



Class of Jobs and/or Job Titles of Workforce Members Who Require Access to PHI/ePHI and the Categories of PHI/ePHI Necessary to Carryout Job Functions and Responsibilities # 1660.105

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
August 31, 2021	August 6, 2025	Office of Compliance and Integrity

POLICY STATEMENT

Florida International University’s (FIU) Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Components (hereinafter facilities and programs) must identify the job titles and/or the class of jobs of Workforce members, as appropriate, in its workforce who need access to Protected Health Information (PHI) to carry out their duties; and for each such job title or class of jobs of Workforce members, the category or categories of PHI to which access is needed and any conditions appropriate for such assess.

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 #1660.80) (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 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 harmonized consistent with the requirements of HIPAA and Florida state statute. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

SCOPE

This policy applies to FIU Components (hereinafter facilities and programs) contained within FIU’s HIPAA Hybrid Designation (FIU Policy and Procedure #1610.005), its Workforce members and Business Associates as defined in the policy and FIU Policy and Procedure #1660.015 regarding Business Associate Agreements.

REASON FOR POLICY

The intent of this policy is to address the job titles or class of jobs of Workforce members within each facility and program who require access to PHI/ePHI to carry out their duties; and for each such job title or class of jobs of Workforce members, the category or categories of PHI/ePHI to which access is required and any conditions appropriate to such access in order to limit the use and disclosure of patient PHI/ePHI by facility or program Workforce members based on their duties and responsibilities.

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 Component (hereinafter 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 Florida state statutes governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI).
- Each facility and program must identify the titles and/or class of job that require access to patient PHI based on the minimum necessary standard.

Compliance Oversight: The Division of Information Technology

- 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 Security Rule policies and procedures.
- Develops and maintains HIPAA Security Rule training modules and ensures appropriate Workforce members complete the required training.
- Assist and provide guidance as necessary and appropriate with identifying the titles and/or class of jobs of Workforce members who require access to patient PHI and the level of access based on the minimum necessary standard.
- Performs audits and assessments of the facilities and programs to ensure their compliance with the Security Rules and associated FIU Policies and Procedures.
- Partners with the Office of Compliance and Integrity Director of Compliance and Privacy for Health Affairs to ensure compliance with all federal and state healthcare privacy and security laws, regulations rules, and ordinances.

Division of Human Resources

- Work closely with the facilities and programs to identify the job titles and/or class of jobs of Workforce members who require access to patient PHI based on the minimum necessary standard and any collective bargaining agreement requirements that may impact the classifications.

RELATED RESOURCES



References

- 45 CFR §164.502
- 45 CFR §164.504
- 45 CFR §164.524
- 45 CFR §164.530

Related Policies

- FIU Policy # 1610.005 (Designated Health Care Components of FIU Community)
- FIU Policy and Procedure #1640.010 (HIPAA Privacy and Security Rule Training)
- FIU Policy and Procedure #1660.015 (Business Associate Agreements)
- FIU Policy and Procedure #1660.070 (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)
- FIU Policy and Procedure #1660.075 (HIPAA Privacy and Security Rule Training)
- FIU Policy and Procedure #1660.080 (Policies and Procedures, Changes to Policies and Procedures, and Documentation)
- FIU Policy and Procedure #1660.085 (Sanctions)
- FIU Policy and Procedure #1660.110 (Designated Record Set)
- FIU Policy and Procedure #1660.120 (Minimum Necessary)

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: August 31, 2021

Review Dates (*review performed, no updates*): N/A

Revision Dates (*review performed, updates made to document*): August 31, 2021; February 29, 2024; August 6, 2025.



Class of Jobs and/or Job Titles of Workforce Members Who Require Access to PHI/ePHI and the Categories of PHI/ePHI Necessary to Carryout Job Functions and Responsibilities # 1660.105a

INITIAL EFFECTIVE DATE: August 31, 2021	LAST REVISION DATE: August 6, 2025	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT Office of Compliance and Integrity
---	--	---

PROCEDURE STATEMENT

I. Workforce Member Access to Patient PHI/ePHI

The Component (facility and program) Privacy Coordinators are responsible for overseeing and ensuring their 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 patient Protected Health Information (PHI) and electronic PHI (ePHI), including, but not limited to ensuring that the Class of Jobs and/or Job Titles (“Roles”) of Workforce members who require access of PHI/ePHI, the categories of PHI/ePHI necessary to carryout job functions and responsibilities, and the level of access are identified and documented. 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 and Program Privacy and Security Coordinators)

