FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Reporting of HIPAA Incidents and Notification in the Case of a Breach #1660.095

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

POLICY STATEMENT

All Florida International University (FIU) Workforce members shall immediately report any and all suspected or known:

- Violations of the Health Insurance Portability and Accountability Act (HIPAA),
- Violations of FIU's associated HIPAA Policies and/or Procedures,
- Violations of any federal law and/or Florida state statutes governing the confidentiality, integrity, or availability of Protected Health information (PHI) (hereinafter "violations")
- Breach(es) of PHI or electronic PHI (ePHI) related to FIU's HIPAA Hybrid Designated Health Care Components (Components) as defined in FIU Policy #1610.005.

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)

Component 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)

A breach of privacy investigation shall commence pursuant to FIU's Incident Response Plan ("IRP") as described in FIU Policy #1930.021.

The HIPAA Privacy and Security Coordinators, in coordination with the Office of Compliance & Integrity, the Division of Information Technology, and the Office of General Counsel shall mitigate, to the extent practicable, any harmful effects of privacy or security violations and breaches. (FIU Policy and Procedure #1660.065) (Complaints Under the HIPAA Privacy Rule, Mitigations, Refraining from Intimidating or Retaliatory Acts, and Waiver)

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 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 describe the requirements and provide guidelines related to the investigative process of determining if a HIPAA Rule, federal law, and/or Florida state statute, and/or associated FIU Policies and/or procedures, and/or a breach occurred, and the notification process requirements described in the Administrative Safeguards of the HIPAA Privacy and Security Rule Standards.

DEFINITIONS

TERM	DEFINITIONS
Access	Means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
Administrative Officer	Means the Component Workforce member responsible for financial management, human resources administration, management of facilities and equipment, and other administrative functions required to support the teaching and research missions of the FIU HIPAA Hybrid Designated Health Care Component. The Administrative Officer is the senior administrative staff position in the department, Division or Office and provides continuity as academic leadership changes.

Administrative Safeguards	Are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
Availability	Means the property that data or information is accessible and useable upon demand by an authorized person.
Breach	Means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted which compromises the privacy or security of the PHI.
Breach of Security (or Breach) **(See Florida Information Protection Act (FIPA/ACT))**	Means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.
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 department, division, office, unit or combination of departments, divisions, offices, or units of a hybrid covered entity designated by the hybrid covered entity. Those programs designated by FIU as Components must comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and state law and regulation regarding the privacy and security of Protected Health Information (PHI) and electronic PHI (ePHI). Components of FIU are required to comply with the Administrative Simplification provisions of HIPAA because the Components perform a covered function.
Confidentiality	Means data or information is not made available or disclosed to unauthorized persons or processes.
Covered Entity	An entity that is subject to HIPAA. 1. a health plan; 2. a health care clearinghouse; and/or 3. a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
Covered Entity (See Florida Information Protection Act (FIPA/Act))	Means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. For purposes of the notice requirements, the term includes a governmental entity.
Department (See Florida Information Protection Act (FIPA/Act))	Means the Florida Department of Legal Affairs
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.
Designated Record Set	1. A group of records maintained by or for a covered entity that is: a. The medical records and billing records about patients maintained by or for a covered health care provider; b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or c. Used, in whole or in part, by or for the covered entity to make decisions about patients. 2. For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
Disclosure	Means the release, transfer, provision of access to, or divulging in any other manner of protected health information outside of the entity holding the information.
Electronic Protected Heath Information (ePHI)	PHI in electronic form. See also: PHI.
Florida Information Protection Act (FIPA/Act)	Florida Statute Section 501.171, "Security of Confidential Personal Information", also known as FIPA was passed in 2014 to better protect Floridians' personal information by ensuring that businesses and government entities take reasonable measures to protect personal information and report data breaches to affected consumers.
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.
Government Entity (See Florida Information Protection Act (FIPA/Act))	Means any department, division, bureau, commission, regional planning agency, board, district, authority, agency, or other instrumentality of this state that acquires, maintains, stores, or uses data in electronic form containing personal information.
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 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 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.
HIPAA	Means the Health Insurance Portability and Accountability Act of 1996.
HIPAA Security Coordinator/Administrator	The FIU Workforce member designated by each Component to assist in the implementation and maintenance of systems and processes for the creation, maintenance and transmission of protected health information via electronic means and to work in collaboration with the HIPAA Security Officer, HIPAA Privacy Officer and other designated University representatives to ensure that the University creates and maintains an information technology environment that is compliant with applicable federal and state law governing health information privacy and confidentiality.
HIPAA Security Officer	The FIU Workforce member designated by the University to assist in the implementation of the HIPAA Security Standards, 45 C.F.R. Parts 160, 162 and 164 and to oversee and monitor the University's compliance with the required technical, administrative and physical safeguards as these relate to protected health information created, maintained or transmitted via electronic means. The University Information Technology Security Officer is designated as the HIPAA Security Officer.
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.
Integrity	Means the property that data or information have not been altered or destroyed in an unauthorized manner.
Patient	The person who is the subject of the PHI.
Person	Means a natural person, trust, estate, partnership, corporation, professional association or corporation, or other entity, public or private.
Personal Information	1. Means either the following:

