FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Business Associate Agreements # 1660.015

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 1, 2009	July 27, 2021	Office of Compliance and Integrity

POLICY STATEMENT

All contracts or other written agreements between a Florida International University (FIU) Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Health Care Component (Component) and a contractor (Vendor), or the FIU Purchasing Services Department (Purchasing Department), Office of the Controller, and a contractor (Vendor), who by definition create, use, disclose, or access protected health information (PHI) as part of treatment, payment, and/or healthcare operations (TPO), must contain language-requiring adherence to the HIPAA Privacy and Security Rules (Business Associate Agreement) (BAA). A Vendor (Business Associate) who receives, transmits, maintains or creates PHI in an electronic format (ePHI) must sign a BAA agreeing to protect the confidentiality, integrity and availability of the electronic information.

When a HIPAA Component has a business associate relationship with an entity that is also a governmental entity, the requirements of the BAA may be met by:

1. Entering into a Memorandum of Understanding (MOU) with the governmental entity; or
2. Determining if current state or federal law requires that the governmental entity/Business Associate comply with regulations that meet the objectives of the Privacy Rule business associate standard.

Unless otherwise approved by the Office of General Counsel, HIPAA Components and the Purchasing Department must enter into an FIU approved BAA (or amendments) with Business Associates and obtain documented satisfactory assurance that the Business Associate will appropriately safeguard all FIU patient PHI created, used, disclosed, or accessed under the BAA. (See FIU BAA. Attachment D).

The Director of Compliance and Privacy for Health Affairs with the Office of Compliance and Integrity, the HIPAA Security Officer with the Information Technology Division, and the Office of General Counsel will provide the Purchasing Department and Components with guidance as to whether a BAA is necessary in those situations where the Purchasing Department or the Component have what appears to be a business associate relationship with a Vendor. The FIU Purchasing Department, and where necessary and appropriate, the HIPAA Component Privacy and/or Security Coordinator will document those determinations by posting a copy of the contract and BAA on the Purchasing Department "Total Contract Manager" system (TCM).

Components and the Purchasing Department 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 and the Purchasing Department 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)

FIU recognizes that a covered entity (i.e., a health plan, a health care clearinghouse, and a health care provider who transmits any health information in electronic form in connection with a transaction covered by the rule) may be a business Associate of another covered entity.

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. (FIU Policy and Procedure #1660.070) (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)

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

SCOPE

The policy applies to the FIU HIPAA Health Care Components that are contained within FIU's HIPAA Hybrid Designation (FIU Policy and Procedure #1610.005), the FIU Purchasing Department, Workforce members as defined in this policy and FIU Policy and Procedure #1610.005, and any FIU department, division, office, and/or unit that may enter into a contract(s) or other written agreement(s) which may require the Vendor to create, use, disclose, or access protected health information (PHI) associated with the FIU HIPAA Hybrid Designated Health Care Components.

REASON FOR POLICY

FIU seeks to ensure that Business Associates adhere to the protections imposed by the HIPAA Privacy and Security Rules, state laws and regulations, and that there is no degradation of privacy and security safeguards when PHI is shared with Business Associates.

To ensure that FIU Workforce members comply and understand the critical significance of complying with FIU's HIPAA Privacy and Security Rules Policies and Procedures and applicable state laws and regulations and to explain the administrative actions that Components must take in order allow a Business Associate to create, use, disclose, or access PHI/ePHI and establishes guidelines for Components and the Purchasing Department to comply with the HIPAA Privacy and Security Rules requirements relating to Business Associate relationships, including entering into Business Associate Agreements (and amendments).

- 45 CFR §164.504 (Use and Disclosures: Organizational Requirements)

DEFINITIONS	
TERM	**DEFINITIONS**
Access	Means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
Administrative Officer	Means the Component Workforce member responsible for financial management, human resources administration, management of facilities and equipment, and other administrative functions required to support the teaching and research missions of the FIU HIPAA Hybrid Designated Health Care Component. The Administrative Officer is the senior administrative staff position in the department, Division or Office and provides continuity as academic leadership changes.
Administrative Safeguards	Are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
Availability	Means the property that data or information is accessible and useable upon demand by an authorized person.
Business Associate	Generally an entity or person who performs a function involving the use or disclosure of Protected Health Information (PHI) on behalf of a covered entity (such as claims processing, case management, utilization review, quality assurance, billing) or provides services for a covered entity that require the disclosure of PHI (such as legal, actuarial, accounting, accreditation). **NOTE:** A business associate relationship exists when an individual or entity, acting on behalf of an FIU HIPAA Component(s), assists in the performance of a function or activity involving the creation, use, disclosure, or access of