- A. Access to PHI/ePHI is limited to specific Roles of Workforce members who perform patient functions directly on behalf of a facility or program as determined by their facility or program and as approved by the HIPAA Security Officer with the Division of Information Technology (Division of IT) and the Director of Compliance and Privacy for Health Affairs.
- B. All access to PHI, whether it be electronic (ePHI) or hardcopy, must be limited to Workforce members who have a legitimate clinical or business need-to-know the information. Accessing or using more information than is necessary to do one’s job is prohibited.
- C. Facility and program Privacy and Security Coordinators, Administrative Officer(s), assigned Human Resources staff members, and Information Technology Directors, or designees (hereinafter facility and program Group) are responsible for analyzing and determining Roles of Workforce members within their facility or program who require access to PHI/ePHI, and what level of access each Role requires. The HIPAA Security Officer and the Director of Compliance and Privacy for Health Affairs will assist and provide guidance, as necessary and appropriate.

- D. The level of access granted (user access rights) will be based on a standard of “minimum necessary” and will identify the Roles of Workforce members and facility or program name. The standard of minimum necessary is essential for functionality while reducing faults and malicious behavior.
- E. Each facility and program Group will evaluate and determine if access to the highest level of PHI (e.g., unlimited access to the entire hard-copy medical record or electronic information) may be justified in the following circumstances:
1. The Role provides direct clinical care (e.g., nurses, physicians, athletic trainers, speech or language pathologist, audiologists, psychologists, mental health therapists, physical therapists, pharmacists, social workers, dieticians, and health care trainees/health care students in assigned rotation or clerkship) and access to different parts of the medical record for different patients may vary from patient to patient depending on the circumstances surrounding the provision of care.
 2. The Role conducts quality assurance, peer review and related functions and access to potentially all protected health information is necessary because different review processes may require access to different parts of a patient’s medical record.
 3. The Role is legal or risk management function and access to potentially all of a patient’s PHI is necessary because review and use of the PHI may require access to different parts of the medical record depending on the circumstances surrounding the legal or risk management inquiry.
 4. The Role is related to Health Information Management (Medical Records) and is necessary to code, release, file, transport, and secure medical records.
 5. The Role in business services/billing in which access to potentially the entire medical record is necessary to provide third party payors with information related to payment of a claim.
 6. The Role needs access to potentially the entire medical record because the individuals in those roles need to investigate employee or patient issues or complaints (e.g., Directors, Managers, Supervisors, Risk Manager, Privacy Coordinator, Privacy Officer, and HIPAA Security Officer and Security Coordinator).
 7. The Role of senior management, administration staff and the facility or program Privacy and Security Coordinators who potentially need access to the entire medical record for treatment, payment, or health care operations purposes.
- F. Each facility and program Group is responsible for ensuring Workforce members have access to appropriate levels of PHI. This includes electronic (ePHI) and paper.
- G. Each facility and program Group will evaluate and determine if varying levels of access to PHI/ePHI may be appropriate, depending upon Role definition. For the following Roles, Workforce member with varying levels of need to access PHI often have access to the entire medical record, and are expected to access and use only that PHI in the hard-copy medical record, that they would normally have access to electronically ePHI:

1. Workforce members that provide support to direct clinical providers (e.g., clinic assistants, clerical support staff, and physician secretaries) and access needs to varying levels of PHI depend on the type of support provided (e.g., ordering tests, supplies, and etc. for patients, maintenance of charts, data collection related to treatment, completion of billing or compliance paperwork).
2. Business management Workforce members in which access to limited PHI (e.g., demographic and financial information) is necessary for business and operations analysis and decision-making.
3. Information Services and Technology Workforce members who need access to electronic systems to provide technological support to these systems.
4. Admissions/Registration Workforce members who need access to limited PHI to process admissions documents, provide information to payors for benefits information and related purposes, and to schedule clinic visits or procedures.
5. Public Affairs Workforce members who need access to limited PHI to handle inquiries from outside sources and to manage marketing and fundraising activities.

NOTE: Minimal access to use PHI is appropriate for the following Roles depending on job duties:

- Some volunteers or others who need minimal access to PHI, for example, to assist families and friends with directory information, to provide information in the surgical waiting room, and to deliver items to patients.

NOTE: Access to use PHI, except when incidental, is inappropriate for the following roles:

- Housekeeping/Environmental services.
- Transportation staff who handle and deliver PHI (i.e., in a sealed envelope or box).
- Plant engineering/facility management.