(See Florida Information Protection Act (FIPA/Act))	a. An individual's first name or first initial and last name in combination with any of the following data elements for the individual: 1. A social security number; 2. A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; 3. A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; 4. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or 5. An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. b. A user-name or e-mail address, in combination with a password or security question and answer that would permit access to an online account. 2. The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.
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.
Reasonable Diligence	Means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.
Responsible Party	As defined in the Incident Response Plan and this policy and procedure means a designee, Workforce member, individual, or Business Associate who reported a suspected or known violation or breach of PHI/ePHI as identified in the above policy statement.
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.
Security incidents	Means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
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 With respect to the privacy of protected health information.
System	Means any electronic computing or communications device or the applications running thereon which can create, access, transmit or receive data. Systems are typically connected to digital networks. Examples of Systems include: 1. A computer system whether or not connected to a data network, 2. A database application used by a client or a set of clients, 3. A computer system used to connect over a network to another computer system, 4. An analog or digital voice mail system, 5. Data network segments including wireless data networks, and 6. Portable digital assistants.
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	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.
Unsecured PHI	Means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(2) of Public Law 111-5.
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 Security Officer/Division of Information Technology**
    - Evaluates all federal and state healthcare security laws, regulations, rules and ordinances (Rules) to ensure compliance with the Rules.
    - Creates and maintains in coordination with the Office of Compliance and Integrity, the Office of General Counsel, and the HIPAA Hybrid Designated Component Security Coordinators all required University-wide Security Rule policies and procedure.
    - Partners with the Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity, to ensure compliance with all federal and state healthcare privacy and security laws, regulations rules, and ordinances.

3. **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 federal laws and Florida state statutes governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to the receipt and processing of HIPAA incidents and notification in the case of a breach.

4. **Incident Response Team:**
    - Oversees investigations of alleged HIPAA Privacy and/or Security Rule violations.

RELATED RESOURCES

References

- 45 CFR §164.308
- 45 CFR §164.400-414
- 45 CFR §164.504
- 45 CFR §164.512
- 45 CFR §164.514
- 45 CFR §164.530
- Florida Statute §501.171
- Florida Statute §456.057
- Florida Statute §95.11

Related Policies

- 1930.021 FIU Incident Response Plan
- FIU Policy # 1610.005 (Designated Health Care Components of FIU Community)
- FIU Policy and Procedure #1660.015 (Business Associate Agreements)
- FIU Policy and Procedure #1660.070 (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)
- FIU Policy and Procedure #16460.075 (HIPAA Privacy and Security Rule Training)
- FIU Policy and Procedure #1660.080 (Policies and Procedures, Changes to Policies and Procedures, and Documentation)
- FIU Policy and Procedure #1660.085 (Sanctions)

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: July 27, 2001
Review Dates *(review performed, no updates)*: n/a
Revision Dates *(review performed, updates made to document)*: July 27, 2021; February 29, 2024.

FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

Reporting of HIPAA Incidents and Notification in the Case of a Breach #1660.095a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
July 27, 2021	February 29, 2024	Office of Compliance and Integrity

PROCEDURE STATEMENT

I. Reporting and Investigative Procedures

Each FIU HIPAA Hybrid Designated Component (Component) must designate a HIPAA 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 associated or applicable federal laws and Florida state statutes governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), and to receive and forward to the Director of Compliance and Privacy for Health Affairs with the Office of Compliance and Integrity, all suspected or known violations and Breaches. (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 overseeing and ensuring the Component's implementation and 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 to receive and forward to the HIPAA Security Office with the Division of Information Technology (IT), all suspected or known violations and Breaches.

