Procedure #1660.070 (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)
- FIU Policy and Procedure #1660.085 (Sanctions)
- FIU Policy and Procedure #1660.015 (Business Associate Agreements)
- FIU Policy and Procedure #1640.025 (Minimum Necessary)
- FIU Policy and Procedure #1660.080 (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

CONTACTS

For further information concerning this policy, please contact the FIU Office of Compliance and Integrity at (305) 348-2216, compliance@fiu.edu, or the appropriate Component Privacy Coordinator.

HISTORY

Initial Effective Date: September 1, 2009
Review Dates (review performed, no updates): n/a
Revision Dates: December, 31, 2017; October 13, 2020

FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

HIPAA Privacy and Security Rule Training # 1660.075a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 1, 2009	October 13, 2020	Office of Compliance and Integrity

PROCEDURE STATEMENT

I. HIPAA Privacy and Security Rule Training

Each HIPAA Component must designate a Privacy Coordinator responsible for overseeing and ensuring the Component's implementation and compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable state laws and/or regulations governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to ensuring Workforce members and students (hereinafter Workforce members) complete all required Privacy and Security Rule training prior to obtaining access to patient PHI and as required by this Policy and Procedure. Privacy Coordinators may delegate and share duties and responsibilities as necessary and appropriate but retain oversight responsibility. (FIU Policy and Procedure #1660.070) (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)

A. HIPAA Privacy and Security Training of FIU HIPAA Hybrid Designated Component Workforce Members and Students (Workforce members)

1. All required HIPAA Privacy and Security Rule training MUST be completed prior to providing Workforce members access to patient PHI. The training is required by federal HIPAA regulations, state law, and FIU Policy and Procedure.

2. Retraining shall occur biennially, or sooner whenever there are material changes in the HIPAA regulations, state law, and/or FIU HIPAA Privacy or Security Rule Policies and Procedures, or whenever the Office of Compliance and Integrity and/or the Division of Information Technology determine it is necessary to ensure compliance with HIPAA regulations and/or state law.

3. HIPAA training must be provided in a format that is accessible to persons with disabilities and those who are not fluent in English.

4. Each Component Privacy and Security Coordinator shall submit to the FIU Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity, and the HIPAA Security Officer, Division of Information Technology, on a calendar

quarterly basis a report of training compliance. (FIU Policy and Procedure #1660.090) (HIPAA Component Privacy Rule Review and Audit).

5. Web-based training for clinical and research settings will be provided by FIU. Component specific training for each clinical setting within the FIU HIPAA Hybrid Designation is the responsibility of the Component's Privacy and Security Coordinators appointed by the Component Administrative Officer(s).

6. Any additional training as described above in Section I.5 that is developed by or for a Component must be developed in consultation with the FIU Director of Compliance and Privacy for Health Affairs and the HIPAA Security Officer to ensure FIU's compliance with HIPAA and state law or regulation and established FIU Policies and Procedures.

7. The FIU Component Privacy and Security Coordinators must ensure students participating in a clinical health professional training program within the FIU HIPAA Hybrid Designated Health Care Components have competed the HIPAA training required for Health Care Component Workforce members, even if the student's academic department includes education regarding HIPAA in its academic curriculum.

8. The FIU Component Privacy and Security Coordinators must ensure all training completed by students participating in a clinical health professional training program within the FIU HIPAA Hybrid Designated Health Care Components is properly documented as required for all Workforce members.

9. To the extent that the Workforce members and students will have access to patient electronic Protected Health Information (ePHI), the education and training will also include a security awareness training which shall be provided by the HIPAA Security Officer and/or the Component HIPAA Security Coordinator, as necessary or appropriate. The information technology security awareness education and training shall include, without limitation:
   a. Protection from malicious software use (including virus protection)
   b. Periodic security updates
   c. Log-in
   d. Password management
   e. Appropriate retention and destruction of electronic PHI (ePHI)

10. A record of each Workforce member's successful completion of training (and retraining) must be retained as identified below in Section II. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation).

B. HIPAA Privacy and Security Rule Training for Students Participating in a Clinical Health Professional Training Program at a non-FIU Health Care Facility

1. The training of students who have access to PHI at health care facilities outside FIU as part of their academic program is the responsibility of the outside health care facility/provider, unless there is a contractual agreement between the facility/provider and FIU requiring otherwise.

C. PHI and ePHI Access for Workforce Members and Students

1. Workforce members and students will not have access to PHI and ePHI until such time as they have successfully completed all required FIU HIPAA Privacy and Security Rule training.

2. Access to PHI and ePHI shall be immediately terminated, or as required by FIU HIPAA Security Rule Policy and Procedure, whenever the Workforce member's or student's responsibilities no longer require such access. (e.g., termination of employment, reassignment of duties, or graduation).

3. Component Privacy and Security Coordinators are responsible for implementing the Workforce member and student access policy.

II. Compliance

A. Because FIU is required to ensure compliance with HIPAA regulations and state law, periodic audits and assessments will be conducted to ensure compliance with the HIPAA Privacy and Security Rules. (FIU Policy and Procedure #1660.090) (HIPAA Component Privacy Review and Audit)

B. Successful completion of initial, biennial, and all other trainings the Office of Compliance and Integrity, the Division of Information Technology, and the Workforce member's Component, determine to be necessary and appropriate, is a prerequisite for system access and a factor of job performance. Failure to successfully complete required training will result in denial of system access and to patient PHI.

III. Curriculum Content

A. While this policy and procedure requires the FIU Components to train students who have access to patient PHI and ePHI in their Component, it is not the intent of this policy and procedure to dictate the inclusion of HIPAA requirements in the curriculum of academic departments. The extent of HIPAA and state law is solely an academic decision.

IV. Record/Documentation Retention

A. Documentation of completion of the required HIPAA Privacy Rule, HIPAA Security Rule, and Security Awareness training shall be maintained by the Component Privacy and Security Coordinators. Training logs shall be made available to the Director of Compliance and Privacy for Health Affairs, the HIPAA Security Officer, the Vice President of Human Resources or the Component Administrative Officer(s) upon request. (Also See FIU Policy and Procedure #1660.090) (HIPAA Component Privacy Review and Audit)

B. If a communication, action, activity, or designation is required to be documented in writing, the document or record owner (e.g. the Office of Compliance and Integrity) will maintain such writings, or an electronic copy, for seven (7) years from the date of its creation or the last effective date, whichever is later. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)