FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Sanctions for the Impermissible Access of Self or Family Medical Records # 1660.086

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
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.

Workforce Members must not access their own or a family members' protected health information (PHI and ePHI) unless specifically permitted under the HIPAA Privacy Rule, federal law, Florida state statute, and FIU associated policy and procedure. (See FIU Policy and Procedure # 1660.051) (Self) and FIU Policy and Procedure # 1660.052) (Family)

Workforce Members may be subject to sanctions, up to and including discharge from employment, for impermissibly accessing their own or a family members' PHI when the Workforce Member used their user identification, unique user credentials, and password to access PHI on the Electronic Medical Records Application (EMR).

Workforce Members may be subject to sanctions, up to and including discharge from employment, for impermissibly accessing their own or a family members' PHI maintained in paper records.

Acknowledging that each incident may have specific and unique circumstances, aggravating and mitigating factors are considered in determining appropriate sanctions.

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 the FIU HIPAA Hybrid Designed Health Care Components/Units.

REASON FOR POLICY
The purpose of this policy is to provide consistency in classifying the level and of sanctions when a Workforce Member impermissibly accesses his/her own electronic or paper medical records/PHI (FIU Policy and Procedure # 1660.051 (Workforce Member Access to Their Own Electronic Protected Health Information (ePHI) or PHI) or a when a Workforce member impermissibly accesses a family members' medical electronic or paper medical records/PHI (FIU Policy and Procedure #1660.052 (Workforce Members' Access to Family Members' Electronic Protected Health Information (ePHI) or PHI)).

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.
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.
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.
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/client 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 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.
Health Information	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.
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.
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.

Sanctions	Means discipline imposed for violations of the HIPAA Privacy or Security Rule, federal law, Florida state statute, or FIU policy and procedure.
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 in coordination with the Office of General Counsel and the HIPAA Hybrid Designated Component Privacy Coordinators/Liaisons 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/Liaison 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 § 164.530(e)

Related Policies

- FIU Policy and Procedure #1660.001 (Representatives)
- FIU Policy and Procedure #1660.050 (Patient Access to Protected Health Information)
- FIU Policy and procedure # 1660.085 (Sanctions)
- FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in Case of a Breach
- FIU Policy and Procedure #1660.105 (Class of Workforce Members Who Require Access to PHI)

CONTACTS

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

HISTORY

Initial Effective Date: November 6, 2023
Review Dates *(review performed, no updates)***:** N/A
Revision Dates *(updates made to document)***:** November 6, 2023

FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

Sanctions for the Impermissible Access of Self or Family Medical Records # 1660.086a

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

PROCEDURE STATEMENT

I. Sanctions may be determined using the table below as a guide.

A. The sanctions may increase with each aggravating factor. Aggravating factors may include, but are not limited to:

1. The number of records impermissibly accessed.
2. The length of time spent in the records.
3. Financial or reputational harm.
4. Reputational harm to the organization.
5. The type of records accessed (i.e., identifying information, sensitive information, etc.).
6. Past policy violations.
7. Past disciplinary actions.
8. Multiple areas of EMR accessed (i.e., labs, diagnosis, treatment plan, etc.).
9. Workforce member falsified or edited record or documentation.
10. Workforce member was dishonest or did not cooperate with the investigation.

B. The sanctions may decrease with each mitigating factor. Mitigating factors may include, but are not limited to:

1. Self-disclosure of the impermissible access.
2. The length of time spent in the records.
3. Family Member gave verbal permission to access record (confirm with the Family Member).
4. Workforce Member acted in good faith with a mistaken belief that the access/disclosure was appropriate.

Sanctions for Impermissible Accessing Self or Family Members' PHI			
Level 1 Coaching	**Level 2 Written Warning and/or 3-Day Suspension**	**Level 3 5-Day Suspension and/or Discharge from Employment**	**Level 4 Immediate Suspension and/or Discharge from Employment**
Accidental or inadvertent access of Self or Family Members' PHI (e.g., Workforce entered the incorrect record number in a search, entered a family members' record, and immediately left the record) Aggravating and mitigating factors are considered	Intentional access of Self or Family Members' PHI-limited information or areas of chart (e.g., Accessing a patient photo, identifying information) Aggravating and mitigating factors are considered	Intentional and extensive access of Self or Family Members' PHI (e.g., Intentional and excessive access of Self in violation of policy) (e.g., Intentional and excessive access of Family Members' sensitive PHI. NOTE: Sensitive PHI includes mental health, reproductive treatment and diagnosis, sexual activity diagnosis, AIDS/HIV treatment and diagnosis) Aggravating and mitigating factors are considered	Intentional and extensive access of Family Members' PHI with malicious intent for financial gain or reputational harm (e.g., Impermissibly accessing a Family Members' PHI and posting about it on social media Impermissibly accessing Self or Family Members' PHI and changing or editing documentation, removing or "zeroing" bill balances) Aggravating and mitigating factors are considered