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 Federal HIPAA Rules and state law. The appropriate Incident Response Team (IRT), as determined by, and including the Office of Compliance & Integrity, and the Division of IT, and the Office of General Counsel, shall be organized to address reported suspected or known violations and Breaches and shall follow the provisions of this policy and procedure for incidents involving PHI/ePHI.

A. Workforce members must immediately report any and all suspected or known violations of the HIPAA Rule(s), FIU associated policies and/or procedures, associated or applicable Florida state and/or federal law(s) and/or regulation(s) (violations) and suspected or known Breach to any of the following:
   1. The Chief Compliance and Privacy Officer, Office of Compliance and Integrity,

2. The Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity,
3. The Chief Information Officer, Division of Information Technology,
4. The HIPAA Security Officer, Division of IT,
5. The Office of General Counsel, and/or
6. His or her department, division, or unit director, manager, supervisor, or designated HIPAA Privacy or Security Coordinator.

A. Directors, managers, supervisors, and HIPAA Privacy or Security Coordinators within each Component who are informed of, become aware of, or observer a suspected or known violation or Breach must immediately notify:
   1. The Director of Compliance and Privacy for Health Affairs with the Office of Compliance and Integrity, and/or
   2. The HIPAA Security Office with the Division of IT of the suspected or known violation or Breach.

B. Reports of a suspected or known violation or Breach may be made orally, via written report, email communication, or through the FIU "Ethical Panther line" at http:www.convercent.com/report/ or by calling (844) 312-3558.

   NOTE: Email communications shall not contain patient identifying PHI in the body of the email or by attachment.

   NOTE: Reports involving electronic media such as laptops, phones or thumb drives containing electronic PHI ("ePHI") shall be immediately reported to FIU's Information Security Officer with the Division of IT.

C. The Office of Compliance and Integrity, the Division of IT, and the Office of General Counsel will promptly notify each other upon receipt of a report of a suspected or known violation or Breach and assemble the appropriate IRT members of the allegation(s).

D. The Office of Compliance and Integrity, the Division of IT, the Office of General Counsel, and the designated IRT members will review the allegations and determine the scope of the investigation. The Office of Compliance and Integrity and the Division of IT are responsible conducting all investigations and will work with the IRT to identify and agree upon a Workforce member(s) from the Office of Compliance and Integrity and the Division of IT to lead the investigation (hereinafter known as the Designated Investigator(s)).

E. The assembled IRT, through the Office of General Counsel, will notify the contracted Cyber Security Insurance Carrier (Carrier) of any suspected or known violations or Breach(es), if required per the terms of the Carrier contract/agreement.

F. If after notice is provided, the Carrier elects to direct or conduct the investigation, the IRT, the Office of Compliance and Integrity, the Division of IT, and the Office of General Counsel will defer to and support the Carrier during the course of their investigation, as necessary and appropriate.

G. If the suspected or known violation(s), and/or Breach(es) does not require or involve the Carrier's participation, the investigation will be spearheaded by the Designated Investigator(s) who will:
   1. Establish an Investigative File, case number, and Intake Log,
   2. Document and properly secure in the Investigative File any and all communications and documentation received or created regarding the allegations and formation of the IRT,
   3. Request the FIU Workforce member(s) and/or other individual(s) (hereinafter Responsible Party(ies)) submit their allegation(s) in writing,
   4. Document in the Investigative File the date, time and method used to make the request,
   5. Properly secure in the Investigative File any and all written communications sent to the Responsible Party(ies).

H. If the Responsible Party(ies) submits his/her allegation(s) in writing, the Designated Investigator(s) will:
   1. Document in the Investigative File receipt of the written allegation(s), and
   2. Properly secure in the Investigative file the written allegation(s).

I. If the Responsible Party(ies) refuse to submit his/her allegation(s) in writing, or if additional information is required, the Designated Investigator(s) will:
   1. Request an interview with the Responsible Party(ies) via their preferred method (e.g., in-person, phone, etc.).
   2. Document in the Investigative File the date, time, and method used to make the request, and
   3. Properly secure in the Investigative File any written communications sent to and/or received from the Responsible Party(ies).

   NOTE: The Designated Investigator(s) will not use email communications to conduct interviews, unless PHI will not be exchanged during the course of the interview.

