FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Business Associate Agreements # 1660.015

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 1, 2009	August 4, 2025	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 Components (hereinafter facilities and programs) 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) and electronic PHI (ePHI) 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, uses or discloses PHI in an electronic format (ePHI) must sign a BAA agreeing to protect the confidentiality, integrity and availability of the electronic information.

When a facility or program 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 comply with regulations that meet the objectives of the Privacy Rule business associate standard.

Unless otherwise approved by the Office of General Counsel, facilities, programs, 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, facilities and programs with guidance as to whether a BAA is necessary in those situations where the Purchasing Department or the facility or program have what appears to be a business associate relationship with a Vendor. The FIU Purchasing Department, and where necessary and appropriate, the facility or program 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).

Facilities, programs 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 facility and program Privacy Coordinator and the Purchasing Department will be responsible for maintaining all HIPAA documentation relevant to his/her facility or program. (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 facility and program Workforce members shall receive mandatory HIPAA Privacy and Security Rule training. (FIU Policy and Procedure # 1660.075) (HIPAA Privacy and Security Rule Training)

Facility and program 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)

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 facilities and programs 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 facilities and programs.

REASON FOR POLICY

FIU seeks to ensure that Business Associates adhere to the protections imposed by the HIPAA Privacy and Security Rules, federal laws and Florida state statutes, 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 facilities and programs must take in order allow a Business Associate to create, use, disclose, or access PHI/ePHI and establishes guidelines for facilities, programs 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.

DEFINITIONS

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

HIPAA Policies Definitions

ROLES AND RESPONSIBILITIES

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

- Evaluates all federal and state healthcare privacy laws, regulations, rules and ordinances (Rules) to ensure compliance with the Rules.
- Develops and maintains all required University-wide Privacy Rule policies and procedures.
- Develops and maintains HIPAA health care Privacy Rule training modules.
- Performs audits and assessments of the facilities and programs to ensure their compliance with the Privacy Rules and associated FIU Policies and Procedures.
- Partners with the Division of Information Technology HIPAA Security Officer to ensure compliance with all federal and state healthcare privacy and security laws, regulations rules, and ordinances.

HIPAA Components (Facilities and Programs):

- Each FIU HIPAA Hybrid Designated facility and program must designate a Privacy Coordinator responsible for overseeing and ensuring the facility's or program's

implementation and compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable federal laws and Florida state statutes 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.

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 Florida state law.
- Properly posts the contracts and other written agreements containing a Business Associate Agreement as required by FIU policy and procedure and Florida state law.
- Retains all contracts and other written agreements which contain a Business Associate Agreement for the retention period required by HIPAA and Florida state statutes.

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
- Florida Statute §456.057
- Florida Statute §95.11

Related Policies

- FIU Incident Response Plan #1930.021
- 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 Director of Compliance and Privacy for Health Affairs at (305) 348-0622 or hipaaprivacy@fiu.edu, or contact the appropriate Component Privacy Coordinator.

HISTORY

Initial Effective Date: September 01, 2009
Review Dates *(review performed, no updates)*: n/a
Revision Dates *(review performed, updates made to document)*: September 01, 2009; June 8, 2015; December 31, 2017; November 1, 2019; March 3, 2020; October 13, 2020; July 31, 2021; February 29, 2024; August 4, 2025.

Business Associate Agreements # 1660.015a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 1, 2009	August 4, 2025	Office of Compliance and Integrity

PROCEDURE STATEMENT

I. Business Associate Agreements

The facility and program Privacy Coordinators are responsible for 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. The facility or program 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 facility or program 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 (HIPAA Privacy Officer) 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 facility or program 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 facility or program 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 HIPAA Privacy and Security Officer, and the Office of General Counsel to determine whether a Business Associate relationship will exist between a facility or program 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 HIPAA Privacy or 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 HIPAA Privacy or Security Officer, and/or the Office of General Counsel determine that a Business Associate relationship exists, the facility or program 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 facility or program. 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 an FIU facility or program involving the creation, use, disclosure, receipt, access, maintenance, and/or transmission of patient PHI.

NOTE: The FIU facilities and programs 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, contract, or other written agreement;
   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 facility or program Privacy Coordinator, the HIPAA Privacy Officer, the HIPAA Security Officer, the Office of General Counsel, the facility or program 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, other written agreement, or law, including any suspected security incidents relating to PHI/ePHI;

6. Ensure that any agent, including subcontractors, to whom it provides PHI/ePHI received from FIU or its HIPAA facilities and programs, or created or received by the Business Associate on behalf of FIU or its HIPAA facilities and programs, 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 FIU HIPAA facilities and programs the information necessary for the facilities and programs to comply with patient rights to have access their PHI, to request amendment of their PHI, and receive an accounting of disclosures of their PHI;
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 facilities and programs available to the Secretary of Health and Human Services for purposes of determining the facility(ies) and/or program(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 received from, or created or received by the Business Associate on behalf of FIU or the facility(ies) or program(s) 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, or 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 FIU HIPAA facility or program Privacy or Security Coordinator, designee, facility or program Administrative Workforce member with the authority to execute contracts or other written agreements on behalf of FIU, the facility or program, or the Director of the Purchasing Department, must forward the proposed Vendor BAA to the HIPAA Privacy and Security Officer, and the Office of General Counsel for review and approval or rejection prior to entering into the contract and BAA.

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 HIPAA facility or program, FIU must not enter into a contract with the Vendor and the matter shall be referred to the HIPAA Privacy and Security Officer, and the Office of General Counsel for review and response.

IV. Posting the Contract and BAA

A. The facility or program Privacy or Security Coordinator, 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 the facility or program Privacy or Security Coordinator, Purchasing Department Workforce member, or any other FIU Workforce member or employee 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 facility or program Privacy or Security Coordinator, Purchasing Department Workforce member, or any other FIU Workforce member or employee must immediately escalate the suspected or known violation and/or breach. (See 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 HIPAA Privacy or HIPAA Security Officer 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), as necessary and appropriate.

D. If the investigation reveals that the Business Associate is in violation or committed a breach, 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 Incident Response Plan and/or HIPAA Investigative Policy and Procedure #1660.095) (Reporting of HIPAA Incidents and Notification in the Case of a Breach), as necessary and appropriate.

E. If reasonable steps are unsuccessful in bringing the Business Associate into compliance or with ceasing and desisting, the Office of General Counsel, may:
   1. Terminate the contract or other agreement; or
   2. If termination is not feasible, the Office of Compliance and Integrity, 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.

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) and the Incident Response Plan, as necessary and appropriate.

   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, or other agreement, 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 HIPAA Privacy and Security Officer, the affected facility or program, the Purchasing Department, if appropriate, and any and all other Departments, Divisions, Sections, 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), and the Incident Response Plan.

H. If the Office of General Counsel terminates a contract with a Business Associate, the Office of General Counsel, the HIPAA Privacy and Security Officer will assist the affected facilities, programs and/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 access, 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), and Incident Response Plan.

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. The facility and program 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)