



**Workforce Member Access to Their Own Electronic Protected Health Information (ePHI) or PHI # 1660.051**

<b>INITIAL EFFECTIVE DATE:</b>	<b>LAST REVISION DATE:</b>	<b>RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT</b>
November 6, 2023	November 6, 2023	Office of University Compliance and Integrity

**POLICY STATEMENT**

Florida International University (“FIU”) is committed to protecting the privacy of Protected Health Information (PHI) in compliance with all applicable federal and state laws, regulations, and rules.

The minimum necessary requirements of the HIPAA Privacy Rule provides that Workforce members must only access the minimum necessary PHI to perform their assigned clinical or business tasks to fulfill their specific job duties and assignments. (See FIU Policy and Procedure #1660.120 (Minimum Necessary)).

Workforce Members’ job duties do not include accessing their own medical records for any reason on FIU’s time. Additionally, spending time in one’s own medical records may be considered a disciplinary offense.

At no time and for no reason is a Workforce member permitted to access, alter, edit, write orders within, sign documents, or change the information in their medical records. This activity may constitute prohibited alteration of a legal record and prohibited practice of medicine.

At no time and for no reason is a Workforce member permitted to use his/her user identification, unique user credentials, and password to access his/her PHI contained within the Electronic Medical Records Application (EMR). Workforce members who want to access their PHI must do so in accordance with FIU Policy and Procedure #1660.050 (Patient Access to Protected Health Information).

When impermissible access is confirmed, Workforce members are subject to sanctions consistent with FIU Policy and Procedure #1660.086 (Sanctions for Impermissible Access to Self or Family Members’ Medical Records).



**SCOPE**

This policy applies to all Workforce members (e.g., employees, faculty, medical staff, volunteers, students, and other persons) and Business Associates performing work for or on behalf of an FIU HIPAA Hybrid Designed Health Care Component(s)/Unit(s).

**REASON FOR POLICY**

The purpose of this policy is to establish requirements for the appropriate access of protected health information (PHI) that is stored, managed, and/or maintained in an Electronic Medical Record Application (EMR). FIU recognizes that individuals, including Workforce members, have a right to request access to and obtain copies of their protected health information.

FIU has established a policy and procedures for patients (including Workforce members) to access and obtain copies of their PHI. Workforce members must adhere to the patient access policy and procedure when seeking to access or obtain their medical records.

**DEFINITIONS**

TERM	DEFINITIONS
<b>Access</b>	Means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
<b>Business Associate</b>	<p>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).</p> <p><b>NOTE:</b> 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.</p> <p><b>NOTE:</b> 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,</p>

	data aggregation, management, administrative, accreditation, software support, or financial services. A Business Associates does not, however, include HIPAA Component workforce members.
<b>Covered Entity</b>	An entity that is subject to HIPAA. <ol style="list-style-type: none"> <li>1. a health plan;</li> <li>2. a health care clearinghouse; and/or</li> <li>3. a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.</li> </ol>
<b>Component</b>	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.
<b>Designated Record Set</b>	Designated Record Sets include medical records, billing records, payment and claims records, health plan enrollment records, case management records, as well as other records used, in whole or in part, by or for a covered entity to make decisions about individuals.
<b>Health Care</b>	Means the care, services, or supplies related to the health of a patient, including: <ol style="list-style-type: none"> <li>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/client or that affects the structure or function of the body; and</li> <li>2. sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.</li> </ol>
<b>Health Care Component</b>	See "Component"
<b>Health Care Provider</b>	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.
<b>Health Information</b>	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 a patient; or the past, present, or future payment for the provision of health care to a patient.
<b>HIPAA</b>	Means the Health Insurance Portability and Accountability Act of 1996.
<b>Hybrid Covered Entity</b>	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.
<b>Protected Health Information (PHI)</b>	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: <ol style="list-style-type: none"> <li>1. Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g (“FERPA”);</li> <li>2. Records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and</li> <li>3. Employment records held by a covered entity in its role as an employer.</li> </ol>
<b>Representative</b>	For purposes of HIPAA's Privacy Rule, a person is an individual's personal representative if, under applicable state law, he or she can act on the individual's behalf in making decisions related to health care.
<b>Standard</b>	Means a rule, condition, or requirement: <ol style="list-style-type: none"> <li>1. Describing the following information for products, systems, services, or practices: <ol style="list-style-type: none"> <li>a. Classification of components;</li> <li>b. Specification of materials, performance, or operations; or</li> <li>c. Delineation of procedures; or</li> </ol> </li> <li>2. With respect to the privacy of protected health information.</li> </ol>
<b>Treatment</b>	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.
<b>Use</b>	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.



<b>Workforce</b>	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 in coordination with the Office of General Counsel and the HIPAA Hybrid Designated Component Privacy Coordinators all required University-wide Privacy Rule 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).