- H. Each facility or program Group will carry out periodic reviews, at least annually, but more frequently when appropriate, of access levels to determine:
1. Changes in Workforce member position or scope of responsibilities; and
 2. Changes in information available through information technologies and tools.
- I. Each facility or program Group will document and maintain a current list of their Workforce members and their access level to PHI/ePHI based on each Workforce member's Role. The Privacy and/or Security Coordinator will provide the HIPAA Security Officer and the Director of Compliance and Privacy for Health Affairs with the most current list identifying the name and title of each Workforce member authorized to access PHI/ePHI, their Role, and the rights that they have been granted with respect to accessing PHI/ePHI.
- J. The Division of IT will keep a comprehensive matrix of how and to whom access rights are granted based on Roles. A Sample list of user access rights can be found in the attached table. (See Attachment A – Role Based Matrix)

- K. Facility or program Information Technology Directors, Privacy and Security Coordinators, in collaboration with data security analysts, will periodically monitor (audit) and document access to determine appropriateness of Workforce member review of PHI/ePHI by reviewing Role-based unit/section assignment within the facility or program.
- L. Workforce members with access to patient PHI/ePHI may not disclose PHI/ePHI, unless the request for access or disclosure is done in compliance with the HIPAA Privacy Rule, federal law, Florida state statutes, and associated FIU HIPAA Privacy and Security Rule Policies and Procedures.
- M. Workforce members may not access either through the FIU information systems or the patient's medical records, the medical and/or demographic information for themselves, family members, friends, FIU Workforce members, or other individuals for personal or other non-work related purposes, even if written authorization or patient oral permission has been given.

If the Workforce member is a patient in a facility or program, the Workforce member must follow the FIU Access Policy and Procedure and make their request for access through their Medical Records Manager/Supervisor in order to request their own PHI. (See FIU Policy and Procedure #1660.050 (Access), FIU Policy and Procedure 1660.051 (Workforce Member Access to Their Own Electronic Protected Health Information) FIU Policy and Procedure #1660.052 (Workforce Members' Access to Family Members' Electronic Protected Health Information (ePHI) or PHI) and FIU Policy and Procedure #1660.150 (Sanctions for the Impermissible Access of Self or Family Medical Records))

- N. In the very rare circumstance when a Workforce member's job requires him/her to access and/or copy the medical information of a family member, a Workforce member, or other personally known individual, then he/she must immediately report the situation to his/her Privacy Coordinator, Administrative Officer, and/or Manager who will determine whether to assign a different Workforce member to complete the task involving the specific patient.
- O. A Workforce member's access to his/her own PHI/ePHI must be based on the same procedures available to other patients and not based on the Workforce member's job-related access to PHI/ePHI and/or FIU information systems.

For example, if a Workforce member is waiting for a lab result or wants to view a clinic note or operative report, the Workforce member must make a request to the facility or program Medical Records Manager/Supervisor. Workforce members are not authorized to access his/her own PHI/ePHI; the Workforce member must go through all the appropriate channels as any other patient would be required to follow. (See FIU Policy and Procedure 1660.051 (Workforce Member Access to Their Own Electronic Protected Health Information))

II. **Record Retention**



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

III. Form

- A. Attachment A - Role Based Matrix



ROLE BASED ACCESS TO PHI

LEVEL 1: None – No Access to Designated Record Set (i.e. Volunteer)

LEVEL 2: May access minimum necessary PHI (not Designated Record Set) to complete assigned tasks and/or to document actions (i.e. PHI discussed)

LEVEL 3: Full access to the Medical Record subset of the Designated Record Set

LEVEL 4: Full access to the Business Office File subset of the Designated Record Set