	PHI. This includes, but not limited to, claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management or repricing. **NOTE:** A Business Associate may include any individual or entity that receives PHI from a HIPAA Component in the course of providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, software support, or financial services. A Business Associates does not, however, include HIPAA Component workforce members.
Business Associate Agreement	Means a contract or other written arrangement with a business associate which must describe the permitted and required uses of protected health information by the business associate; provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.
Breach	Means the unauthorized acquisition, access, use, or disclosure of Protected Health Information (PHI) that compromises the security or privacy of the data and poses a significant risk of financial, reputational, or other harm to the client.
Code of Federal Regulations	Also known as CFR
Component	Means a component or combination of components of a hybrid entity designated by the hybrid entity (Florida International University). Those programs designated by FIU that must comply with the requirements of the Health Insurance Portability and Accountability Act of 1996, hereinafter referred to as "Components". Components of FIU are required to comply with the Administrative Simplification provisions of HIPAA because the Components perform a covered function.
Confidentiality	Means data or information is not made available or disclosed to unauthorized persons or processes.
Covered Entity	An entity that is subject to HIPAA. 1. a health plan; 2. a health care clearinghouse; and/or 3. a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Disclosure	Means the release, transfer, provision of access to, or divulging in any other manner of protected health information outside of the entity holding the information.
Electronic Protected Heath Information (ePHI)	PHI in electronic form. See also: PHI.
Florida Statutes	Also known as F.S.
Health Care	Means the care, services, or supplies related to the health of a patient, including: 1. preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of a patient or that affects the structure or function of the body; and 2. sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
Health Care Component	See "Component"
Health Care Operations	Means any of the following activities: 1. quality assessment and improvement activities, including case management and care coordination; 2. competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; 3. conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; 4. specified insurance functions, such as underwriting, risk rating, and reinsuring risk; 5. business planning, development, management, and administration; and 6. business management and general administrative activities of the entity, including but not limited to: a. de-identifying protected health information, b. creating a limited data set, and c. certain fundraising for the benefit of the covered entity.
Health Care Provider	Means a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
U.S. Department of Health and Human Services	Also known as HHS.
Health Information	Means any information, whether oral or recorded in any form or medium, that is created or received by a health care provider,

	health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an patient; the provision of health care to an patient; or the past, present, or future payment for the provision of health care to an patient.
HIPAA	Means the Health Insurance Portability and Accountability Act of 1996.
Hybrid Covered Entity	Means a single legal entity that performs both covered and non-covered functions. The entity has a defined health care component that engages in HIPAA electronic transactions.
Individually Identifiable Health Information	Means information that is a subset of health information, including demographic information collected from an individual, and 1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and 2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and a. That identifies the individual; or b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Integrity	Means the property that data or information have not been altered or destroyed in an unauthorized manner.
Memorandum of Understanding (MOU)	When a covered entity (or one or more of its components) and its business associate are both government entities, the covered entity may enter into a memorandum of understanding (MOU) with the business associate and the MOU contains terms which accomplish the objectives of the Business Associate Contracts section of the Privacy and Security Rule.
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.
Subcontractor	Means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
Technical safeguards	Means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
Secretary	Means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.
Standard	Means a rule, condition, or requirement: 1. Describing the following information for products, systems, services, or practices: a. Classification of components; b. Specification of materials, performance, or operations; or c. Delineation of procedures; or 2. With respect to the privacy of protected health information.

Treatment, payment, and healthcare operations	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.
Use	With respect to patient identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
Workforce	Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity (FIU HIPAA Component) or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

ROLES AND RESPONSIBILITIES

1. **Compliance Oversight:** The Office of University Compliance and Integrity (University Compliance)
   - Evaluates all federal and state healthcare privacy laws, regulations, rules and ordinances (Rules) to ensure compliance with the Rules.
   - Develops and maintains all required University-wide Privacy Rule policies and procedures.
   - Develops and maintains HIPAA health care Privacy Rule training modules and ensures appropriate Workforce members complete the required training.
   - Performs audits and assessments of the Components to ensure their compliance with the Privacy Rules and associated FIU Policies and Procedures.
   - Partners with the Division of Information Technology HIPAA Security Officer to ensure compliance with all federal and state healthcare privacy and security laws, regulations rules, and ordinances.

