FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Sanctions #1660.085

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
August 1, 2009	August 6, 2025	Office of Compliance and Integrity

POLICY STATEMENT

Florida International University (FIU) must take disciplinary action against Workforce members, Business Associates, and students (hereinafter Workforce members) who unknowingly, reasonably cause, or willfully neglect to comply with the Health Insurance Portability and Accountability Act (HIPAA) Privacy or Security Rules, FIU's associated HIPAA Privacy or Security Policies and/or Procedures, federal law, and Florida state statutes governing the confidentiality, integrity, or availability of patient Protected Health information (PHI) or commit a breach of PHI or electronic PHI (ePHI) related to FIU's HIPAA Hybrid Designated Components (hereinafter facilities and programs) as defined in FIU Policy #1610.005.

Administrative and disciplinary action taken as it relates to any FIU Workforce member must be in accordance with the applicable FIU Collective Bargaining Agreement, if any, the Human Resources Division administrative or disciplinary policies and procedures, or any other relevant FIU administrative or disciplinary policies or procedures. Administrative and disciplinary action taken as it relates to students shall be in accordance with applicable FIU student disciplinary policies and procedures.

FIU Workforce members, Business Associates, and students will not intimidate, threaten, coerce, harass, discriminate against, or take any retaliatory action against any individual who is the subject of the PHI or other person for exercising any right established under the HIPAA Privacy and Security Rules, or for participating in any process provided for by the HIPAA Privacy and Security Rules, Florida state statutes, and/or FIU associated policy and procedure, including filing a complaint.

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 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.

FIU will not sanction or retaliate against Workforce members or Business Associates who disclose patient PHI, provided:

1. The Workforce member or Business Associate had a good faith belief that an FIU facility or program 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 a facility or program 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 facility or program; 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.

FIU will not sanction or retaliate against Workforce members or Business Associate who discloses patient PHI, if the Workforce member or Business Associate 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,
2. The disclosure is limited to the requirements of the Minimum Necessary Rule and Florida state statute.
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. (See FIU Policy and Procedure #1660.120) (Minimum Necessary)

As a University-wide policy and procedure, this policy and procedure takes precedence over any facility or program-specific policies, procedures, or protocols that conflict 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)

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

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 harmonized 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 the FIU Components (hereinafter facilities and programs) contained within FIU's HIPAA Hybrid Designation (FIU Policy and Procedure #1610.005), its Workforce members, students and Business Associates as defined in this policy and FIU Policy and Procedure #1660.015 regarding Business Associate Agreements.

REASON FOR POLICY

To ensure that FIU Workforce members understand the critical significance of complying with FIU's HIPAA Privacy and Security Rules Policies and Procedures and applicable federal rules and regulations and Florida state statutes, and to provide notice to FIU Workforce members and students that and violation of FIU's HIPAA Privacy and/or Security Rule policies and procedures and/or applicable federal rules and regulations and/or Florida states statutes may result in administrative and/or disciplinary action taken against Workforce members and students. Additionally, this policy and procedure explains the appropriate administrative and/or disciplinary action to be taken against FIU Workforce members who do not comply with the aforementioned rules, laws, regulations, policies and/or procedures.

DEFINITIONS

Please refer to the following link for a complete list of definitions pertaining to all HIPAA policies.

HIPAA Policies Definitions

ROLES AND RESPONSIBILITIES

Compliance Oversight: The Director of Compliance and Privacy for Health Affairs:

- 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.

- Performs audits and assessments of the facilities and programs 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.

HIPAA Facilities and Programs:

- Each FIU HIPAA Hybrid Designated Component (hereinafter facility and program) must designate a Privacy Coordinator responsible for overseeing and ensuring the facility's or program's implementation and compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable Florida state statutes governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to ensuring disciplinary action is properly taken against Workforce members.

Human Resources Division

- Imposes and documents disciplinary action taken against Workforce members found responsible for committing HIPAA Privacy and/or Security Rule violations, and/or associate FIU Policy and Procedure violations.

Student Affairs

- Imposes and documents disciplinary action taken against FIU students found responsible for committing HIPAA Privacy Rule and/or Security Rule violations and/or associated FIU Policy and Procedure violations.

RELATED RESOURCES

References

- 45 CFR §164.502
- 45 CFR §164.504
- 45 CFR §164.524
- 45 CFR §164.530
- Florida Statute §95.11

Related Policies

- FIU Policy # 1610.005 (Designated Health Care Components for FIU Community)
- 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 #1640.025 (Minimum Necessary)

- 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 #1660.050 (Patient Access to Protected Health Information)
- FIU Policy and Procedure #1660.065 (Complaints Under the HIPAA Privacy Rule, Mitigation, Refraining from Intimidating or Retaliatory Acts, and Waiver)
- FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in the Case of a Breach)

CONTACTS

For further information concerning this policy, please contact the Director of Compliance and Privacy for Health Affairs at (305) 348-0622 or hipaaprivacy@fiu.edu, or contact the appropriate Component Privacy Coordinator.