Class of Jobs or Job Titles	Access Level				Explanation/Duties Performed Requiring Access
	1	2	3	4	
	HWC				
Dean		x	x	x	Treatment/Payment/Operations (Example) Provides treatment, etc.
CEO		x	x	x	Treatment/payment/Operations
Assistant to the Dean		x			Operations (Example) Obtains patient information necessary for the...
Assistant to the CEO		x			Operations
Risk Manager		x	x	x	Treatment/Payment Operations (Example) Reviewing risks, evaluates patient records, treatment incidents, reports incidents....
Risk Administrative Assistant		x	x	x	Treatment/Payment Operations (Example) Obtains necessary documentation for the Risk Manager’s review and prepares reports...
Director of IT		x	x	x	Treatment/Payment Operations (Example) Reviews all IT equipment containing ePHI and resolves IT problems...
	HWC Faculty Practice/Psychiatry				
Medical Doctor		x	x	x	Treatment/payment/Operations
Admissions/Marketing		x	x	x	Operations/Payment
Clinical Staff		x	x	x	Treatment/Payment/Operations
Financial Staff		x		x	Operations/Payment
Management Staff		x	x	x	Treatment/Payment/Operations
Assistant Administrator		x	x	x	Operations/Payment
Assistant Director of Nursing		x	x	x	Treatment/Payment/Operations
Business Office Manager		x	x	x	Operations/Payment
Business Office Staff/Patient Services		x		x	Operations/Payment (Example) Appointment; Scheduling; Override schedule – with RN approval; View/Modify Patient Information, and Daily Appointment and Reports.
Central Supply Clerk		x			Operations/Payment



Certified Nursing Assistant		x			Treatment
Front Desk/Medical Assistant		x			Treatment/Operations (Example) Schedules and modifies appointments, verifies insurance and receives payments, view/modify Patient Information; Daily Appointment Reports, and Batch – Case Management; Enrollment and Encounter Information; Transaction Entry; Check-in; and Create fees and Tickets.
Medial Student		x	x		Treatment
Director of Nursing		x	x	x	Treatment/Payment/Operations
Housekeeping, Laundry, Maintenance Staff		x			Operations
Nursing Student		x			Treatment
LPN		x	x		Treatment/Operations
MDS Coordinator		x	x	x	Treatment/Payment/Operations
Medical Records Supervisor		x	x	x	Operations/Payment
Nurse Manager		x	x	x	Treatment/Operations
Privacy and Security Coordinator		x	x	x	Treatment/Payment/Operations (Example) Evaluates patient complaints, conducts HIPAA Privacy Rule assessments involving patient PHI...
Medical Records Manager/Supervisor		x	x	x	Treatment/Payment/Operations View Patient Information; Run Chart; Pull Reports (daily appointments), and View Schedule.
Receptionist	x				
Restorative Nursing Assistant		x			Treatment/Operations
RN		x	x		Treatment/Operations
Social Services Staff		x	x	x	Treatment/Payment/Operations
Staff Development Nurse		x	x		Treatment
Volunteers	x				
	HWCOP Neighborhood Help and Mammogram				
Medical Doctor		x	x	x	Treatment/Payment/Operations
Restorative Nursing Assistant		x	x	x	Treatment/Operations
Billing Clerk		x	x		Treatment/Payment (Example) Payment and Remittance Advice; Charge Entry; Claim Entry; Process Claim; Financial Report, and Payer Information/Edit/Modify Patient financial records.
Administrative Officer					
Physician Assistant					
Medical Student					
Social Worker Student (PhD Candidate)					
Nurse Practitioner					



Social Worker Student (MS Candidate)					
Nursing Student					
	Pharmacy				
Pharmacist					Treatment/Payment/Operations Full access to patient records
Pharmacy Assistant					
	Division of Information Technology				
CIO		x	x	x	Operations
Application Analyst		x	x	x	Operations (Example) Schedule template -add/ modify; Full System Administrative Rights; Full File Maintenance, and All Operational functions in EMR.
HIPAA Security Officer		x	x	x	Operations (Example) Schedule template -add/ modify; Full System Administrative Rights; Full File Maintenance, and All Operational functions in EMR. Access Hardcopy and electronic medical records and Designated record Set for auditing, compliance and investigative purposes.
Director of Infrastructure					Operations
	Office of General Counsel				
General Counsel		x	x	x	Operations
Deputy General Counsel		x	x	x	Operations
Sr. Legal Counsel		x	x	x	Operations
Sr. Legal Counsel Chief Legal Officer		x	x	x	Operations
Associate General Counsel		x	x	x	Operations
Assistant General Counsel		x	x	x	Operations
Special Assistant to General Counsel		x	x	x	Operations
Paralegal III		x	x	x	Operations
Senior Coordinator		x	x	x	Operations
Administrative Assistant		x	x	x	Operations
	Office of Compliance & Integrity				



Psychologist (PhD)					
Student (Psychology) (PhD Candidate)					
Student (Psychology) (M.S. Candidate)					
Student (Psychology) (B.S. Candidate)					
Billing Clerk					
Administrative Assistant					
Administrative Coordinator					
Information Technology Manager					