



**Patient Access to Protected Health Information #1660.050**

<b>INITIAL EFFECTIVE DATE:</b>	<b>LAST REVISION DATE:</b>	<b>RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT</b>
October 13, 2020	July 27, 2021	Office of Compliance and Integrity

**POLICY STATEMENT**

Each Florida International University (FIU) Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Health Care Component (Component) must provide their patients, and/or the patient’s legal representative (hereinafter “patient”) with the right to inspect and/or obtain a copy (hereinafter “access”) of the Protected Health Information (PHI) in medical and billing records (hereinafter “Designated Record Set”) about the patient which are maintained by the Component, or a Business Associate on behalf of the Component:

- For as long as the PHI is maintained in the Designated Record Set,
- Whether the PHI is maintained in paper or electronic systems onsite, remotely, or is archived, or where the PHI originated, and
- In the requested Form and Format, if it is readily producible in such Form and Format.

Patient’s may make their request for access verbally and will not be required to make their request for access is writing.

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. (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 accordingly made 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**

The policy applies to FIU’s Health Care Components that are 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 Associates Agreements.

**REASON FOR POLICY**

To establish patient right to access their PHI as described in the HIPAA Privacy Rule and state law, and to describe the steps the Components must take to grant or deny a patient’s right to access.

45 CFR §164.524 (Access of Individual’s to PHI)  
Florida Statute §456.057

**DEFINITIONS**

Terms may be found in the Policy Statement or Procedures

TERM	DEFINITIONS
<b>Access</b>	Means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any <u>system</u> resource.
<b>Administrative Officer</b>	Means the Component Workforce member responsible for financial management, human resources administration, management of facilities and equipment, and other administrative functions required to support the teaching and research missions of the FIU HIPAA Hybrid Designated Health Care Component.



	The Administrative Officer is the senior administrative staff position in the department, Division or Office and provides continuity as academic leadership changes.
<b>Administrative Safeguards</b>	Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
<b>Alternate Communication</b>	Means a communication from provider to patient by an alternative means or at an alternative location. Examples may include using an alternate mailing address or phone number; or using an alternate communication vehicle (phone, mail, text message, facsimile or email) rather than the Component's/provider's standard method of communication.
<b>Availability</b>	Means the property that data or information is accessible and useable upon demand by an authorized person.
<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, data aggregation, management, administrative, accreditation, software support, or financial services. A Business Associates does not, however, include HIPAA Component workforce members.</p>
<b>Business Associate Agreement</b>	Means a contract or other written arrangement with a business associate which must describe the permitted and required uses of protected health information by the business associate; Provide that the business associate will not use or further disclose the



	protected health information 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 protected health information other than as provided for by the contract.
<b>Breach</b>	Means the unauthorized acquisition, access, use, or disclosure of Protected Health Information (PHI) that compromises the security or privacy of the data and poses a significant risk of financial, reputational, or other harm to the client.
<b>CCF</b>	Means Center for Children and Family
<b>Code of Federal Regulations</b>	Also known as CFR
<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>Confidentiality</b>	Means data or information is not made available or disclosed to unauthorized persons or processes.
<b>Correctional Institution</b>	Means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.
<b>Covered Entity</b>	An entity that is subject to HIPAA. <ul 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> </ul> <p><b>Note:</b> FIU, the legal entity, is the Covered Entity for HIPAA compliance purposes. FIU is a Hybrid Entity, only FIU</p>



	designated Components, to the extent it performs covered functions, are subject to HIPAA requirements.
<b>Disclosure</b>	Means the release, transfer, provision of access to, or divulging in any other manner of protected health information outside of the entity holding the information.
<b>Designated Record Set</b>	<ol style="list-style-type: none"> <li>1. A group of records maintained by or for a covered entity that is: <ol style="list-style-type: none"> <li>a. The medical records and billing records about patients maintained by or for a covered health care provider;</li> <li>b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or</li> <li>c. Used, in whole or in part, by or for the covered entity to make decisions about patients.</li> </ol> </li> <li>2. For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.</li> </ol>
<b>Electronic Media</b>	<p>Means:</p> <ol style="list-style-type: none"> <li>1. Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;</li> <li>2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.</li> </ol>
<b>Electronic Protected Health Information (ePHI)</b>	PHI in electronic form. See also: <a href="#"><u>PHI</u></a> .
<b>Florida Statutes</b>	Also known as F.S. is a permanent collection of state <b>laws</b> organized by subject area into a code made up of titles, chapters, parts, and sections. ... <b>Laws of Florida</b> – a compilation of all the <b>laws</b> , resolutions, and memorials passed during a legislative session.
<b>Form and Format</b>	Refer to how the PHI is conveyed to the individual (e.g., on paper or electronically, type of file, etc.)