J. If the Responsible Party(ies) agree to participate in the investigative interview, the Designated Investigator(s) will request information regarding the alleged violation(s) and/or Breach(es), including, but not limited to:
   1. The name(s) of the Workforce member(s) involved in or responsible for the alleged violation(s) and/or Breach(es),
   2. The nature of the alleged violation(s) and/or Breach(es),
   3. Identification of the patient's/client(s) who may have been adversely impacted by the alleged violation(s) and/or Breach(es), if known,

4. The date(s) of the alleged violation(s) and/or Breach(es), and
5. Any other relevant information as determined by the Designated Investigator(s).

K. Following the investigative interview, the Designated Investigator(s) will:
   1. Prepare an investigative interview statement and provide it to the Responsible Party(ies) for review and signature,
   2. Record in the Investigative File:
      a. The date of receipt of the allegation(s), the written allegation(s) and/or the investigative interview statement(s) on the Intake Log of the Investigative File.

L. Upon receipt of a written allegation(s) and/or competition of the investigative interview statement(s), the Designated Investigator(s) will initiate a formal investigation. The Designated Investigator(s) will include any additional Workforce member(s) in the investigative process, as necessary and appropriate, and document their participation on the Intake Log of the Investigative File.

M. Following receipt of a written allegation(s) and/or competition of the investigative interview statement(s), the Designated Investigator(s) will promptly draft a "Notice of Complaint" (Notice) which will be addressed to the affected HIPAA Component(s) senior official(s) and copied to Workforce members and Business Associates as the IRT determine necessary and appropriate. The Notice must identify that the IRT, Office of Compliance and Integrity, and Division of IT are in receipt of a complaint alleging a violation(s) or Breach(es), the basis of the allegation(s), and that a formal HIPAA investigation is being undertaken.

NOTE: ***Law Enforcement Delay***

If a law enforcement official states that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Designated Investigator(s) shall:

1. *Delay such notification, notice, or posting for the time period specified by the official, If the statement is in writing and specifies the time for which a delay is required; (See "#1" immediately below) or*
2. *Delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, if the statement is made orally, unless a written statement as identified in paragraph 1 immediately above of this section is submitted during that time. (See immediately below)*

If the Law Enforcement official provides a written statement, the Designated Investigator(s) must:

1. *Verify the identity and authority of the Law Enforcement Official (FIU Policy and Procedure #1660.040) (Verification);*
2. *Document in the Investigative File the method utilized to verify the identity and authority of the Law Enforcement Official;*

3. *Verify that the document is on official letterhead or other legal document (FIU Policy and Procedure #1660.040) (Verification);*
4. *Document in the Investigative File the method utilized to verify the official letterhead or other legal document (FIU Policy and Procedure #1660.040) (Verification);*
5. *Document in the Investigative File, the period of the temporary suspension;*
6. *Properly secure the written statement in the Investigative File;*
7. *Notify necessary and appropriate Workforce members of the temporary suspension;*
8. *Document the notification in the Investigative File, and*
9. *Document the date and the name and title of the Designated Investigator(s) who completed the verification and notification process.*

If the Law Enforcement official's statement is made orally, the Designated Investigator(s) must:

1. *Verify the identify and authority of the Law Enforcement official (FIU Policy and Procedure #1660.040) (Verification);*
2. *Document in the Investigative File the method utilized to verify the identify and authority of the Law Enforcement official;*
3. *Document in the Investigative File the oral statement;*
4. *Document in the Investigative File the period of the temporary suspension;*
5. *Limit the temporary suspension to no longer than 30-days from the date of the oral statement; unless a written statement is submitted during that time;*
6. *Notify necessary and appropriate Workforce members of the temporary suspension;*
7. *Document the notification in the Investigative File, and*
8. *Document the date and the name and title of the Designated Investigator(s) who completed the verification and notification process.*

NOTE: *This exception applies only during the period of law enforcement delay.*

N. Once the Notice is approved, it must be delivered to the recipients approved by the IRT, in a confidential manner via email attachment and via hardcopy in a sealed envelope containing the word "Confidential" on the exterior of the envelope. The sealed envelope containing the Notice may be hand-delivered, or the sealed envelope containing the Notice must be placed inside of an interoffice envelope and delivered through the FIU interoffice mail system.

O. The Designated Investigator(s) shall:
   1. Record in the Investigative File:
      a. The date the Notice was delivered,
      b. The names and titles of the approved recipient(s) to whom the Notice was sent, and
      c. The name and title of the Designated Investigator(s) who delivered the Notice.
   2. Properly secure a copy of the email communication(s) containing the attached Notice within the Investigative File.
   3. Properly secure a copy of the hardcopy Notice within the Investigative File.

