FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

HIPAA Component Privacy Review and Audit #1660.090

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

POLICY STATEMENT

Each Florida International University (FIU) Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Health Care Component (Component) must conduct quarterly assessments of the Component 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, shall perform an annual HIPAA Privacy Rule Audit of each Component 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 and associated FIU 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 Component Administrative Office(s) of identified HIPAA Privacy Rule and/or associated FIU HIPAA Privacy Rule Policy and Procedure problems and concerns and required corrective action.

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

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)

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

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) 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, and to ensure the Workforce members within FIU's Components are adhering to FIU's HIPAA Privacy Rule policies and procedures.

DEFINITIONS

TERM	DEFINITIONS
Access	Means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
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	Means the 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 patient.
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.
HITECH	The Health Information Technology for Economic and Clinical Health (**HITECH**) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology.
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.
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.
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.
Required by law	Means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
Technical safeguards	Means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
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	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 FIU HIPAA Hybrid Designated Component must designate a Privacy Coordinator responsible for overseeing and ensuring the Component's implementation and compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable state laws and/or

regulations governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to 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 FIU Office of Compliance and Integrity at (305) 348-2216, compliance@fiu.edu, or the appropriate Component Privacy Coordinator.

HISTORY

Initial Effective Date: October 13, 2020
Review Dates (review performed, no updates): n/a
Revision Dates: October 13, 2020

HIPAA Component Privacy Review and Audit #1660.090a

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

PROCEDURE STATEMENT

I. Quarterly Privacy Rule Assessments

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 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 Component Privacy and Security Coordinators)

A. Each calendar quarterly (January-March, April-June, July-September, and October-December), the Component 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) no-later 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(s) or issue(s) of noncompliance with the HIPAA Privacy Rules 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(s) or issue(s) to ensure it/they is/are 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(s) or issue(s) 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 Component Administrative Officer.

II. Annual Privacy Rule Audits

- Each month, beginning January of each calendar year, the Director of Compliance, or designee, shall complete an annual HIPAA Privacy Audit (audit) of a designated Component. The Component 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(s) or issue(s) 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(s) or issue(s) to ensure it/they is/are 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 Component Administrative Officer.

- The Director of Compliance, or designee, shall conduct the monthly audits in the following order, beginning January of each calendar year. (This schedule and order is subject to change based on the demands and obligations of the Director of Compliance, designee and /or the Office of Compliance and Integrity).
  1. Herbert Wertheim College of Medicine (HWCOM), excluding Research,
  2. Student Health Pharmacy Services,
  3. College of Arts and Science Center for Children and Family,
  4. Office of General Counsel,
  5. Office of Internal Audits,
  6. Office of Compliance and Integrity,
  7. Division of Information Technology,
  8. Office of Human Resources, and
  9. FIU Foundation.

III. Record/Documentation Retention

A. If a communication, action, activity, or designation is required to be documented in writing, the document or record owner (e.g., the Office of Compliance and Integrity) 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)