<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 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>U.S. Department of Health and Human Services</b>	Also known as HHS.
<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 an patient; or the past, present, or future payment for the provision of health care to an 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>Inmate</b>	Means a person incarcerated in or otherwise confined to a correctional institution
<b>Integrity</b>	Means the property that data or information have not been altered or destroyed in an unauthorized manner.
<b>Law enforcement official</b>	Means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to: <ol style="list-style-type: none"> <li>1. Investigate or conduct an official inquiry into a potential violation of law; or</li> <li>2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.</li> </ol>



<b>Patient</b>	The person who is the subject of PHI.
<b>Privacy Coordinator</b>	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.
<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: <ul 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> </ul>
<b>Privacy Rule</b>	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.
<b>Psychotherapy Notes</b>	Means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual’s medical record. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of

	the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
<b>Representative</b>	Means someone with the legal authority to act on behalf of an incompetent adult client, a minor client or a deceased client or the client’s estate in making health care decisions or in exercising the client’s rights related to the client’s protected health information.
<b>Research</b>	<p>Means any systematic investigation designed to develop or contribute to generalizable knowledge. The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual’s authorization, provided the covered entity obtains either:</p> <ul style="list-style-type: none"> <li>(1) documentation that an alteration or waiver of individuals’ authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board;</li> <li>(2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or</li> <li>(3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought. A covered entity also may use or disclose, without an individuals’ authorization, a limited data set of protected health information for research purposes.</li> </ul>
<b>Secretary</b>	Means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.
<b>Standards</b>	<p>Means a rule, condition, or requirement:</p> <ul style="list-style-type: none"> <li>1. Describing the following information for products, systems, services, or practices: <ul style="list-style-type: none"> <li>i. Classification of components;</li> <li>ii. Specification of materials, performance, or operations; or</li> </ul> </li> </ul>





	iii. Delineation of procedures; or 2. With respect to the privacy of protected health information.
<b>Treatment, payment, and healthcare operations</b>	(TPO)
<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 FIU’s compliance with the Rules.
  - Develops and maintains all required University-wide health care Privacy Rule policies, procedures and associated forms.
  - Develops and maintains HIPAA health care Privacy Rule training modules and ensures appropriate Workforce members complete the required training.
  - 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 and maintain a Privacy Rule Coordinator who will work closely with and under the direction of the Director of Compliance and Privacy for Health Affairs to overseeing and ensure 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 receiving and processing requests by patients for access to their PHI.

## RELATED RESOURCES

### References

- 45 CFR §160.306
- 45 CFR §164.502
- 45 CFR §164.514
- 45 CFR §164.522
- 45 CFR §164.530
- F.S. §456.057
- F.S. §95.11
- F.S. §394.4615

### Related Policies

- FIU Policy # 1610.005 (Designated Health Care Components of FIU Community)
- FIU Policy and Procedure #1660.005 (Right of Patients to Request Confidential Communications Regarding the Use and Disclosure of Their Protected Health Information)
- FIU Policy and Procedure #1660.015 (Business Associate Agreements)
- FIU Policy and Procedure #1660.020 (Authorization for Uses and Disclosures of Patient Protected Health Information)
- FIU Policy and Procedure #1660.040 (Verification)
- 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, [compliance@fiu.edu](mailto:compliance@fiu.edu), or the appropriate Component Privacy Coordinator.

## HISTORY

**Initial Effective Date:** October 13, 2020



FLORIDA  
INTERNATIONAL  
UNIVERSITY



**Review Dates** (review performed, no updates): n/a  
**Revision Dates:** October 13, 2020; July 27, 2021



**Patient Access to Protected Health Information #1660.050a**

<b>INITIAL EFFECTIVE DATE:</b>	<b>LAST REVISION DATE:</b>	<b>RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT</b>
October 13, 2020	July 27, 2021	Office of Compliance and Integrity

**PROCEDURE STATEMENT**

**I. Requests to Access**

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 PHI and electronic PHI (ePHI), including, but not limited to receiving and processing requests by patients, and/or their legal representatives (hereinafter “patient”) for access to the PHI contained within their Designated Record Set. Privacy Coordinators may delegate and share duties and responsibilities as necessary and appropriate but retain oversight responsibility. (FIU Policy and Procedure #1660.070) (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)

- A. When a patient requests access to PHI contained within their Designated Record Set, the Privacy Coordinator will request the patient make their request in writing by completing and submitting the Patient Request for Access to Protected Health Information in the Designated Record Set Form. (See Sample Access Form attached). However, the Privacy Coordinator will accept any written request for access if the required information and signature are provided.
- B. The Privacy Coordinator will assist the patient with completing the Access Form, if necessary.
- C. The Privacy Coordinator will not ask the patient the reason(s) for making the request for access to inspect and/or to obtain copy their PHI.
- D. The Privacy Coordinator will honor requests for alternate means of making a request for access if reasonable accommodations (such as disability or illiteracy) are needed.

