FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Incidental Disclosure # 1660.135

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 (FIU) HIPAA Hybrid Designated Health Care Components (hereinafter facilities and programs) will make reasonable efforts to use or disclose the minimum amount of PHI as is necessary to accomplish the intended use or disclosure and limit the potential for "incidental disclosure" when the use or disclosure of an individual's PHI that cannot reasonably be prevented by chance or without intention or calculation during an otherwise permitted or required use or disclosure.

Facilities and programs are expected to develop procedures or protocols supplementing this policy and procedure when facility and program-specific procedures are needed. As a University-wide policy and procedure approved by the HIPAA Steering Committee, Facility and program Privacy Coordinators, the Office of Compliance and Integrity, and the Office of General Counsel, this policy and procedure takes precedence over any facility or program-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)

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, or designee 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, federal law and Florida state statutes. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

SCOPE

This policy applies to FIU's HIPAA Components (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 this policy and FIU Policy and Procedure #1660.015 regarding Business Associate Agreements.

REASON FOR POLICY

To ensure the uses and disclosures of Protected Health Information (PHI) are limited to the minimum necessary to accomplish the intended purpose as required by HIPAA and Florida state statutes and to limit incidental disclosures to situations that reasonably cannot be prevented.

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 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), including, but not limited to the use, disclosure, the minimum necessary rule, and incidental disclosures.

RELATED RESOURCES

References

- 45 CFR §164.502
- 45 CFR §164.506
- 45 CFR §164.510
- 45 CFR §164.512
- 45 CFR §164.514
- 45 CFR §164.522
- 45 CFR §164.524
- Florida Statute §95.11
- Florida Statute §456.057

Related Policies

- FIU Policy # 1610.005 (Designated Health Care Components of FIU Community)
- FIU Policy and Procedure #1660.010 (Uses and Disclosures of Protected Health Information for Marketing and the Sale of PHI)
- FIU Policy and Procedure #1660.015 (Business Associate Agreements)
- FIU Policy and Procedure #1660.020 (Uses and Disclosures of Protected Health Information That Require Patient Authorization)
- FIU Policy and Procedure #1660.025 (Uses and Disclosures for Which an Authorization or Opportunity to Agree or Object is NOT Required)
- FIU Policy and Procedure #1660.030 (Uses and Disclosures Requiring an Opportunity for the Patient to Agree or to Object)
- FIU Policy and Procedure #1660.035 (Uses and Disclosures of Protected Health Information for Fundraising)
- FIU Policy and Procedure #1660.060 (Accounting of Disclosures)
- 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)

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.

Incidental Disclosure # 1660.135a

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

PROCEDURE STATEMENT

I. Incidental Disclosures of Patient Protected Health Information (PHI)

Each 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 federal law and Florida state statutes governing the confidentiality, integrity and availability of Protected Health Information (PHI) and electronic PHI (ePHI), including, but not limited to the use and disclosure of the minimum amount of PHI necessary to accomplish the intended purpose and any incidental disclosures resulting from those uses and disclosures. Privacy Coordinators may delegate and share duties and responsibilities as necessary and appropriate but retain oversight responsibility. (See FIU Policy and Procedure #1660.070) (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)

A. Implementation of the Incidental Disclosure Standard - Workforce Members:

1. Facility and program Workforce members who use or disclose PHI must comply with the Minimum Necessary Standard (See FIU Policy and Procedure #1640.025) (Minimum Necessary) and the HIPAA administrative, technical, and physical safeguards to protect the privacy of PHI.

2. Facility and program Workforce members will take all reasonable measures necessary to avoid uses and disclosures of PHI to persons and entities who have no responsibilities or duties that require access to PHI, such as those noted in Attachment A (Frequently Asked Questions), in order to protect PHI in both paper (faxes, paper medical records) and electronic forms (ePHI). To avoid these events to the extent possible:

    a. **Workforce Members with Treatment Responsibilities** will reasonably safeguard PHI to limit the incidental uses and disclosures made to that which is necessary to carry out their treatment responsibilities. Such limitations may include:

i. to the extent possible, limit discussions about patients with other health care providers to areas which are reasonably secure and not open to the public, such as conference rooms.

ii. avoid discussions about PHI in the elevator, campus restaurants, lobbies, and other public places.

