FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Complaints Under the HIPAA Privacy Rule, Mitigation, Refraining From Intimidating or Retaliatory Acts, and Waiver #1660.065

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 13, 2020	February 29, 2024	Office of Compliance and Integrity

POLICY STATEMENT

Florida International University (FIU) requires that each FIU Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Health Care Component (Component) receive complaints from individuals who believe FIU is not complying with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable federal laws or Florida state statutes governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI) and to provide further information in response to complaints.

An individual who believes a Component is not complying with the applicable requirements of the HIPAA Privacy Rule, federal law or Florida state statute may file a complaint with the Component Privacy Coordinator, the Director of Compliance and Privacy for Health Affairs, the FIU Office of General Counsel, the Office of Compliance and Integrity, and/or the Secretary of the U.S. Department of Health and Human Services (HHS).

FIU acknowledges that the Secretary of HHS is empowered to and may investigate any complaints. Accordingly, FIU will cooperate with any investigation or compliance review. FIU will keep records including pertinent policies, procedures, or practices and of the circumstances regarding any alleged violation. FIU will submit compliance reports or corrective action plans, in a timely manner as requested by the Secretary of HHS.

FIU's Office of Compliance and Integrity and the Division of Information Technology, in cooperation with appropriate Component Privacy and Security Coordinators will investigate alleged violation of FIU's HIPAA Privacy and Security Rule Policies and Procedures consistent with the requirements of FIU's Reporting of HIPAA Incidents and Notification in Cases of Breaches Policy and Procedure #1660.095 and the FIU Incident Response Plan.

FIU will include contact information for filing a complaint in its Notice of Privacy Practices. The contact information will include the name, title, and telephone number of the FIU Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity.

FIU Workforce members and its Business Associates will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising any right established under the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies

and Procedures, or for participation in any process provided by the HIPAA Privacy Rule HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, including the filing of a complaint; and FIU and its Business Associates will not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual for:

(1) Filing of a complaint with the Secretary of HHS;
(2) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing regarding the HIPAA Privacy and/or Security Rules and FIU's associated HIPAA Privacy Policies and Procedures, or
(3) Opposing any act or practice made unlawful under the HIPAA Privacy and/or Security Rules, provided the individual has a good faith belief that the practice opposed is unlawful or in violation of FIU HIPAA Privacy and Security Policy and Procedure, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the Privacy Rules.

FIU and the FIU Components will not require an individual who is the subject of the PHI who believes FIU and/or an FIU Component or Business Associate is not in compliance with, or has not complied with the HIPAA Privacy and/or Security Rules, federal law and/or Florida state statute to waive their right to file a complaint with the Secretary of HHS as a condition of the provision of treatment, payment or eligibility for benefits.

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)

All Component Workforce members shall receive mandatory HIPAA Privacy and Security Rule training. (FIU Policy and Procedure # 1660.075) (HIPAA Privacy and Security Rule Training)

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 Coordinator. (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) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

SCOPE

This policy applies to FIU's HIPAA Hybrid Designated Components that are contained within FIU's HIPAA Hybrid Designation (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 Associates Agreements.

REASON FOR POLICY

To establish procedures necessary for individuals to file complaints and report known or suspected violations related to the HIPAA Privacy Rule, federal law, Florida state statutes, and FIU's HIPAA Privacy and Security Policies and Procedures.

DEFINITIONS	
TERM	**DEFINITIONS**
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.
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.
Code of Federal Regulations	Also known as CFR is the codification of the general and permanent regulations promulgated by the executive departments and agencies of the federal government of the United States
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.
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.
Florida Statutes	Also known as F.S. are the codified, statutory laws of Florida
Health Care Component	See "Component"

U.S. Department of Health and Human Services	Also known as HHS is a cabinet-level executive branch department of the U.S. federal government created to protect the health of the U.S. people and providing essential human services.
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.
Implementation Specifications	Means specific requirements or instructions for implementing a standard.
Patient	The person who is the subject of the PHI.
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.
Privacy Rule	Means 45 CFR Part 160 and Subparts A and E of Part 164. The U.S. Department of Health and Human Services (at https://www.hhs.gov/hipaa/for-professionals/privacy/index.html?language=es) states that the "Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patient's rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

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.
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: i. Classification of components; ii. Specification of materials, performance, or operations; or iii. Delineation of procedures; or 2. With respect to the privacy of protected health information.
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 and procedures.
    - 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 processing and handling complaints under the HIPAA Privacy Rule.