HISTORY

Initial Effective Date: August 1, 2009
Review Dates *(review performed, no updates)*: n/a
Revision Dates *(review performed, updates made to document)*: June 8, 2015; December 31, 2017; October 13, 2020; February 29, 2024; August 6, 2025.

Sanctions # 1660.085a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
August 1, 2009	August 6, 2025	Office of Compliance and Integrity

PROCEDURE STATEMENT

I. Administrative and Disciplinary Procedures

The Component (hereinafter facility and program) Privacy Coordinators are responsible for ensuring the facility's or program's compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable federal laws and Florida state statutes governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), and for ensuring that any administrative and/or disciplinary action taken against Workforce members found responsible for having committed a violation(s) and/or a breach(es) is properly administered, documented, and reported to the Director or Compliance and Privacy for Health Affairs with the Office of Compliance and Integrity and the HIPAA Security Officer with the Information Technology Division. (FIU Policy and Procedure #1660.070). (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)

Each facility or program must designate a HIPAA Security Coordinator responsible for ensuring compliance with the HIPAA Security Rule, FIU's associated HIPAA Security Policies and Procedures, and any associated or applicable federal laws and Florida state statutes governing the administrative, physical and technical safeguards of PHI and ePHI, and for ensuring that any administrative and/or disciplinary action taken against Workforce members found responsible for having committed a violation(s) and/or a breach(es) is properly administered, documented, and reported to the Director or Compliance and Privacy for Health Affairs with the Office of Compliance and Integrity and the HIPAA Security Officer with the Information Technology Division. (FIU Policy and Procedure #1660.070). (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)

FIU has an Incident Response Plan ("IRP") designed to address the collective requirements and obligations associated with data compromises for all activities at FIU. This policy and procedure supplements FIU's IRP by providing procedures required pursuant to the Health Insurance Portability and Accountability Act (HIPAA), federal law, and Florida state statutes.

The appropriate Incident Response Team (IRT) shall be assembled, as necessary and appropriate, and a Designated Investigator(s) will be selected in a manner consistent with the IRP (FIU Policy and Procedure #1930.021) (Incident Response Plan) and FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in the Case of a Breach)

A. Following competition of an investigation into an alleged HIPAA violation and/or breach, the Designated Investigator(s), in consultation with the IRT, (if assembled) will prepare a properly redacted or de-identified (hereinafter redacted) hardcopy of the Investigative Report. (FIU Policy and Procedure #1660.095) (Reporting of HIPAA Incidents and Notification in the Case of a Breach)

B. The Designated Investigator(s) will document in the Investigative File:
   1. The date, name and title of the Designated Investigator(s),
   2. The name(s) of the IRT who reviewed and approved the redacted portions of the hardcopy Investigative Report (if assembled), and
   3. The name(s) and title(s) of the Workforce member(s) the IRT approved to receive a copy of the redacted Investigative Report (if assembled).

C. The Designated Investigator(s) will:
   1. Deliver a hardcopy of the redacted Investigative Report to Workforce members as approved by the IRT (if assembled),
   2. Document in the Investigative File the:
      a. Name(s) and title(s) of the Designated Investigator(s) who delivered the redacted Investigative Report(s),
      b. The date(s), name(s) and title(s) of the Workforce member(s) who received a copy of the redacted Investigative Report as approved by the IRT (if assembled).
      c. Properly secure a copy of the redacted Investigative Report in the Investigative File.

D. If the investigative findings support that a Workforce member(s) committed a violation(s) and/or breach(es), the IRT (if assembled), in consultation with appropriate Workforce members from the impacted facility or program, and the Office of Human Resources will confer, identify and recommend sanctions against the Workforce member(s) (and/or student(s)) who committed the violation(s) or breach(es).

E. The Workforce member's Administrative Officer and the designee of the Office of Human Resources (or the designee of Academic Affairs if the violation(s) and/or breach(es) involved a student) will promptly schedule a meeting with the Workforce member(s) in a manner consistent with the Office of Human Resources Policy and Procedure (or Academic Affairs if a student was involved) and inform the Workforce member(s) (and student(s) if involved) of the level of violation, the sanction being imposed, and document the same within the Workforce members' personnel file in a manner consistent with the applicable Human Resources or Academic Affairs Policies and Procedures, if the violation(s) and/or breach(es) involved a student.

F. The facility or program Privacy or Security Coordinator will promptly provide a copy of the Office of Human Resources Personnel Action Form (or the Student Action

Form if the incident involves a student) to the Designated Investigator(s) identifying the agreed upon level of violation and the sanction imposed.

G. The Designated Investigator(s) will:
   1. Document in the Investigative File the level of violation and the sanction imposed,
   2. The date, name and title of the Workforce member who delivered the Personnel Action Form (or the Student Action Form, and
   3. Properly secure the Personnel Action Form (or the Student Action Form) within the Investigative Report file.

