



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	August 6, 2025	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 Florida 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 (facilities and programs).

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

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:

- Each FIU HIPAA Hybrid Designated Component (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 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 #1660.095 (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 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: November 6, 2023

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

Revision Dates (*updates made to document*): November 6, 2023; August 6, 2025.



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

INITIAL EFFECTIVE DATE: November 6, 2023	LAST REVISION DATE: August 6, 2025	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT 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 a 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

<p>Level 1 Coaching</p>	<p>Level 2 Written Warning and/or 3-Day Suspension</p>	<p>Level 3 5-Day Suspension and/or Discharge from Employment</p>	<p>Level 4 Immediate Suspension and/or Discharge from Employment</p>
<p>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</p>	<p>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</p>	<p>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</p>	<p>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</p>