2. **HIPAA Components:**

   - Each 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 that required BAAs are obtained prior to allowing Business Associates to create, use, disclose, or access PHI and must ensure BAAs are maintained during the course of the contract or other written agreement.

3. **Purchasing Department**

- Ensures that all contracts and other written agreements which may require a Business Associate Agreement are reviewed by the Office of Compliance and Integrity, the Division of Information Technology, and the Office of General Counsel to ensure proper application of HIPAA and state law.
- Properly posts the contracts and other written agreements containing a Business Associate Agreement as required by FIU policy and procedure and state law.
- Retains all contracts and other written agreements which contain a Business Associate Agreement for the retention period required by HIPAA and state law.

RELATED RESOURCES

References

- 45 CFR §164.502
- 45 CFR §164.504
- 45 CFR §164.524
- 45 CFR §164.526
- 45 CFR §164.528
- 45 CFR §164.530
- F.S. §456.057
- F.S. §95.11

Related Policies

-
- FIU Incident Response Plan
- FIU Policy # 1610.005 (Designated Health Care Components of FIU Community)
- FIU Policy and Procedure #1640.025 (Minimum Necessary)
- FIU Policy and Procedure #1660.050 (Patient Access to Protected Health Information)
- FIU Policy and Procedure #1660.055 (Amendment of Protected Health Information)
- FIU Policy and Procedure #1660.060 (Accounting of Disclosures of Protected Health Information)
- FIU Policy and Procedure #1660.070 (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)
- FIU Policy and Procedure #1660.075 (HIPAA Privacy and Security Rule Training)
- FIU Policy and Procedure #1660.80 (Policies and Procedures, Changes to Policies and Procedures, and Documentation)
- FIU Policy and Procedure #1660.085 (Sanctions)
- FIU Policy and Procedure #1660.095) (Reporting of HIPAA Incidents and Notification in Case of a Breach).

CONTACTS

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

HISTORY

Initial Effective Date: September 01, 2009
Review Dates (review performed, no updates): n/a
Revision Dates: September 01, 2009; June 8, 2015; December 31, 2017; November 1, 2019; March 3, 2010; October 13, 2020; July 27, 2021

Business Associate Agreements # 1660.015a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 1, 2009	July 27, 2021	Office of Compliance and Integrity

PROCEDURE STATEMENT

I. Business Associate Agreements

Each HIPAA Component must designate a Privacy Coordinator responsible for overseeing and ensuring the Component's implementation and compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable state laws and/or regulations governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to ensuring that required BAAs are obtained prior to allowing Business Associates to create, use, disclose, or access PHI and must ensure BAAs are maintained during the course of the contract or other written agreement. Privacy Coordinators may delegate and share duties and responsibilities as necessary and appropriate but retain oversight responsibility. (FIU Policy and Procedure #1660.070) (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)

A. HIPAA Component Privacy and/or Security Coordinator, designee or Administrative Workforce members with the authority to execute contracts or other written agreements (hereinafter contract(s)) on behalf of the HIPAA Component in which the individual or entity (hereinafter Vendor) seeking the contract performs a function(s) involving the creation, use, disclosure, or access of patient PHI, must forward a copy of the contract (or provide a link to the contract) to the Director of Compliance and Privacy for Health Affairs (Director of Compliance) with the Office of Compliance and Integrity, the HIPAA Security Officer (HIPAA Security Officer) with the Division of Information Technology, and the Office of General Counsel to determine whether a Business Associate relationship exists between the HIPAA Component and the external Vendor prior to entering into the contract.

B. The Director of the FIU Purchasing Department or staff designated with the authority to execute contracts on behalf of FIU in which a HIPAA Component may be impacted by the contract in which the Vendor seeking the contract performs a function involving the creation, use, disclosure, or access of patient PHI, must forward a copy of the contract (or provide a link to the contract) to the Director of Compliance, the HIPAA Security Officer, and the Office of General Counsel to determine whether a Business Associate relationship will exist between a Component(s) and the external Vendor prior to entering into the contract.

NOTE: See Attachment A for Common Examples of Business Associate Relationships.

NOTE: See Attachment B "*Decision Tree for Determining BAA Relationship*".

NOTE: A covered entity (a health care provider, health plan, or health care clearinghouse) can be a Business Associate of another covered entity.

C. If the Director of Compliance, the HIPAA Security Officer, and/or the Office of General Counsel determine that a Vendor would be a Business Associate, they must determine whether the appropriate BAA language has been included in the contract or needs to be included as an attachment.