NOTE: The Designated Investigator(s) should use as necessary and appropriate the "Sample Breach Risk Assessment Tool" to assist with the investigative process and breach assessment. (See Sample Breach Risk Assessment Tool" attached)

P. If necessary, the Designated Investigator(s) shall request from the Privacy and/or Security Coordinator of the HIPAA Component where the alleged violation(s) or Breach(es) occurred, all relevant policies, procedures, training transcripts, and any other documentation, as deemed necessary and appropriate.

Q. The Designated Investigator(s) shall:
1. Record within the Investigative File:
    a. The day and manner (i.e. email, hardcopy written request) the request for documentation was made,
2. The name(s) and title(s) of the Privacy and/or Security Coordinator(s) to whom the request was made, and
3. The name(s) of the Designated Investigator(s) who made the request(s).
4. Print and properly secure a copy of the email communication(s) and/or hardcopy written request(s) within the Investigative File.

R. Upon receipt of the requested documentation, the Designated Investigator(s) shall:
1. Record in the Investigative file:
    a. The date the requested documentation was received,
    b. The name and tile of the Designated Investigator(s) member who delivered the documentation, and
    c. The means of delivery (e.g., email communication or hardcopy).
2. Properly secure the requested documentation within the Investigative File.
3. Print and properly secure any email communications received within the Investigative File.

S. If necessary and appropriate, the Designated Investigator(s) shall:
1. Schedule and conduct investigative interviews with:
    1. The Workforce member(s) who allegedly committed or were involved in the violation(s) or Breach(es), and
    2. The Workforce member(s) and any other individual(s) and Business Associate(s) who may possess relevant information regarding the alleged violation(s) and/or Breaches(es)
2. Record in the Investigative File:
    1. The date and method (i.e., email, phone, hardcopy written request) the investigative interviews were requested and conducted,
    2. The name and title of the Workforce member(s), individual(s), and Business Associate(s) who participate in an investigative interview, and
    3. The name and title of the Designated Investigator(s) who scheduled and conducted the investigative interviews.
3. Properly secure copies of any email communications and/or hardcopy written

investigative interview communications requests in the Investigative File.

T. The Designated Investigator(s) shall promptly:
   1. Prepare a typed written investigative interview statement for each Workforce member, individual, and Business Associate who participated in an investigative interview by documenting their relevant statements and responses made during the investigative interview,
   2. Provide each Workforce member, individual, and Business Associate an opportunity to review, edit, and/or add to their investigative interview statement,
   3. Request each Workforce member, individual, and Business Associate sign and date their investigative interview statement,
   4. Document the name, title and date the Designated Investigator(s) who met with each Workforce member, individual, and Business Associate, and
   5. Properly secure the signed and dated investigative interview statement(s) in the Investigative File.

U. The Designated Investigator(s) shall request additional documentation and conduct follow-up interviews, as necessary and appropriate.

   NOTE: All electronic and hardcopy documentation received and/or created during the course of the investigation, including, but not limited to the Sample Breach Risk Assessment Tool, must be saved in a manner consistent with the requirements of the HIPAA Security Rule, FIU Policy and Procedure, and as approved by the HIPAA Security Officer.

V. The Designated Investigator(s) shall prepare a DRAFT HIPAA Investigative Report (Report) and submit it to the IRT for review, comment, and approval.

W. The Designated Investigator(s) and IRT, or Business Associate, if applicable, shall presume that an impermissible acquisition, use, or disclosure of PHI/ePHI is a Breach, unless the Designated Investigator(s) and IRT, or Business Associate, if applicable, can demonstrate that there is a low probability that the PHI/ePHI has been compromised. The Designated Investigator(s) and IRT, or Business Associate, if applicable, shall review all relevant data to conduct a risk assessment, which shall include an analysis of at least the following:
   1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   2. The unauthorized individual who used PHI or to whom the disclosure was made;
   3. Whether the PHI was actually acquired or viewed, and
   4. The extent to which the risk to the PHI has been mitigated.

X. If such review confirms that an impermissible action occurred, the Designated Investigator(s) and IRT, or Business Associate, it applicable, shall determine whether the reported violation meets any of the following exceptions:

1. An unintentional acquisition, access, or use of FIU PHI/ePHI by a Workforce member or an individual who is acting under the authority of FIU or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of his/her authority, provided that action does not and cannot result in further use or disclosure of the PHI/ePHI in a manner not permitted by the Privacy Rule;
2. An inadvertent disclosure of FIU PHI/ePHI by a Workforce member or Business Associate to another Workforce member or Business Associate authorized to access FIU PHI/ePHI, provided that such action does not and cannot result in further use or disclosure of the PHI/ePHI in a manner not permitted by the Privacy Rule; and/or
3. A disclosure of FIU PHI/ePHI to an unauthorized individual, and FIU has a good faith belief that the unauthorized individual would not have been able to retain the information.

