FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Sanctions #1660.085

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
August 1, 2009	February 29, 2024	Office of Compliance and Integrity

POLICY STATEMENT

Florida International University (FIU) must take disciplinary action against Workforce members, Business Associates, and students 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 Health Care Component (Components) 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 policy and procedure, 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, state law or regulation, 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 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 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.

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 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)

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)

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 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 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 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 law and Florida state statutes, and to provide notice to FIU Workforce members that violations of FIU's HIPAA Privacy and/or Security Rule policies and procedures and/or applicable federal and state laws and regulations may result in administrative and/or disciplinary action taken against Workforce members who do not comply which may include, without limitation, termination of employment. 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	
TERM	**DEFINITIONS**
Access	Means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
Act	Means the Social Security Act
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	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 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.
Confidentiality	Means data or information is not made available or disclosed to unauthorized persons or processes.
Covered Entity/Program	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.
Designated Investigator(s)	Means a Workforce member(s) from the Office of Compliance and Integrity and/or the Information Technology (IT) Division, selected by the Office of Compliance and Integrity and the IT Division, in consultation with the designated members of the Incident Response Team, to conduct an investigations into suspected or known violations and/or suspected or known breaches.
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 Health Record	Means an electronic record of health-related information on a client that is created, gathered, managed and consulted by authorized health care clinicians and staff.
Electronic Media	Means: 1. Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such

	as magnetic tape or disk, optical disk, or digital memory card; 2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission. 3. Any electronic device that stores information including, but not limited to: cellular phones, PDAs (personal digital assistant), and tablets.
Electronic Protected Heath Information (ePHI)	PHI in electronic form. See also: PHI.
Encryption	For the sender of electronic protected health information, encryption converts the message in a file or document from a readable to an unreadable format. It means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Decryption is the reverse, allowing encrypted information to be converted from an unreadable format to a readable format by the recipient.
Facility	Means the physical premises and the interior and exterior of a building(s).
Florida Statutes	Also known as F.S. are the codified, statutory laws of Florida; it currently has 49 titles. A chapter in the Florida Statutes represents all relevant statutory laws on a particular subject.
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 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.
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.
Health Oversight Agency	Means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

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
Incidental Disclosure	Means a use or disclosure that occurs as a by-product of another permissible or required use or disclosure, as long as the covered entity or Component has applied reasonable safeguards and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure. An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Privacy Rule. However, an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule.
Individual	Means the person who is the subject of the PHI
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.
Law Enforcement Official	Means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to: 1. Investigate or conduct an official inquiry into a potential violation of law; or 2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
Patient	The person who is the subject of the PHI

Person	Means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.
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.
Public Health Authority	Means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of

	authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.
Reasonable Cause	Means a Workforce Member knew, or by exercising reasonable diligence would have known, that their act or omission might be a violation and he/she took reasonable steps to comply with HIPAA but was unable to do so despite exercising ordinary business care. The potential federal penalties against FIU are $1,000 - $50,000 per violation. The minimum federal penalties are $100,000 for violations of an identical provision in the same calendar year.
Record	Means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or on behalf of a Covered Program.
Sanction	Means the administrative/corrective action taken against FIU Workforce members who fail to comply with HIPAA and/or associated FIU policies and procedures that result in a HIPAA and/or associated FIU policies and procedures privacy or security violation as defined by federal or state regulations and/or FIU policy or procedure.
Security Incident	Means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
Standards	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.
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.
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.
State refers to one of the following:	1. For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan. 2. For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.
Technical Safeguards	Means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
Treatment, payment, and healthcare operations	Also known as 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.
Unknowing	Means a Workforce Member did not know and reasonably should not have known of the violation. (The potential federal penalties against FIU are $100 - $50,000 per violation. The minimum federal penalties are $25,000 for violations of an identical provision in the same calendar year).
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.
User	Means a person or entity with authorized access.
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.
Willful Neglect-Corrected	Means the violation was the result of conscious, intentional failure or reckless indifference to fulfill an obligation and the violation was corrected within 30 days of discovery. (The potential federal penalties to FIU are $10,000 - $50,000 per violation. The minimum federal penalties are $250,000 for violations of an identical provision in the same calendar year).
Willful Neglect-Uncorrected	Means the violation was the result of willful neglect, but corrective action was not taken within 30 days of the time when the Workforce member became aware of the problem or should

	have been aware of it. (The potential federal penalties to FIU $50,000 per violation. The minimum federal penalties are $1,500,000 for violations of an identical provision in the same calendar year).

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.
    - Creates and maintains in coordination with the Office of General Counsel and the HIPAA Hybrid Designated Component Privacy Coordinators 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 ensuring disciplinary action is properly taken against Workforce members.

3. **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.

4. **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 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: 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.

Sanctions # 1660.085a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
August 1, 2009	February 29, 2024	Office of Compliance and Integrity

PROCEDURE STATEMENT

I. Administrative and Disciplinary Procedures

Each FIU HIPAA Hybrid Designated Component (Component) must designate a HIPAA Privacy Coordinator responsible for ensuring the Component'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 Component 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 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, 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, 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.

C. The Designated Investigator(s) will:
   1. Deliver a hardcopy of the redacted Investigative Report to Workforce members as approved by the IRT,
   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.
      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, in consultation with appropriate Workforce members from the impacted Component, 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 Component's 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 by the IRT, in consultation with appropriate staff within the HIPAA Component, 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, State or federal law, 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 and state law 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).