FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Incidental Disclosure # 1660.135

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

POLICY STATEMENT

Florida International University (FIU) HIPAA Hybrid Designated Health Care Components (Components) 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.

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

Components 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 Component Privacy Coordinator will be responsible for maintaining all HIPAA documentation relevant to his/her Component. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

All Component Workforce members shall receive mandatory HIPAA Privacy and Security Rule training. (FIU Policy and Procedure #1660.075) (HIPAA Privacy and Security Rule Training)

Component 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)

Each Component must designate a HIPAA Privacy Coordinator and a HIPAA Security Coordinator. (FIU Policy and Procedure #1660.070) (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)

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 state law and regulation. (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 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 law and to limit incidental disclosures to situations that reasonably cannot be prevented.

45 CFR §164.502(a)(1)(iii)

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.
Business Associate	Generally, an entity or person who performs a function involving the use or disclosure of 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). **NOTE:** 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. **NOTE:** 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, data aggregation, management, administrative, accreditation, software support, or financial services. A Business Associates does not, however, include HIPAA Component workforce members.
Business Associate Agreement	Means a contract or other written arrangement with a business associate which must describe the permitted and required uses of PHI by the business associate; Provide that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law; and Require the business associate to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the contract.
Code of Federal Regulations	Also known as CFR is the codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the Federal Government. It is divided into 50 titles that represent broad areas subject to Federal regulation.
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.
Confidentiality	Means data or information is not made available or disclosed to unauthorized persons or processes.
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.
Disclosure	Means the release, transfer, provision of access to, or divulging in any other manner of PHI outside of the entity holding the information.
Electronic Protected Heath Information (ePHI)	PHI in electronic form. See also: PHI.
Florida Statutes	Also known as F.S. is a permanent collection of state laws organized by subject area into a code made up of titles, chapters, parts, and sections. The *Florida Statutes* are updated annually by laws that create, amend, transfer, or repeal statutory material.
Health Care Component	See "Component"

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/client; the provision of health care to an patient/client; or the past, present, or future payment for the provision of health care to an patient/client.
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
Incidental Use or Disclosure	A secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Privacy Rule.
Minimum Necessary	Using, disclosing, or requesting the minimum amount of PHI as is necessary to accomplish the intended use or disclosure.
Need-to-Know	The limiting of access to information to just that information for which an individual has a legitimate clinical or business need.
Patient	The person who is the subject of PHI.
Privacy Coordinator	Means an FIU Workforce member, appointed by the director, manager, or supervisor of a HIPAA Designated Component to conduct and/or coordinate with necessary and appropriate Workforce members all HIPAA Privacy Rule activities and actions within the Component, including but not limited to tracking HIPAA training activities; coordinating HIPAA Privacy Rule implementation; participating in HIPAA Privacy and Security Rule violation investigations, as necessary and appropriate, communicating with the Director of Compliance and Privacy for Health Affairs, the HIPAA Security Officer, and the Office of General Counsel, as necessary and appropriate, regarding HIPAA Privacy and Security Rule activities and concerns; conducting and reporting monitoring activities; participate in assessments; and responding to, tracking and documenting HIPAA Privacy Rule activities. Maintain ongoing communication with the Director of Compliance and Privacy for Health Affairs and the HIPAA Security Officer.
Protected Health Information	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. PHI, 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.
Privacy Rule	The regulations at 45 CFR 160 and 164, which detail the requirements for complying with the standards for privacy under the administrative simplification provisions of HIPAA.
Treatment	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.
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 all required University-wide Privacy Rule policies, procedures and associated forms.
   - Performs audits and assessments of the Components to ensure their compliance with the Privacy Rules and associated FIU Policies and Procedures.
   - Performs audits and assessments of the Components 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.

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), 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
- F.S. §95.11
- F.S. §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 FIU Office of Compliance & Integrity at (305) 348-2216 or the appropriate Component Privacy Coordinator. Contact information is available within the "Contact Us" tab at compliance@fiu.edu.

HISTORY

Initial Effective Date: August 31, 2021
Review Dates (*review performed, no updates*): N/A
Revision Dates (*updates made to document*): August 31, 2021

Incidental Disclosure # 1660.135a

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

PROCEDURE STATEMENT

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

Each 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 federal and state laws and regulations 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. Components 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. Component Workforce members will take reasonable steps, such as those noted in Attachment A (Frequently Asked Questions), to protect PHI in both paper (faxes, paper medical records) and electronic forms (ePHI) to avoid these events to the extent possible.

3. Workforce members will not use or disclose PHI in a manner that violates the Privacy Rule.

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. <u>Frequently Asked Questions</u>

- (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.