iii. to the extent possible, avoid using PHI on boards in triage areas or other areas to communicate patient status to other Workforce members. Where such boards must be used, use the patient's initials rather than the patient's name. Limit other information to the minimum necessary.

iv. for Health Care Component (facility and program) sign-in logs/sheets, limit incidental disclosure of patient's name by blocking it out after the patient has been called. If the log/sheet is retained, remove the logs/sheets periodically and store in area not opened to the public. Do not request diagnosis or treatment information on the sign in log/sheet. Speak quietly when discussing PHI in connection with your job responsibilities.

v. protect the patient's chart with a coversheet.

vi. keep curtains pulled, or doors closed, during examination and treatment.

vii. mail test results to patient in a sealed envelope rather than on a postcard.

b. **Designated Workforce Members with Billing, Collections, or Health Care Operations Responsibilities** will reasonably safeguard PHI to limit the incidental uses and disclosures made to that which is necessary to carry out their responsibilities. Such limitations may include:

i. speaking quietly when discussing protected health information in connection with your job responsibilities.

ii. to the extent possible, avoid using individuals' names, health benefit claims histories, treatment histories and diagnoses when discussing PHI within the Facility and program.

iii. avoid leaving work papers containing PHI on desks or other surfaces in plain view of others.

iv. keeping records, papers and other materials in file cabinets or drawers when not in immediate use.

II. Record/Documentation Retention

A. If a communication, action, activity, or designation is required to be documented in writing, the document or record owner 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. Frequently Asked Questions

- (Attachment A)

Attachment A – Frequently Asked Questions

1. **Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?**

Answer:

Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring health care provider to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers' primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high-quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

For example, the following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- Health care staff may orally coordinate services at hospital nursing stations.
- Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member.
- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
- A physician may discuss a patients' condition or treatment regimen in the patient's semi-private room.
- Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.
- A pharmacist may discuss a prescription with a patient over the pharmacy counter, or with a physician or the patient over the phone.

In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. However, in an emergency situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Health care providers are free to engage in communications as required for quick, effective, and high-quality health care.

2. **May physician's offices or pharmacists leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or prescription refill reminders to patients' homes?**

Answer:

Yes. The HIPAA Privacy Rule permits health care providers to communicate with patients regarding their health care. This includes communicating with patients at their homes, whether through the mail or by phone or in some other manner. In addition, the Rule does not prohibit health care providers from leaving messages for patients on their answering machines. However, to reasonably safeguard the individual's privacy, covered entities should take care to limit the amount of information disclosed on the answering machine. For example, a health care provider might want to consider leaving only its name and number and other information necessary to confirm an appointment or ask the individual to call back.

A health care provider also may leave a message with a family member or other person who answers the phone when the patient is not home. The Privacy Rule permits health care providers to disclose limited information to family members, friends, or other persons regarding an individual's care, even when the individual is not present. However, health care providers should use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed.

In situations where a patient has requested that the health care provider communicate with him in a confidential manner, such as by alternative means or at an alternative location, the health care provider must accommodate that request, if reasonable.

3. **May physician's offices use patient sign-in sheets or call out the names of their patients in their waiting rooms?**

Answer:

Yes. Health care providers may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice, for example, when other patients in a waiting room hear the identity of the person whose name is called or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the health care provider has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician).

4. **Are covered entities required to document incidental disclosures permitted by the HIPAA Privacy Rule, in an accounting of disclosures provided to an individual?**

Answer:

No. The Privacy Rule includes a specific exception from the accounting standard for incidental disclosures permitted by the Rule.

5. **Do the HIPAA Privacy Rule's provisions permitting certain incidental uses and disclosures apply only to treatment situations or discussions among health care providers?**

Answer:

No. The provisions apply universally to incidental uses and disclosures that result from any use or disclosure permitted under the Privacy Rule, and not just to incidental uses and disclosures resulting from treatment communications, or only to communications among health care providers or other medical staff. For example:

- A health care provider may instruct an administrative staff member to bill a patient for a particular procedure and may be overheard by one or more persons in the waiting room.

If the health care provider made reasonable efforts to avoid being overheard and reasonably limited the information shared, an incidental use or disclosure resulting from such conversations would be permissible under the Rule.

6. **Is a covered entity required to prevent any incidental use or disclosure of protected health information?**

Answer:

No. The HIPAA Privacy Rule does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Rule requires only that health care providers implement reasonable safeguards to limit incidental uses or disclosures.