**NOTE:** Although the Privacy Coordinator will request the patient to complete the Access Form, the Privacy Coordinator **MUST** accept all verbal request for access and **WILL NOT** require the patient to make his/her access request by submitting a completed Access Form or by submitting his/her request in writing.

**NOTE:** If the patient makes a verbal request for access to his/her PHI, the Privacy Coordinator must complete the Access Form, including the "For FIU Healthcare Component USE ONLY" section of the Access Form and properly secure it within the patient's medical records. In the alternative, the Privacy Coordinator may document in the patient's medical record the verbal request and all action taken by the Privacy Coordinator on the request.

- E. Upon receipt of a complete or incomplete Access Form, or other written document, the Privacy Coordinator must verify the identity of the patient making the request (FIU Policy and Procedure #1660.040) (Verification)

## **II. Incomplete Access Form**

- A. If a patient submits an incomplete Access Form, or other written document, the Privacy Coordinator will not evaluate the request for access until all required information is provided. The Privacy Coordinator will:
  - 1. Date stamp the incomplete Access Form, or other written document, on the day received;
  - 2. Document in the patient's medical records:
    - a. That the Access Form, or other written document, is incomplete;
    - b. The reason(s) the Access Form is incomplete;
    - c. The date and time the incomplete Access Form, or other written document, was received, and
    - d. The name and title of the Privacy Coordinator who received the incomplete Access Form or other written document.
  - 3. Make a photocopy of the patient's incomplete Access Form, or other written document, and
  - 4. Properly secure the photocopy of the incomplete Access Form, or other written document, in the patient's medical records.

**NOTE:** It is preferable for the Privacy Coordinator to contact the patient in-person or via the telephone and advise him/her that required information is missing and their request for access cannot be evaluated until the required information is provided, verses mailing a written notice to the patient, as mailing a written notice may unreasonably delay the patient's right to access.

- B. Prior to contacting the patient to advise him/her of the need for the missing information, the Privacy Coordinator must review the patient's Access Form, or other written document, and the medial records to identify:
  - 1. If the patient previously identified a preferred method of communication, and/or
  - 2. If the patient previously requested, and the Component agreed to communicate with the patient via alternate means or location. (FIU Policy and Procedure

#1660.05) (Right of Patients to Request Confidential Communications Regarding the Use and Disclosure of Their Protected Health Information) (hereinafter Confidential Communications)

- C. If the patient is not available in-person, or via the telephone, and had not previously requested and been approved for Confidential Communications via electronic means (e.g., email/facsimile/text message) , the Privacy Coordinator may notify the patient of the need for the missing information by sending the original incomplete Access Form, or other written document, and the Component’s Cover Letter (See Sample Cover letter Requesting Complete or Additional Information) without undue delay to the patient via the United States Postal Service First-Class Mail in an envelope that identifies the name of the Component. (e.g., Center for Children and Family)

**NOTE:** Electronic communications/means (e.g., email/facsimile/text message) are only available as an option if the patient previously requested and was approved by the Privacy Coordinator, in which event the procedures set forth for delivery and documentation are outlined in FIU Policy and Procedure #1660.005 (Confidential Communications)

- D. The Privacy Coordinator must:
1. Document in the patient’s medical records:
    - a. The date, name, and title of the Privacy Coordinator who completed the delivery, and
    - b. The method of delivery.
  2. Properly secure a copy of the incomplete Access Form, or other written document, and Cover Letter in the patient’s medical records, and
  3. If the delivery is accomplished via previously request and approved electronic communication, the Privacy Coordinator must:
    - a. Print a hardcopy of the electronic communication/means (e.g., email/facsimile/text message) and properly secure it in the patient’s medical records, and
    - b. If the delivery was completed via facsimile, print a hardcopy of the facsimile transmittal report and properly secure it in the patient’s medical records.