D. If the Director of Compliance, the HIPAA Security Officer, and/or the Office of General Counsel determine that a Business Associate relationship exists, the Component Privacy and/or Security Coordinator, designee, or Administrative Workforce members with the authority to execute contracts or other written agreements shall be responsible for negotiating a BAA for all contracts that originate with the Component. The Director of the FIU Purchasing Department or staff designated with the authority to execute contracts on behalf of FIU shall be responsible for negotiating a BAA for all contracts that originate with the Purchasing Department.

NOTE: FIU will obtain a Business Associate Agreement with all external covered entities that meets the definition of a Business Associate if they perform a function on behalf of a Component involving the creation, use, disclosure, receipt, maintenance, and/or transmission of patient PHI.

NOTE: The HIPAA Components and the Purchasing Department generally must use the FIU BAA approved by the Office of General Counsel. See Attachment D

II. Required BAA Elements

A. BAAs must include the following elements as specified in the HIPAA Privacy Rule:
1. A description of the permitted and required uses of PHI by the Business Associate;
2. Provide that the Business Associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law;
3. Require that the Business Associate use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the BAA;
4. Require that the Business Associate use reasonable and required administrative, technical and physical safeguards to protect PHI and electronic PHI (ePHI);
5. Report to the Components' Privacy Coordinator, the Director of Compliance and Privacy for Health Affairs with the Office of Compliance and Integrity, the HIPAA Security Officer with the Information Technology Division, the Office of General Counsel, the Components' Director or Designee, or other FIU Workforce members

as required by the terms of the BAA, contract, or other written document, any use or disclosure not permitted by the contract or law, including any suspected security incidents relating to ePHI;

6. Ensure that any agents, including subcontractors, to whom it provides PHI/ePHI received from FIU or its HIPAA Components, or created or received by the Business Associate on behalf of FIU or its HIPAA Components, agent(s), including subcontractors, agrees to the same restrictions and conditions that apply to the Business Associate with respect to such information;
7. Make available to the HIPAA Component(s) the information necessary for the Component(s) to comply with patient rights to have access their PHI (FIU Policy and Procedure #1660.050) (Patient Access to Protected Health Information), to request amendment of their PHI (FIU Policy and Procedure #1660.055) (Amendment of Protected Health Information), and receive an accounting of disclosures of their PHI (FIU Policy and Procedure #1660.060) (Accounting of Disclosures of Protected Health Information);
8. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of FIU or the HIPAA Component(s) available to the Secretary of Health and Human Services for purposes of determining the HIPAA Component's and/or the Business Associate's compliance with the HIPAA Privacy and/or Security Rules; and
9. At termination of the contract, if feasible, return or destroy all PHI/ePHI received from, or created or received by the Business Associate on behalf of FIU or the HIPAA Components that the Business Associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

B. Any modifications to the FIU approved standard BAA must be reviewed and approved by the Office of General Counsel.

C. BAAs that are not included as part of a contract may be attached to the contract as an exhibit/attachment.

III. Utilizing Vendor BAAs and/or Vendor's Refusal to Sign a BAA

A. If a BAA is required and the Vendor provides its own BAA, the Component Privacy or Security Coordinator, designee, Component Administrative Workforce members with the authority to execute contracts or other written agreements on behalf of FIU, or the Director of the Purchasing Department, must forward the proposed Vendor BAA to the Director of Compliance, the HIPAA Security Officer, and the Office of General Counsel for review and approval/rejection prior to entering into the contract.

B. If an external Vendor refuses to sign a required BAA, the Vendor will not be permitted to create, use, disclose, or access patient PHI. If the Vendor requires the use or access to PHI in order to perform a function or service on behalf of FIU or a Component, FIU must not enter into a contract with the Vendor and the matter shall be referred to the Director of Compliance, the HIPAA Security Officer, and the Office of General Counsel for review and response.

IV. Posting the Contract and BAA

A. The Component Privacy or Security Coordinators, designee, and the Director of the Purchasing Department must maintain and update within the Purchasing Department "Total Contract Management" system, on a monthly basis, all executed contracts with BAAs.

