



HIPAA Component Privacy Review and Audit #1660.090

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 13, 2020	August 6, 2025	Office of Compliance and Integrity

POLICY STATEMENT

The Florida International University (FIU) Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Components (hereinafter facilities and programs) Privacy Coordinators must conduct a quarterly assessment of their facility or program and utilize the HIPAA Facility Review Form to document the assessment. (Attachment A)

The Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity, or designee will perform an annual HIPAA Privacy Rule Audit of each facility and program and utilize the HIPAA Privacy Rule and HITECH Act Audit Tool to document the Privacy Audit. (Attachment B)

Privacy concerns or issues identified during the quarterly assessments and/or annual HIPAA Privacy Rule Audit shall be addressed by bringing the concern or issue into compliance with the requirements of the HIPAA Privacy Rule, Florida state statutes, and FIU associated HIPAA Privacy Rule Policies and Procedures.

The Director of Compliance and Privacy for Health Affairs will document and advise the Chief Compliance and Privacy Officer and the facility or program Administrative Officer of identified HIPAA Privacy Rule, federal law, Florida state statute, and/or associated FIU HIPAA Privacy Rule Policy and Procedure compliance issues and concerns and identify required corrective action.

As a University-wide policy and procedure, this policy and procedure takes precedence over any facility or program-specific policies, procedures, or protocols that conflict with this policy and procedure, unless prior approval is obtained from the Office of Compliance and Integrity. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

Facilities and programs 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 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)



All facility or program Workforce members shall receive mandatory HIPAA, federal rules and regulations, and Florida state statute privacy and security rule training. (FIU Policy and Procedure #1660.075) (HIPAA Privacy and Security Rule Training)

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

SCOPE

This policy applies to the FIU Components (hereinafter facilities and programs) contained within FIU's HIPAA Hybrid Designation (FIU Policy and Procedure #1610.005) and its Workforce members as defined in this policy and policy #1610.005.

REASON FOR POLICY

To establish procedures necessary to comply with the HIPAA mandate that all covered entities establish policies and procedures to ensure the privacy and confidentiality of protected health information (PHI). FIU's comprehensive assessment and audit program was designed as an ongoing internal HIPAA compliance monitoring program to ensure that the privacy policies and procedures are being followed correctly, that appropriate safeguards are in place, and that the privacy of PHI is being maintained in accordance with the mandated standards of HIPAA, the Health Information Technology for Economic and Clinical Health Act (HITECH), the Omnibus Rules and any amendments thereto, federal law, Florida state statutes, and to ensure the Workforce members within FIU's facilities and programs are adhering to FIU's HIPAA Privacy Rule policies and procedures.

DEFINITIONS

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

[HIPAA Policies Definitions](#)

ROLES AND RESPONSIBILITIES

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

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

HIPAA Components (Facilities and Programs):

- Each FIU HIPAA Hybrid Designated Components (hereinafter facilities and programs) must designate a Privacy Coordinator responsible for overseeing and ensuring the facility's or program's implementation and compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable Florida state statutes governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to completing quarterly Privacy Rule Reviews and participating in Privacy Rule Audits.

RELATED RESOURCES

References

- 45 CFR §164.504
- 45 CFR §164.530

Related Policies

- FIU Policy # 1610.005 (Designated Health Care Components of FIU Community)
- 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 #1660.080 (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

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: October 13, 2020

Review Dates (*review performed, no updates*): n/a

Revision Dates (*review performed, updates made to document*): October 13, 2020; February 29, 2024; August 6, 2025.



HIPAA Component Privacy Review and Audit #1660.090a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 13, 2020	August 6, 2025	Office of Compliance and Integrity

PROCEDURE STATEMENT

I. Quarterly Privacy Rule Assessments

The Component (facility and program) Privacy Coordinators are responsible for overseeing and ensuring the facility’s or program’s implementation and compliance with the HIPAA Privacy Rule, federal law, FIU’s associated HIPAA Privacy Policies and Procedures, and any applicable federal and Florida state statutes governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to conducting quarterly HIPAA Privacy Rule compliance assessments and assisting with the annual HIPAA Privacy Rule Audit. 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 Facility or Program Privacy and Security Coordinators)

- A. Each calendar quarterly (January-March, April-June, July-September, and October-December), the facility and program Privacy Coordinators shall complete a quarterly HIPAA Privacy Assessment. The Privacy Coordinators shall:
 - 1. Complete, sign, and date the HIPAA Facility Review Form to document the assessment (Attachment A),
 - 2. Submit the completed HIPAA Facility Review Form to the Director of Compliance and Privacy for Health Affairs (Director of Compliance) not- greater than ten (10) calendar days following the completed calendar quarter, and
 - 3. The Director of Compliance, or designee, shall ensure the completed HIPAA Facility Review Forms are scanned and posted within a designated folder within the HIPAA SharePoint.

- B. If the Privacy Coordinator identifies a concern or issue of noncompliance with the HIPAA Privacy Rules, Florida state statutes, and/or associated FIU HIPAA Privacy Rule Policies or Procedures, the Privacy Coordinator and the Director of Compliance, or designee shall:
 - 1. Respond to the noncompliance concern or issue to ensure it is brought into compliance.
 - 2. Document the corrective action taken, and the Director of Compliance, or designee, shall within fifteen (15) calendar days, or as time permits:

- a. Submit an Assessment Report to the Chief Compliance and Privacy Officer, Office of Compliance and Integrity, as necessary and appropriate, identifying the noncompliance concern or issue and the corrective action taken.
3. As necessary and appropriate, the Director of Compliance shall provide a copy of the final Assessment Report to the facility or program Administrative Officer.

II. Annual Privacy Rule Audits

- The Director of Compliance, or designee shall complete an annual HIPAA Privacy Audit (Audit) of a designated facilities and programs. The facility or program Privacy Coordinator shall assist with the Audit. The Director of Compliance, or designee shall:
 1. Complete, sign, and date the HIPAA Privacy Rule and HITECH Act Audit Tool (Audit Tool) to document the Audit (Attachment B),
 2. Scan and post the completed Audit Tool within a designated folder within the HIPAA SharePoint,
 3. If during the course of the Audit the Director of Compliance, designee, or Privacy Coordinator identifies a concern or issue of noncompliance with the HIPAA Privacy Rules and/or associated FIU HIPAA Privacy Policies and Procedures, the Director of Compliance, designee, or Privacy Coordinator shall:
 - a. Respond to the noncompliance concern or issue to ensure it is brought into compliance,
 - b. Document the corrective action taken within fifteen (15) calendar days, or as time permits:
 1. Submit an Audit Report to the Chief Compliance and Privacy Officer identifying the noncompliance concern(s) or issue(s) and the corrective action taken, and
 4. As necessary and appropriate, provide a copy of the final Audit Report to the facility or program Administrative Officer.

III. Record/Documentation Retention

- A. If a communication, action, activity, or designation is required to be documented in writing, the document or record owner (The facility or program) will maintain such writings, or an electronic copy, for seven (7) years from the date of its creation or the last effective date, whichever is later. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

IV. Forms

- HIPAA Facility Review Form (Attachment A)
- HIPAA Privacy Rule and HITECH Act Audit Tool (Attachment B)



FLORIDA
INTERNATIONAL
UNIVERSITY