**III. Properly Completed Access Form**  
**Timely Action by the Component**

- A. Upon receipt of a properly completed Access Form, or other written document, the Privacy Coordinator must:
1. Date stamp receipt of the completed Access Form, or other written document, on the day received;

2. Complete the "Date Received" and "Recipient" portions of the "For FIU Entities USE ONLY" section of the Access Form;
  3. Promptly document in the patient's medical records:
    - a. Receipt of the Access Form, or other written document, and
    - b. The date, name, and title of the Privacy Coordinator who received the properly completed Access Form, or other written document, and
  4. Properly secure the original completed Access Form, or other written document, in the patient's medical records.
- B. The Privacy Coordinator and other Workforce members as necessary and appropriate will promptly review and evaluate the Access Form, other written document, or the verbal request, and determine whether to grant, delay, or deny the request for access as outlined below in Sections VIII and IX.
- C. The Privacy Coordinator must act on a request for access in a timely manner, without delays for legal review, but not greater than 30 days following receipt of a properly completed Access Form, other written document, or verbal request and determine what portion(s), if any, of the Designated Record Set the patient may access. This may mean providing access to only a portion of the Designated Record Set or making portions of it unreadable or unavailable.
- D. If the Privacy Coordinator is not able to act on the request for access within 30 days, the Privacy Coordinator may extend the time to act on the request for access by not greater than an additional 30-days, but the Privacy Coordinator must provide the patient with a written statement of the reason(s) for the delay and the date by which the Privacy Coordinator will complete its action on the request for access. (See Sample 30-Day Extension Letter attached)

**NOTE:** The Privacy Coordinator must deliver the 30-Day Extension Letter to the patient prior to the expiration of the initial 30-days.

**NOTE:** The Privacy Coordinator may have only one 30-day extension of time for action on a request for access.

**NOTE:** The preferred method of delivering the Component's 30-Day Extension Letter is in-person; however, delivery may be made to the patient via the United States Postal Serviced First-Class Mail in an envelope that identifies the name of the Component (e.g., Center for Children and Family).

- E. Prior to notifying the patient of the need for an extension of time, the Privacy Coordinator must review the patient's Access Form, or other written document, and the medical records to identify:

1. If the patient previously identified a preferred method of communication, and/or
2. If the patient previously requested, and the Component agreed to communicate with the patient via alternate means or location. (FIU Policy and Procedure #1660.005) (Confidential Communications)

**NOTE:** Electronic communications/means (e.g., email/facsimile/text message) are only available as an option if previously requested by the patient and approved by the Privacy Coordinator in which event the procedures set forth for delivery and documentation are outlined in FIU Policy and Procedure #1660.005 (Confidential Communications).

F. The Privacy Coordinator must:

1. Document in the patient's medical records:
  - a. The date, name, and title of the Privacy Coordinator who completed the delivery of the 30-Day Extension Letter, and
  - b. The method of delivery.
3. Properly secure a copy of the 30-Day Extension Letter in the patient's medical records, and
4. If the delivery is accomplished via previously requested and approved electronic communication, the Privacy Coordinator must:
  - a. Print a hardcopy of the electronic communication (i.e., email/facsimile/text message) and properly secure it in the patient's medical records, or
  - b. If the delivery was completed via facsimile, print a hardcopy of the facsimile transmittal report and properly secure it in the patient's medical records.

**IV. Approval of Request for Access (in whole)**

- A. The Privacy Coordinator will provide the patient with access to his/her PHI in the Form and Format requested, if it is readily producible, unless there is reasonable cause to deny the request.
- B. The Privacy Coordinator will contact the patient to discuss the Form and Format of access and inform the patient of any cost-based fees that will be charged if the patient requests a copy of the PHI (or agrees to receive a summary or explanation of the information).
- C. The preferred method of contacting the patient is in-person; however, delivery may be made to the patient via the United States Postal Serviced First-Class Mail in an envelope that identifies the name of the Component (e.g. Center for Children and Family).
- D. Prior to notifying the patient to advise him/her of the approval and to discuss the Form and Format of access and any cost-based fees, the Privacy Coordinator must review the



patient's Access Form, other written document, or verbal request and the medical records to identify:

1. If the patient previously identified a preferred method of communication, and/or
2. If the patient previously requested, and the Component agreed to communicate with the patient via alternate means or location. (FIU Policy and Procedure #1660.005) (Confidential Communications).

**NOTE:** Electronic communications (e.g., email/facsimile/text message) are only available as an option if previously requested by the patient and approved by the Privacy Coordinator in which event the procedures set forth for delivery and documentation are outlined in FIU Policy and Procedure #1660.005 (Confidential Communications).

- E. The Privacy Coordinator must document in the patient's medical records:
1. The name and title of the Privacy Coordinator who discussed and verified the Form and Format of access and relevant fees and actual cost, associated with the request for which the patient was advised, which may include, but are not limited to:
    - a. Labor for copying the PHI requested, whether in paper or electronic form,
    - b. Supplies for creating the paper copy or electronic media (e.g., CD or USB drive) if the patient requests the electronic copy be provided on portable media,
    - c. Labor cost for preparation a written explanation or summary of the PHI, if requested and agreed to by the patient, and
    - d. Postage, if the patient requests that the copy, electronic media, or written summary or explanation be mailed.
  2. The Form and Format of access requested and agreed to, and
  3. The total estimated fees.