V. Business Associate Violations, Noncompliance, or Breaches

A. If a Component Privacy or Security Coordinator, Purchasing Department Workforce member(s), or any other FIU Workforce member(s) or employee(s) believes a Business Associate, or the Business Associate's subcontractor, if any, has engaged in a pattern of activity or practice that constitutes a violation of the HIPAA Privacy and/or Security Rule(s), committed a breach, or a violation(s) of the Business Associate's obligation under the contract and/or BAA, the Component Privacy or Security Coordinator, Purchasing Department Workforce member(s), or any other FIU Workforce member(s) or employee(s) must immediately escalate the suspected or known violation and/or breach in a manner as described FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

B. Workforce members who receive notification of the suspected or known violation(s) or breach(es) must immediately escalate the notification to the Director of Compliance and Privacy for Health Affairs with the Office of Compliance and Integrity, the HIPAA Security Officer with the Division of Information Technology, the Privacy Officer with the Office of Compliance and Integrity, and/or the Office of General Counsel. (See FIU Policy and Procedure #1660.095) (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

C. An investigation of the suspected or known violation(s) or breach(es) will be conducted in a manner described in the FIU "Incident Response Plan" and the FIU HIPAA Investigative Policy and Procedure #1660.095) (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

D. If the investigation reveals that the Business Associate is in violation or committed a breach, the Director of Compliance and Privacy for Health Affairs with the Office of Compliance and Integrity, the HIPAA Security Officer with the Division of Information

Technology, and/or the Office of General Counsel, must contact the Business Associate verbally and in writing and ask that they immediately cease and desist operating in a manner inconsistent with the terms of the contract and/or BAA. The verbal and written notification must be documented in the Investigative File in a manner consistent with the requirements of the FIU HIPAA Investigative Policy and Procedure #1660.095) (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

E. If reasonable steps are unsuccessful in bringing the Business Associate into compliance or ceasing and desisting, the Office of General Counsel, may:
   1. Terminate the contract or arrangement; or
   2. If termination is not feasible, the Office of Compliance and Integrity, the Information Technology Division, and/or the Office of General Counsel will report the suspected or known violation(s) or breach(es) to the Secretary of the U. S. Department of Health and Human Services, and the Florida Attorney General in a manner consistent with FIU Policy and Procedure #1660.095) (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

F. The reasonable steps taken must be documented in the Investigative File in a manner consistent with the requirements of FIU HIPAA Investigative Policy and Procedure #1660.095) (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

   NOTE: All contract terminations are handled by the Office of General Counsel.

G. If the Office of General Counsel terminates a contract for noncompliance of the terms and conditions of the contract and/or the BAA, or a violation(s) or breach(es) of the HIPAA Privacy and/or Security Rules, the Office of General Counsel must provide written notice to the Director of Compliance and Privacy for Health Affairs, the HIPAA Security Officer, the affected Component, the Purchasing Department, if appropriate, and any and all other Department, Division, Section, and FIU Workforce members as deemed necessary and appropriate by the Office of General Counsel. The written notification must be documented in the Investigative File in a manner consistent with the requirements of the FIU HIPAA Investigative Policy and Procedure #1660.095) (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

H. If the Office of General Counsel terminates a contract with a Business Associate, the Office of General Counsel, the Director of Compliance and Privacy for Health Affairs and the HIPAA Security Officer will assist the affected Component or Purchasing Department with respect to the Business Associate's obligations to return or destroy all PHI or, if return or destruction is not feasible, to extend the protections of the Business Associate requirements to the PHI and to limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible. The verbal and written efforts, the disposition of the PHI, and any extension of protections provided for under the BAA must be documented in the Investigative File in a manner consistent

with the requirements of the FIU HIPAA Investigative Policy and Procedure #1660.095) (Reporting of HIPAA Incidents and Notification in the Case of a Breach).

I. A Business Associate is not in compliance with the terms of the Business Associate Agreement if the Business Associate knows of a pattern of activity or practice of their subcontractor(s) that constitutes a material breach or violation of the subcontractor's obligation(s) under the Business Associate Agreement, unless the Business Associate takes reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminate the contract or arrangement, if feasible.

VI. Record/Documentation Retention

A. HIPAA Component Privacy Coordinators and the Procurement Department Director, when appropriate, shall maintain the original signed contract and any contract addendums, amendments and attachments containing BAA language for seven (7) years after the contract was last in effect. The contract shall remain posted on the Total Contract Management system for seven (7) years from the date of its creation or the last effective date, whichever is later.

VII. Forms

- Business Associate Agreement (Attachment D)

VIII. Attachments

- BAA Common Questions (Attachment A)
- BAA Decision Tree (Attachment B)

IX. Frequently Asked Questions

- (Attachment C)