II. Administrative and Disciplinary Sanctions

A. The following list of offenses and corresponding sanctions is to be used, in consultation with appropriate staff within the HIPAA facility or program, the Office of Human Resources, the Office of General Counsel, the Office of Compliance and Integrity, the Division of Information Technology, and Academic Affairs as a guide in identifying the level of violation and appropriate corresponding sanction to be administered against Workforce members and students who violate HIPAA, Florida state statutes or federal rules and regulations, and/or associated FIU policies and procedures:

Class 1 Offenses	**Examples of "Unknowing" Offenses**
1.	Unknowingly using or disclosing patient information even though the workforce member (or student) attempted to prevent patient information from being use or disclosed
2.	Unintentionally corrupting ePHI/PHI
3.	Unintentionally exploiting ePHI/PHI

Class 2 Offenses	**Examples of "Reasonable Cause" Offenses**
1.	Second offense of any Class 1 violation (Does not have to be the same violation)

2.	Workforce member (or student) attempted to address the backlog of Client Privacy requests
3.	Talking about an individual's PHI in public areas within the workplace, such as elevators, reception areas, and the cafeteria
4.	Workforce members (or student) who handle PHI as a normal part of duties listen to voice mail messages on a speaker if the message may be overheard by others
5.	Not delivering incoming mail directly to the recipient or to a secure mailroom
6.	Not using standard voice mail greeting message advising the caller not to leave any PHI in their voice mail
Class 3 Offenses	**Examples of "Willful Neglect-Corrected" Offense (corrected within 30 days)**
1.	Third offense of any Class 1 offense (does not have to be the same offense)
2.	Second offense of any Class 2 offense (does not have to be the same offense)
3.	Obtaining PHI under false pretenses
4.	Using or disclosing PHI for personal gain or malicious harm
5.	Leaving your computer unattended while you are logged into a program containing PHI
6.	Accessing client information that you do not need to know to do your job
7.	Sharing your unique computer/network access credentials with other Workforce members
8.	Unauthorized use or disclosure of PHI
9.	Leaving PHI unattended
10.	Discussing PHI with an unauthorized person
11.	Intentionally corrupting ePHI
12.	Sharing passwords with others, posting or keeping passwords written down where they can be readily found by someone else (e.g., taped to desk, side of computer, or telephone)
13.	Posting documents containing PHI where it may be visible to others

14.	Saving electronic files containing PHI on an unencrypted shared drive or within an unencrypted client management system
15.	Not securing PHI used off-site when not in use, such as locking it in a cabinet
16.	Leaving PHI in an unattended vehicle

Class 4 Offenses	**Examples of "Willful Neglect-Uncorrected" Offense (not corrected within 30 days)**
1.	Third offense of any Class 1 offense
2.	Second offense of any Class 2 offense
3.	Obtaining PHI under false pretenses
4.	Using or disclosing PHI to public for personal gain or malicious harm
5.	Failure to cooperate with management, the Office of Compliance & Integrity, the IT Department, the Privacy Officer, Security Officer, Privacy Coordinator, or members of the Incident Response Team
6.	Not attempting to address a backlog of client requests
7.	Not alerting appropriate Workforce members of suspected or known HIPAA privacy or security violations or violations of associated FIU policies and procedures
8.	Not "Logging-Off" of a computer at the end of the workday
9.	Not taking steps to ensure faxes are kept confidential
10.	Not shredding paper documents containing PHI that do not have to be retained, prior to disposal, unless properly secured in a designated receptacle for shredding by a third-party
11.	Leaving PHI in an unattended vehicle
12.	Leaving PHI unattended
13.	Not reporting that Electronic Media containing PHI is lost or stolen

Class 1 Offenses	**Description of Sanctions**
1.	Verbal reprimand

2.	Written reprimand in Workforce member's personnel file (or student's ___ file)
3.	Retraining on HIPAA Privacy and Security Awareness
4.	Retraining on FIU's HIPAA Privacy and Security Policies and Procedures
5.	Retraining on the proper use of internal forms and HIPAA required forms

Class 2 Offenses	**Description of Sanctions**
1.	Written reprimand in Workforce member's personnel file (or student's ___ file)
2.	Retraining on FIU's HIPAA Privacy and Security Policies and Procedures
3.	Suspension of Workforce member (or student) without compensation (Minimum of one (1) day/maximum of thirty (30) days)
4.	Retraining on the proper use of internal forms and HIPAA required forms

Class 3 Offenses	**Description of Sanctions**
1.	Subject to termination of employment (or expulsion from school for students)
2.	Civil penalties as provided under HIPAA or other applicable Federal/State/Local law
3.	Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law

Class 4 Offenses	**Description of Sanctions**
1.	Subject to termination of employment (or expulsion from school for students)
2.	Civil penalties as provided under HIPAA or other applicable Federal/State/Local law
3.	Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law

Record Retention

The Office of Compliance and Integrity, and the Division of Information Technology must retain all documentation regarding the sanctions taken against Workforce members and students within the Investigative file for not less than seven (7) years from the creation date or the last effective date, whichever is later. A copy of any administrative or disciplinary action (sanctions) taken against Workforce members must be retained in the Workforce member's Human Resource's personnel file as required by federal rules and regulations and Florida state statutes and FIU Policy and Procedures, and in a student's record as required by HIPAA, federal law, Florida state statutes, and FIU Policy and Procedure #1660.080 (Policies and Procedures, Changes to Policies and Procedures, and Documentation).