**NOTE:** After discussing the Form and Format and relevant and estimated fees, the patient may modify or withdraw his/her request. The patient must provide an updated Access Form, other written document or verbal request to reflect any modifications or a withdrawal of his/her request. The Privacy Coordinator must update the Access Form or medical records to reflect any modifications made to the initial request.

**NOTE: C.C.F., Psychiatry, and Psychology ONLY.** The Privacy Coordinator will contact the identified clinician and/or supervisor (hereinafter Clinician) to verify the appropriateness of the patient's request for the following items:

1. Initial Psychiatric Evaluation (Must contact the Medical Director and/or ARPN);
2. Biopsychosocial, Spiritual, Risk Assessments, and
3. Any reports or assessment that were not generated by the health care Components (i.e. C.C.F., Psychiatry, and/or Psychology)

**NOTE:** If the request for access to the PHI contained with the medical record is denied in-whole or in-part to one or more of the three (3) items identified immediately above, review Sections V, VI, VII, VIII below for guidance regarding reviewable and non-reviewable grounds of a denial and how to proceed with the patient's request for access.

**NOTE:** If the **NOTES** immediately above are applicable, the Privacy Coordinator must document in the patient's medical record:

1. The date, name, and title of the Privacy Coordinator who contacted the identified Clinician(s) to verify the appropriateness of the access, and
2. The name and title of the Clinician(s) who approved or denied access in-whole or in-part to any or all of the three (3) items contained within the patient's medical records.

**NOTE:** A patient's complete psychiatric records shall be provided directly to a subsequent treating psychiatrist upon a patient's written request for complete copies. F.S. 456.057(6)

- F. When a patient's request for access is approved in-whole to PHI contained within the Designated Record Set, the Privacy Coordinator must:
1. Notify the patient of the approval of the access request in a timely manner, without delays for legal review, but not greater than 30 days of receipt of the request (or no later than within 60 calendar days if the Component notified the patient of an extension);
  2. Provide the patient access to his/her PHI in the Form or Format requested, if it is readily producible in such Form or Format;
  3. Document in the patient's medical records:
    - a. The name and title of the Privacy Coordinator who completed the notification, and
    - b. The date and method of notification.
  4. Properly secure a copy of the completed Access Form within the patient's medical records.
- G. If the patient requests that PHI contained within his/her Designated Record Set be delivered via the United States Postal Service, or any other reasonably available carrier (e.g., Registered or certified Mail, FedEx, etc.), the Privacy Coordinator must:
1. Verify the patient's mailing address in the patient's medical records, or utilize the mailing address as provided on the Access Form, or other written document;
  2. Complete the "Date Access Provided" portions of the "For FIU Healthcare Component USE ONLY" section of the Access Form;
  3. Mail the documents, via the United States Postal Service First-Class Mail, unless the patient requested otherwise (e.g. Registered or Certified Mail, FedEx, etc.), to the mailing address provided on the Access Form, or other written document;

4. Secure the Certified, Registered, or other mail delivery receipt/ documents in the patient's medical records;
5. Document in the patient's medical records the date, name, and title of the Privacy Coordinator who mailed the documents to the patient;
6. Document in the patient's medical record the date the Certified, Register, or other delivery documentation was returned to the Component, and
7. Properly secure the certified, registered, or other documentation in the patient's medical records.

H. If the patient has requested an in-person review of the PHI contained within his/her Designated Record Set, the Privacy Coordinator must:

1. Contact the patient via their preferred method or as identified on the Access Form, other written document, or verbal request, and schedule a convenient time and location to meet with the patient;
2. Document in the patient's medical records:
  - a. The agreed upon scheduled meeting time and location, and
  - b. The name and title of the Privacy Coordinator who scheduled the time and location to meet with the patient.
3. Be present during the review, and
4. Document the access review in the patient's medical records.

**NOTE:** The patient may take notes of the information contained within the Designated Record Set, but the Privacy Coordinator **will not** explain the PHI contained within the Designated Record Set.

I. If the patient request and explanation of some or all of the PHI contained within the Designated Record Set, the Privacy Coordinator must:

1. Contact the identified healthcare provider associated with the PHI and coordinate a date, time, and location for the access review;
2. Document in the patient's medical records:
  - a. The method(s) and date(s) each relevant healthcare provider was contacted, and
  - a. The agreed upon date, time, and location for the access review.
3. Properly secure within the medical record any hardcopy or email communications sent to each healthcare provider and the patient;
4. Document in the patient's medical records:
  - a. The name and title of the Privacy Coordinator who scheduled the date, time, and location of the access review.
5. Be present during the access review, if necessary and appropriate, and
6. Document in the patient's medical records the access review.