Y. If none of the exceptions are deemed to have been met, then the event shall be deemed a Breach and the Designated Investigator(s) and the IRT, or Business Associate, if applicable, will proceed with the notification process pursuant to federal and state law.

NOTE: A breach under the Florida Information Protection Act (FIPA/Act) does not require the same analysis as HIPAA or the same degree of unauthorized disclosure/access. A FIPA/Act breach occurs when unauthorized access/disclosure of data in electronic form containing personal information occurs. FIPA/Act requires only that the individual's first name or first initial and last name in combination with one or more specifically listed data elements is disclosed or accessed without authorization. The combined data element can be "any information regarding the individual's medical history, mental or physical condition, medical treatment or diagnosis by a health care professional, a health insurance or subscriber identification number, and any unique identifier used by a health insurer to identify the individual."

Z. The Designated Investigator(s), IRT, and Business Associates shall treat a Breach as discovered as of the first day on which the Breach is known by a person exercising reasonable diligence (other than the person committing the Breach), who is a Workforce member or agent of FIU or the Business Associate.

NOTE: See Law Enforcement Delay and Verification requirements in "M" above.

NOTE: See Documenting requirements in "M" above

AA. The Designated Investigator(s) shall prepare a DRAFT HIPAA Investigative Report (Report) and submit it to the IRT for review, comment, and approval.

BB. If the Designated Investigator(s) receive comments or recommended edits or modifications to the Report, the Designated Investigator(s) will revise the Report as

appropriate and resubmit a FINAL Report for signature by the Director of Compliance and Privacy for Health Affairs, the HIPAA Security Officer, or designee as approved by the IRT.

CC. Upon receipt of the signed FINAL Report, the Designated Investigator(s) will forward a copy to the affected HIPAA Component(s) Administrative Officer(s) and any additional FIU Workforce member(s) as approved by the IRT, Office of General Counsel, the Office of Compliance and Integrity, and the Division of IT.

DD. The Designated Investigator(s) will document in the Investigative File:

1. The date(s), names, titles of IRT members involved in the review and approval process;
2. The steps taken to obtain approval of the Report, and
3. The date, name and title of all Workforce members provided a copy of the FINAL Report.

NOTE: The FINAL Report must be delivered in hardcopy form and not via email attachment, unless properly encrypted as required by the HIPAA Security Officer and FIU HIPAA Security policy and procedure.

EE. The Designated Investigator(s) shall properly secure a copy of the FINAL Report within the Investigative File.

FF. Workforce members of the Division of IT, Office of Compliance and Integrity, and the Office of General Counsel shall work together with Workforce members of the HIPAA Component where the incident occurred to mitigate, to the extent possible, any harmful effect resulting from the impermissible use, disclosure, or safeguarding of PHI in accordance with the HIPAA Privacy and/or Security Rules and/or associated FIU HIPAA Policies and Procedures. (FIU Policy and Procedure #1660.065) (Complaints under the HIPAA Privacy Rule, Mitigations, Refraining from Intimidating or Retaliatory Acts, and Waiver)

GG. The Designated Investigator(s) will document in the Investigative File all actions taken to mitigate any harmful effects occurring as resulting of the incident, the results of those efforts, and provide the IRT with written recommendations for improvement or proactive steps that may be taken to limit or prevent the same or similar incidents from occurring in the future.

HH. The Division of IT, the Office of Compliance and Integrity, the Office of General Counsel, and the Component where the incident occurred will implement recommendations as approved by the IRT.

II. Workforce members shall not intimidate or retaliate against individuals or groups that may exercise their privacy rights as described in the HIPAA Privacy Rule, associated

FIU HIPAA Policy and Procedure, Florida state statutes, or federal law. (FIU Policy and Procedure #1660.065) (Complaints under the HIPAA Privacy Rule, Mitigations, Refraining from Intimidating or Retaliatory Acts, and Waiver)

II. Notification:

NOTE: The Cyber Security Insurance Carrier (Carrier) with whom FIU has a contract, may be responsible for all notification requirements involving a Breach. Accordingly, in situations in which the Carrier is responsible, the IRT, the Responsible Party, the Office of Compliance and Integrity, and the Division of IT will defer to Office of General Counsel and the Carrier.