RELATED RESOURCES

References

- 45 CFR §164.502
- 45 CFR §164.504
- 45 CFR §164.524
- 45 CFR §164.526
- 45 CFR §164.528
- Florida Statute §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 #1660.075 (HIPAA Privacy and Security Rule Training)
- FIU Policy and Procedure #1660.015 (Business Associate Agreements)
- FIU Policy and Procedure #1660.080 (Policies and Procedures, Changes to Policies and Procedures, and Documentation)
- FIU Policy and Procedure #1660.040 (Verification)
- FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in Cases of Breaches)
- 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, hipaaprivacy@fiu.edu, or the appropriate Component Privacy Coordinator.

HISTORY

Initial Effective Date: October 13, 2020
Review Dates *(review performed, no updates)*: n/a
Revision Dates *(review performed, updates made to document)*: October 13, 2020; February 29, 2024.

Complaints Under the HIPAA Privacy Rule, Mitigation, Refraining From Intimidating or Retaliatory Acts, and Waiver #1660.065a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 13, 2020	February 29, 2024	Office of Compliance and Integrity

PROCEDURES

I. Receiving and Processing HIPAA Privacy Rule, Federal Privacy and/or Florida State Statute Privacy Complaints

Each Florida International University (FIU) health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Health Care Component (Component) must designate a Privacy Coordinator responsible for overseeing and ensuring the Component's implementation and compliance with the HIPAA Privacy Rule, federal law, Florida state statute, and FIU's associated HIPAA Privacy Rule Policies and Procedures governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to accepting and processing patient complaints, mitigating, to the extent practicable, any harmful effect that is known to the Component of a use or disclosure of PHI/ePHI in violation of the HIPAA Privacy Rule and FIU's associated HIPAA Privacy Rule Policies and Procedures, ensuring Workforce members and Business Associates refrain from intimidating and retaliatory acts against individuals for exercising any right established under the HIPAA Privacy Rule, federal law, Florida state statutes, and FIU's associated HIPAA Privacy Rule Policies and Procedures, or for participation in any process provided by the HIPAA Privacy Rule, federal law, Florida state statutes, and FIU's associated HIPAA Privacy Rule Policies and Procedures, including the filing of a complaint, and that individuals are not required to waive their right to file a complaint with the Secretary of the federal Department of Health and Human Services (HHS) as a condition of the provision of treatment, payment or eligibility for benefits. 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. The Director of Compliance and Privacy for Health Affairs with the Office of Compliance and Integrity (Designated HIPAA Privacy Officer) and each Component Privacy Coordinator's contact information (i.e., names, telephone numbers and office addresses) must be conspicuously posted in each Health Care Component required to post a Notice of Privacy Practices.

B. Each Privacy Coordinator will be directly accountable to their Component Administrative Officer(s) to whom he/she reports (e.g., CEO, Provost, Dean or Director) for proper and careful handling of patient complaints and questions.

C. Each Privacy Coordinator will use the usual Component processes to provide patient satisfaction and improve patient care on an informal basis.

D. For concerns and questions that can be answered and resolved at the Component level, no other review process is needed.

E. The Privacy Coordinator may consult with the Director of Compliance and Privacy for Health Affairs to assist in resolving and responding to privacy complaints and questions.

F. The Privacy Coordinator must document the receipt and disposition of all complaints received within their Component.

G. If a complaint or question cannot be resolved to the satisfaction of the patient at the Component level or, if at any time, the patient indicates that he/she wishes to make a written complaint related to a HIPAA Privacy Rule or FIU's associated HIPAA Privacy Rule Policies and Procedures, the following procedures will be followed:

1. The Privacy Coordinator will provide the patient with the "Patient Complaint Form", with instructions on how to complete and file the complaint. (See Sample Patient Complaint Form attached). However, the Privacy Coordinator will accept all written complaints if the required information as required on the Patient Complaint Form is provided.

2. The written complaint may be filed with the Component, the Director of Compliance and Privacy for Health Affairs, or the Office of Compliance and Integrity, as identified in FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

3. If the written complaint is filed with the Component, the Privacy Coordinator must:
   a. Document receipt of the complaint on the day received,
   b. Document the name and title of the Privacy Coordinator who received the complaint, and
   c. Timely provide a copy of the complaint to the Director of Compliance and Privacy for Health Affairs.