**V. Denial of Request for Access (in whole)**

- A. If the Privacy Coordinator denies the patient's request for access in whole to the Designated Record Set, he/she must:
1. Provide the patient a timely, written denial in plain language no later than within 30 calendar days of receipt of the request (or no later than within 60 calendar days if the Component notified the patient of an extension) which contains:
    - a. The basis for the denial (See Reviewable and Non-Reviewable grounds in Sections VIII and IX below), and
    - b. A description of how the patient may complain to the Component, the FIU Office of Compliance and Integrity, and/or the Secretary of the Department of Health and Human Services. (FIU Policy and Procedure #1660.065) (Complaints Under the HIPAA Privacy Rule, Mitigation, Refraining from Intimidating or Retaliatory Acts, and Waiver) The description must include the name, or title, and telephone number of the Component Privacy Coordinator and the Director of Compliance and Privacy for Health Affairs with the Office of Compliance and Integrity. (See Sample Letter Denying Individual's Request to Obtain a Copy of Protected Health Information attached) (Denial Letter)

**NOTE:** The basis of denial is either "Reviewable" or "Non-Reviewable". See guidance below in Sections VIII and IV.

- B. The preferred method of delivery of the written statement to the patient is in-person; however, delivery may be made to the patient via the United States Postal Serviced First-Class Mail in an envelope that identifies the name of the Component (e.g., Center for Children and Family).
- C. Prior to contacting the patient to advise him/her of the denial, the Privacy Coordinator must review the patient's Access Form, or other written document, and the medical records to identify:
1. If the patient previously identified a preferred method of communication, and/or
  2. If the patient previously requested, and the Component agreed to communicate with the patient via alternate means or location. (FIU Policy and Procedure #1660.005) (Confidential Communications)

**NOTE:** Electronic communications/means (e.g., email/facsimile/text message) are only available as an option if previously requested by the patient and approved by the Privacy Coordinator in which event the procedures set forth for delivery and documentation are outlined in FIU Policy and Procedure #1660.005 (Confidential Communications).

- D. The Privacy Coordinator must:
1. Document in the patient's medical records:
    - a. The date, name, and title of the Privacy Coordinator who completed the delivery of the Denial letter, and

- b. The method of delivery.
2. Properly secure a copy of the Denial Letter in the patient's medical record, and
3. If the delivery is accomplished via previously approved electronic communication, the Privacy Coordinator must:
  - a. Print a hardcopy of the electronic communication (e.g., email/facsimile/text message) and properly secure it in the patient's medical records, or
  - b. If the delivery was completed via facsimile, print a hardcopy of the facsimile transmittal report and properly secure it in the patient's medical records.

## **VI. Review of a Denial of Access**

- A. If the basis for the denial is reviewable, the Privacy Coordinator must provide the patient with a written statement of the review rights, including a description of how the patient may exercise such review rights. (See Section V above) (Denial Letter)
- B. If the request for access is denied in whole on a ground(s) permitted under this section, the patient has the right to have the denial reviewed. The Privacy Coordinator must designate a licensed health care professional (hereinafter Designated Reviewing Official) who was not directly involved in the original decision to deny access to review the appropriateness of the initial decision to deny access.
- C. If the patient requests a review of the denial, the Privacy Coordinator must:
  1. Promptly refer the request for review to the Designated Reviewing Official who must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards identified in Section VIII (Reviewable Grounds for Denial) immediately below, and
  2. Document in the patient's medical records:
    - a. The date, name, and title of the Privacy Coordinator who contacted and arranged review by the Designated Reviewing Official;
    - b. The name and title of the Designated Reviewing Official, and
    - c. The agreed upon date, time, and location for the scheduled review.
- D. The Designated Reviewing Official must within a reasonable period of time:
  1. Determine whether to affirm, reverse, or modify in-whole or in-part, the initial denial of access requested, and
  2. Provide a written response to the Privacy Coordinator identifying if the initial denial is affirmed, reversed, or modified, in-whole or in-part, and if the initial denial is modified or reversed in-whole or in-part, and must identify in writing the extent and manner of the modification or reversal.
- E. Upon receipt of the Designated Reviewing Official's written response, the Privacy Coordinator must:
  1. Date stamp receipt of the written response on the day received;