A. When a reported incident is confirmed to be a Breach of unsecured PHI/ePHI and FIU is responsible for providing a required notice, the Designated Investigator(s), in consultation with the Office of General Counsel, the Office of Compliance and Integrity, and the Division of IT must adhere to the notification process without unreasonable delay, and in no case later than 60 days after the date of discovery of the Breach, with the follow key elements described immediately below in III(A). The Designated Investigator(s) must submit any proposed notifications to the Office of General Counsel, the Office of Compliance and Integrity, and the Division of IT for approval prior to delivering the notification to any individual or regulatory agency.

III. The Notification Shall be in Writing.

A. Notification sent to patients will include at a minimum, to the extent possible, a brief description of the Breach, a description of the types of information involved in the Breach, the steps affected patients should take to protect themselves from potential harm, a brief description of what FIU is doing to investigate the Breach, mitigate the harm, and prevent further recurrence of such events in the future, as well as contact information for patients to ask questions or learn additional information about the Breach. The contact information should include a toll-free telephone number, email address, website or physical address. The notifications must be mailed first-class mail, or electronically if such patient preference is documented (FIU Policy and Procedure #1600.005) (Right of Patients to Request Confidential Communications Regarding the Use and Disclosure of Their Protected Health Information), to the last known address of the patient (or to patient's representative, if known) (FIU Policy and Procedure #1660.001) (Representative). (See Sample Breach Notification to Patients Letter attached)

NOTE: The Florida Information Protection Act (FIPA/Act) requires that notice must be given to "each individual in this state whose personal information was, or the covered entity reasonable believes to have been, accessed as a result of the breach. Notice shall be made expeditiously as practicable and without unreasonable delay… but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized" by FIPA/Act.

B. Specific notification will be sent to the Secretary of the Department of Health and Human Services (HHS) in the manner prescribed by the HIPAA Rules. For Breaches of unsecured PHI involving 500 or more individuals, notification must be sent to the Secretary at the same time as notifying the individuals, and the media in (III)(A) and (III)(F).

C. For Breaches of unsecured PHI involving fewer than 500 individuals, notification must be provided to HHS no later than 60 days after the end of the calendar year in which the Breach occurred in a manner prescribed by HHS.

D. The Office of Compliance and Integrity will keep a log and report annually.

E. Notification must be sent to Florida's Department of Legal Affairs (for Breaches involving electronic information and affecting (500) or more patients within the state).

NOTE: The Florida Information Protection Act (FIPA/Act) requires that breaches (as defined by the FIPA/Act) be provided to Florida's Department of Legal Affairs of any breach of security affecting 500 or more individuals in the State of Florida. With limited exception, such notice must be provided as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred.

F. Notification for a Breach involving more than 500 residents of a particular jurisdiction, must be provided in a prominent media outlet serving that jurisdiction, the notification must occur without unreasonable delay and in no case later than 60 days after the discovery of the Breach, and the notification must meet the same requirements as identified above in III(A).

G. Notification via FIU's website must be provided when there is insufficient or out-of-date contact information that prevents direct notifications to (10) or more patients. This substitute notification must be posted conspicuously for (90) days on the website providing a toll-free telephone number, email address, website or physical address.

H. Additional notice by telephone may be provided to patients in urgent situations due to possible imminent misuse of unsecured PHI/ePHI.

I. If the Breach is at, or by a Business Associate, then the Business Associate will address notifications without unreasonable delay as described in the signed Business Associate Agreement and provisions described in this policy under Section III. (FIU Policy and Procedure #1660.015 (Business Associate Agreements). The Business Associate is required to maintain all documentation related to any and all events and subsequent actions for a minimum of seven (7) years from the time of discovery.

NOTE: See Law Enforcement Delay and Verification requirements above.

NOTE: See Documenting requirements above

J. Redacted copies of the FINAL Report will only be disclosed to additional department, division, and/or unit Workforce members with the prior written approval from the IRT, the Office of Compliance and Integrity, the Office of General Counsel, and the IT Division. The Office of Compliance and Integrity, the Office of General Counsel, and the IT Division will identify items within the FINAL Report that must be redacted, the limitations on who may view the FINAL Report, how the FINAL Report may be utilized, and how it must be safeguarded to prevent further disclosure.