4. The Director of Compliance and Privacy for Health Affairs will, as necessary and appropriate, adhere to the procedures identified in FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

H. If the complaint or question cannot be resolved to the satisfaction of the patient at the Component level or, if at any time, the patient indicates that he/she wishes to make a

verbal complaint related to the HIPAA Privacy Rule or FIU's associated HIPAA Privacy Rule Policies and Procedures, the following procedures will be followed:

1. The Privacy Coordinator will:
   a. Request and document the name and contact information for the patient,
   b. Document the date, title and name of the Privacy Coordinator who received the complaint,
   c. Document the basis of the complaint,
   d. Provide the patient the contact information for the Office of Compliance and Integrity, the FIU "Ethical Panther line" at https://compliance.fiu.edu/hotline, and
   e. Timely provide the Director of Compliance and Privacy for Health Affairs with a copy of any and all information the patient provided.

2. The Director of Compliance and Privacy for Health Affairs will, as necessary and appropriate, adhere to the procedures identified in FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

I. Investigative Reports to Component Administrative Officer(s) (e.g., CEO, Provost, Dean or Director)

1. Upon competition of an investigation by the Office of Compliance and Integrity, the Director of Compliance and Privacy for Health Affairs will timely notify and provide a copy of all Investigative Reports to the Administrative Officer(s) of the FIU Health Care Component(s) generated in response to formal patient complaints filed against the Component as outlined in FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

2. The Director of Compliance and Privacy for Health Affairs will periodically provide the Health Care Component Administrative Officers with information regarding the number, nature, and resolution of complaints received by the Office of Compliance and Integrity related to their Health Care Component.

II. Mitigation

A. The Director of Compliance and Privacy for Health Affairs, the HIPAA Security Officer, the Office of General Counsel, the Component Privacy and Security Coordinators, and other FIU Workforce members, as deemed necessary and appropriate by the Incident Response Team, will work collaboratively to mitigate, to the extent practicable, any harmful effect that is known to FIU of a use or disclosure of PHI/ePHI in violation of the HIPAA Privacy Rule, federal law, Florida state statutes, and FIU's associated HIPAA Privacy Policies and Procedures governing the confidentiality, integrity and availability of PHI and electronic PHI

(ePHI) by an FIU Workforce member(s) or its Business Associate(s). Mitigation may include retrieving, deleting, or destroying improperly disclosed PHI; terminating access or changing passwords; remote wiping mobile devices; modifying policies or practices; warning recipients of potential penalties for further violations. In some cases, it might include paying for the cost of a credit monitoring service or similar action, and/or notifying affected individuals even if the breach is not required to be reported under the breach notification rules.

B. The Dedicated Investigator(s) will:
   1. Document in the Final Investigative Report file:
      a. The dates, names, and titles of those involved in mitigation efforts and,
      b. The mitigation efforts and outcomes.
   2. Properly secure all written communications sent and received among the Incident Response Team members regarding the mitigation efforts and outcomes, and
   3. Properly secure any and all written communications sent to or received from individuals aversely or potentially adversely impacted by the alleged violation or breach. (FIU Policy and Procedure #1660.095) (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

III. **Refraining From intimidating or Retaliatory Acts**

Complainants/Witnesses

A. FIU Workforce members, Business Associates, and students must refrain from intimidation and retaliation against any individual or other person for:
   - Filing a complaint with the Secretary of the federal Department of Health and Human Services
   - Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing; or
   - Opposing any act or practice made unlawful by the HIPAA Privacy or Security Rules, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of protected health information.

B. FIU will not take any administrative or disciplinary action (sanction) or retaliate against Workforce members or Business Associates who disclose patient PHI, provided:
   1. The Workforce member or Business Associate has a good faith belief that a Health Care Component engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided potentially endangered one or more patients, workers, or the public; and
   2. The disclosure is to:

a. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Health Care Component or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the Health Care Component; or
b. An attorney retained by or on behalf of the Workforce member or Business Associate for the purpose of determining the legal options of the Workforce member or Business Associate with regard to conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided potentially endangered one or more patients, workers, or the public.

Workforce Members who are Victims of Crime

C. FIU will not sanction or retaliate against Workforce members who discloses patient PHI, if the Workforce member is the victim of a criminal act and he/she discloses the PHI to a law enforcement official, provided that:
1. The PHI disclosed is about the suspected perpetrator of the criminal act; and
2. The PHI disclosed is limited to the suspected perpetrator's:
   a. Name and address.
   b. Date and place of birth.
   c. Social security number.
   d. ABO blood type and rh factor.
   e. Type of injury.
   f. Date and time of treatment.
   g. Date and time of death, if applicable.
   h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos, and
3. The Workforce member did not disclose for the purposes of identification or location any PHI related to the suspected perpetrator's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

IV. Waiver

A. See Policy Statement

V. Forms

- Sample Patient Complaint Form

VI. Record/Documentation Retention

A. 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

or the Component) will maintain such writings, or an electronic copy, for seven (7) years m 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)