2. Document in the patient's medical records:
    - a. Receipt of the written response, and
    - b. The date, title, and name of the Privacy Coordinator who received the written response.
  3. Promptly provide the patient with a copy of the Reviewing Official's written response via US Mail, in-person delivery, or electronic communication if previously requested and approved by the Privacy Coordinator (FIU Policy and Procedure #1660.005) (Confidential Communications), and
  4. Properly secure the Designated Reviewing Official's original written response in the patient's medical records.
- F. Prior to contacting the patient to advise him/her of the denial, the Privacy Coordinator must review the patient's Access Form, or other written document, and the medical records to identify:
1. If the patient previously identified a preferred method of communication, and/or
  2. If the patient previously requested, and the Component agreed to communicate with the patient via alternate means or location. (FIU Policy and Procedure #1660.005) (Confidential Communications)

**NOTE:** Electronic communications/means (e.g., email/facsimile/text message) are only available as an option if previously requested by the patient and approved by the Privacy Coordinator in which event the procedures set forth for delivery and documentation are outlined in FIU Policy and Procedure #1660.005 (Confidential Communications).

- G. If the Designated Reviewing Official approves access in-whole or in-part, the Privacy Coordinator must provide the level of access as approved by the Designated Reviewing Official. The Privacy Coordinator must follow the procedures as outlined in Section IV.

## **VII. Denial of Access In-Part**

- A. If the Privacy Coordinator denies the patient's request for access in-part to the Designated Record Set, he/she must:
1. Complete the Response section of the Access Form and to the extent possible:
    - a. Provide the patient a timely, written denial in plain language which contains:
      1. The basis for the denial, and
      2. A description of how the patient may complain to the Component, the Office of Compliance and Integrity, and/or the Secretary of the Department of Health and Human Services. (FIU Policy and Procedure #1660.065) (Complaints Under the HIPAA Privacy Rule, Mitigation, Refraining from Intimidating or Retaliatory Acts, and Waiver) The description must include the name, or title, and telephone number of the Component Privacy Coordinator and the FIU Director of Compliance and Privacy for Health

Affairs with the Office of Compliance and Integrity (See Sample Letter Denying Individual's Request to Obtain a Copy of Protected Health Information attached) (Denial Letter)

- b. Provide the patient access to any remaining PHI for which access was not denied,
- c. Document the actions taken as outlined in Section IV above, and
- d. Adhere to the review process, procedure and, documentation requirements for those in-part denials that are reviewable as outlined in Sections V. and VI. above.

**NOTE:** Complexity in segregating the PHI does not excuse the obligation to provide access to the PHI to which the ground for denial does not apply.

VIII. **Reviewable Grounds for Denial**

- A. The Privacy Coordinator may deny a patient access to his/her PHI, as long as the patient is provided an opportunity to have the denial reviewed in the following circumstances:
  - 1. The Component's licensed health care professional has determined, in the exercise of professional judgment, that the access to the PHI requested is reasonably likely to endanger the life or physical safety of the patient or another person.

Ex: Emotionally Unstable:

If the patient is emotionally unstable (in the judgment of the health care professional) and access to inspect or obtain a copy of the PHI (in whole or in part) may cause the patient to harm him/herself or others.

(Florida Statute §394.4615(11) (Mental Health Clinical Records) provides: Patients shall have reasonable access to their clinical records, unless such access is determined by the patient's physician to be harmful to the patient. If the patient's right to inspect his or her clinical record is restricted by the facility, written notice of such restriction shall be given to the patient and the patient's guardian, guardian advocate, attorney, and representative. In addition, the restriction shall be recorded in the clinical record, together with the reasons for it. The restriction of a patient's right to inspect his or her clinical record shall expire after 7 days but may be renewed, after review, for a subsequent 7-day period.

- 2. The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that accessing or obtaining the requested PHI is reasonably likely to cause substantial harm to such other person.

3. The request for access to inspect or obtain a copy of a patient's PHI is made by the patient's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of accessing the PHI by such personal representative is reasonably likely to cause substantial harm to the patient or another person.

#### **IX. Unreviewable Grounds for Denial**

- A. The Privacy Coordinator may deny a patient access to his/her PHI without providing the patient an opportunity for review, in the following circumstances:

1. Psychotherapy Notes

Do not share any psychotherapy notes with the patient. This reason for denial is not reviewable. (This is an exception to the patient's right to access)

2. A covered entity that is a correctional institution or a covered healthcare provider acting under the direction of the correctional institution, if obtaining such copy would jeopardize the health, or safety, security, custody or rehabilitation of the patient of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

**NOTE:** FIU and the Health Care Components are not a correction institution or acting under the direction of a correctional institution.