**RELATED RESOURCES**

**References**

- 45 CFR § 164.502(a)
- 45 CFR § 164.502(b)

**Related Policies**

- FIU Policy and Procedure #1610.005 (Designated HIPAA Health Care Components of FIU Community)
- FIU Policy and Procedure #1660.015 (Business Associate Agreements)
- FIU Policy and Procedure #1660.050 (Patient Access to Protected Health Information)
- FIU Policy and Procedure #1660.070 (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)
- FIU Policy and Procedure #1660.085 (Sanctions)



- FIU Policy and Procedure #1660.105 (Class of Workforce Members who Require Access to PHI)
- FIU Policy and Procedure #1660.120 (Minimum Necessary)

### CONTACTS

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

### HISTORY

**Initial Effective Date:** November 6, 2023

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

**Revision Dates** (*updates made to document*): November 6, 2023



**Workforce Member Access to Their Own Electronic Protected Health Information (ePHI) or PHI # 1660.051a**

<b>INITIAL EFFECTIVE DATE:</b>	<b>LAST REVISION DATE:</b>	<b>RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT</b>
November 6, 2023	November 6, 2023	Office of Compliance and Integrity

**PROCEDURE STATEMENT**

**I. Workforce Member Access to Their Own Electronic Protected Health Information**

- A. Workforce members must make their request with the Medical Records Manager, or designee (hereinafter Medical Records Manager) to access and/or obtain a copy of their PHI contained within their Designated Record Set.
- B. The Medical Records Manager will request the Workforce member make their request in writing by completing and submitting the Patient Access Request form (Access Form).
- C. Although the Medical Records Manager will request the Workforce member complete and submit the Access Form, the Medical Records Manager will accept all verbal request for access and will not require the Workforce member to make their access request by submitting a completed Access Form.
- D. If a Workforce member makes a verbal request to access to his/her PHI, the Medical Records Manager will complete the Access Form, including the "For FIU Healthcare Component USE ONLY" section of the Access Form and properly secure it within the Workforce member's medical records. In the alternative, the Medical Records Manager may document in the Workforce member's medical records the Workforce member's verbal request and all action taken by the Medical Records Manager on the request.
- E. The Medical Records Manager will not ask the Workforce member the reason(s) for making the request for access and/or to obtain copy their PHI.
- F. If the Workforce member makes a request for a copy of a document(s) contained within the medical records, the Medical Records Manager will make the requested copy, provide it to the Workforce member, and document the action taken within the Workforce member's medical records. (See I(A-D) immediately above)



G. In the alternative, the Workforce member may make his/her request for access to his/her PHI via the Electronic Medical Records Application (EMR) portal. In response to such a request, the Medical Records Manager must provide the requested access via the portal if consistent with internal policies and procedures regarding portal access.

II. The Medical Records Manager Adherence to the Patient Access to Protected Health Information Policy and Procedure.

A. The Medical Records Manager must use his/her identification, unique user credentials, and password to log into the Electronic Medical Records Application (EMR) and provide the Workforce member access to his/her requested PHI.

B. The Medical Records Manager must remain with the Workforce member during the entire time the Workforce member is accessing his/her medical records and engaging in a visual inspection of the PHI.

C. The Medical Records Manager will only permit the Workforce member to view the medical records. If the Workforce member makes a request for a copy of the medical records or specific PHI, the Medical Records Manager will produce a copy of the requested documents in the form, format and manner requested.

D. In the alternative, the Workforce member may make his/her request for access to the PHI via the Electronic Medical Records Application (EMR) Portal. In response to such a request, the Medical Records Manager must provide the requested access via the Portal if consistent with internal policies and procedures regarding Portal access.

E. The Medical Records Manager will charge the Workforce member access fees in the same manner that all patients and Representatives are charged a reasonable cost-based fee.

F. The Medical Records Manager will ensure that any request to edit, modify, add or delete information contained within the medical records is addressed and completed in a manner consistent with the requirements of FIU Policy #1660.055 (Amendment of Protected Health Information).

G. The Medical Records Manager will ensure that all documents requiring a signature (e.g., laboratory reports) are signed by the ordering health care provider.

**NOTE:** The ordering health care provider must not be the patient of the Medical Records/PHI, unless previously approved by the Healthcare Component Administrative Officer or Medical Director and the Administrative Officer or Medical Director documented the approval in the health care provider's/patient's medical records at the time of the approval.





H. Any and all suspected or known violations of this policy and/or procedure must be reported to the Director of Compliance and Privacy for Health Affairs.

III. Confidentiality Agreement

A. All Workforce members within the Healthcare Component must annually read, sign and date the “Confidentiality Agreement - User Activity in Systems Containing Protected Health Information (PHI)” form as part of the new employee Healthcare Component onboarding process and annually thereafter by no-later than March 15<sup>th</sup>.

IV. 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 Center for Children and Family) 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)