IV. Sanctions:

A. In the event the investigative findings support a finding that a HIPAA Privacy and/or Security Rule violation occurred, but did not result in a Breach, appropriate sanctions must be taken against the Workforce member(s) and students who failed to comply with the HIPAA Regulations, and/or associated FIU policies and procedures. The level and type of sanctions applied must be consistent with the terms of the FIU Sanction Policy and Procedures and must be documented in the Investigative File. (FIU Policy and Procedure #1660.085 (Sanctions)

B. In the event the investigative findings support that Breach of unsecured PHI occurred, appropriate sanctions must be taken against the Workforce member(s) and students who failed to comply with the requirements of the HIPAA Regulations, and/or associated FIU policies and procedures. The level and type of sanctions applied must be consistent with the terms of the FIU Sanction Policy and Procedures and must be documented in the Investigative File. (FIU Policy and Procedure #1660.085) (Sanctions)

V. Cooperation with Investigators:

A. FIU's Healthcare Components and Business Associates shall cooperate with the Secretary of the HHS and the state of Florida, if the Secretary or the Florida Attorney General undertakes an investigation or compliance review of the policies, procedures, or practices of FIU and its Components to determine whether it is complying with the applicable administrative simplification provisions.

VI. Business Associates:

A. FIU Business Associates must notify FIU within not greater than seven (7) days after the discovery of any suspected or actual Breach of security, intrusion or unauthorized access, use or disclosure of unsecured PHI and/or any actual or suspected use or disclosure of PHI in violation of any applicable federal or state laws or regulations. The notice must include:

1. The identification of each patient whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during such Breach;
2. A brief description of what happened, including the date of the Breach and the date of Business Associate's discovery of the Breach;
3. A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
4. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach, and
5. A brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches.

B. The Business Associate must take prompt corrective actions to cure any such deficiencies and any action pertaining to such unauthorized disclosure required by applicable federal and state statutes and regulations. A Breach shall be treated as discovered by Business Associate as of the first day on which such Breach is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate. A Business Associate shall be deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person who is an employee, officer, or other agent of Business Associate, other than the person committing the Breach.

C. The Business Associate shall bear all costs and liabilities associated with required notifications resulting from a Breach (including but not limited to notifications to individuals, the Secretary of HHS and/or the state of Florida, and the media).

NOTE: See Law Enforcement Delay and Verification requirements above.

NOTE: See Documenting requirements above

D. In the event that the investigative findings support that Breach occurred as a result of the action or inaction of a Business Associate, the FIU Office of General Counsel, the affected HIPAA Component(s), the FIU Office of Compliance and Integrity, and the Division of IT, in consultation with any other FIU departments, divisions, units, as reasonable and appropriate, shall take action against the Business Associate as permitted by the HIPAA Regulations, the Business Associate Agreement, and/or FIU policy and procedure. Unless otherwise provided, cancellation of a contract shall be reserved to the FIU Office of General Counsel.

E. The Designated Investigator(s) must document in the Investigative File the actions taken against the Business Associate, if any.

F. As necessary and appropriate, and under the direction of and with the assistance of the Office of General Counsel, the Office of Compliance and Integrity, the Division of IT, Workforce members shall mitigate, to the extent possible, any harmful effect the Business Associate identified regarding PHI within their control that was not used, disclosed, or safeguarded in accordance with the HIPAA Privacy and/or Security Rules, and/or Business Associate Agreement, and for which FIU is able to assist. (FIU Policy and Procedure #1600.065) (Complaints under the HIPAA Privacy Rule, Mitigations, Refraining from Intimidating or Retaliatory Acts, Waiver)

G. Workforce members shall not intimidate or retaliate against individuals or groups that may exercise their privacy rights as described in the HIPAA Privacy Rule, state law and/or associated FIU HIPAA Policy and Procedure. (FIU Policy and Procedure #1660.065) (Complaints under the HIPAA Privacy Rule, Mitigations, Refraining from Intimidating or Retaliatory Acts, Waiver)

VII. Record/Documentation Retention

A. All policies, procedures, communications, actions, notification, activities and/or designations, including investigations and risk assessment(s), shall be maintained by the Office of Compliance & Integrity and/or the Division of IT in hardcopy and/or electronic form and retained for a period not less than seven (7) years from the date of its creation or the date when it was last in effect, whichever is later. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures and Documentation

VIII. Forms

- Sample Breach Notification to Patients Letter
- Sample Breach Risk Assessment Tool