3. Legal Matters

Do not share any material, which is compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding (i.e., audits or investigations). However, the underlying information should be shared. For example, documents being prepared specifically for a lawsuit regarding the way that the Component treated a patient should not be shared, but the patient's diagnosis and treatment can be disclosed. (Always consult with the Office of General Counsel and the Office of Compliance and Integrity prior to providing access to the PHI in this circumstance.) This reason for denial is not reviewable. (This is an exception to the patient's right to access)

4. Treatment-Related Research

The PHI was created or obtained in the course of treatment-related research for which access has been temporally suspended for as long as the research is in



progress, provided the patient agreed to the denial of access when consenting to participate in the research and the Component health care provider informed the patient that the right to access will be reinstated upon completion of the research.

5. Privacy Act of 1974, 5 U.S.C. §552a

A patient's access to PHI that is contained in records that are subject to the Privacy Act of 1974, 5 U.S.C. §552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law. (i.e., certain records under the control of a federal agency, which may be maintained by a federal agency or a contractor to a federal agency) (Always consult with the Office of General Counsel and the Office of Compliance and Integrity)

6. Protecting Confidential Sources of Information

A patient's access to his or her PHI may be denied if it is determined that the Designated Records Set contains any information obtained by a Component from confidential sources other than a health care provider under a promise of confidentiality, and the access requested would be reasonably likely to reveal the source of the information. (e.g., a family member of the patient). Keep this information and the source of the information confidential. (Always consult with the Office of General Counsel and the Office of Compliance and Integrity prior to providing access to the PHI.)

7. Confidential Communications

If a patient has asked for Confidential Communications of their PHI which was approved by the Component, (See FIU Policy and Procedure #1660.05) (Right of Patients to Request Confidential Communications Regarding the Use and Disclosure of Their Protected Health Information), the Privacy Coordinator will not use or disclose the patient's PHI in a manner that violates the agreed upon method or manner of communication and will not provide access to a representative (See FIU Policy and Procedure #1660.001 (Representatives), or any other person(s) or entity as requested by the patient and approved by the Component (FIU Policy and Procedure #1660.045) (Right of Patients to Request Restrictions Regarding the Use and Disclosure of Their Protected Health Information), unless prior, written approval has been obtained from the patient. Disclose to the Representative only that portion of the Designated Record Set that the patient authorized.

8. The PHI is NOT part of the Patient's Designated Record Set

**NOTE:** If a Component does not maintain the PHI that is the subject of the patient's request for access, and the Privacy Coordinator knows where the requested information is maintained, the Privacy Coordinator must inform the patient where to direct the request for access. (See Denial Letter)

**NOTE:** If the patient's request for access instructs the Component to send a copy of their PHI directly to another individual or entity designated by the patient, the Privacy Coordinator must provide/send within 30-days, a copy to the individual or entity designated by the patient.

**NOTE:** The patient's request must be in writing, be signed by the patient, and clearly identify the designated individual or entity and where and how to send the copy of the PHI. (See Authorization for Uses and Disclosures of Patient Protected Health Information. FIU Policy and Procedure #1660.020)

B. The Privacy Coordinator must:

1. Date stamp receipt the written request;
2. Promptly document receipt of the written request in the patient's medical records;
3. Properly secure the written request in the patient's medical records;
4. Promptly mail the PHI to the address provided by the patient, via First-Class U.S. Mail;
5. Document in the patient's medical record:
  - a. The date, title, and name of the Privacy Coordinator who received the request and mailed the PHI to the identified third party or entity, and
6. If the PHI was mailed Certified Mail-Return Receipt, upon receipt of the Return Receipt, document the receipt, and properly secure the Return Receipt in the patient's medical records.

**NOTE:** If the US Postal Service returns the patient documents (PHI) as undeliverable for any reason, the Privacy Coordinator must:

1. Document in the patient's medical records:
  - a. The date the US Mail containing the patient PHI was returned, and
  - b. The title and name of the Privacy Coordinator who received the US Mail containing the patient PHI.
2. Attempt to contact the patient via his/her preferred method and manner;
3. Document the attempt/contact in the patient's medical records;
4. Provide the patient with an opportunity to obtain the requested documents through another means, (See FIU Policy and Procedure #1660.005 (Confidential Communications));
5. Document the agreed upon method;
6. Resend the PHI to the patient via the agreed upon method, and
7. Document the date and process of delivery utilized.

**X. 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 Office of Compliance and Integrity or the Component) 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)

**XI. Frequently Asked Questions**

- A. Attachment A

**XII. Forms**

- Sample Patient Request for Access to PHI Form
- Sample Cover Letter Requesting Additional or Complete Information
- Sample Letter Notifying Individual of Need for 30-Day Extension
- Sample letter Denying Individuals Request to Obtain a Copy of PHI