FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Verification #1660.040

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 13, 2020	October 13, 2020	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 verify the identity of a person requesting access to or the disclosure of patient Protected Health Information (PHI) and the authority of any such person to access or request disclosure of patient PHI, if the identity or authority of the person is not known to the Component Workforce member receiving the request; and obtain any documentation, statements, or representations, whether oral or written, from the person requesting access to or the disclosure of the patient PHI when such documentation, statement, or representation is a condition of the disclosure.

As a University-wide policy and procedure, 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

This policy applies to FIU's HIPAA 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 Associate Agreements.

REASON FOR POLICY

This policy describes the policy and procedures required to verify the identify and authority of a person requesting access to or the disclosure a patient's PHI and the procedures for approving and denying a request for access or disclosure.

45 CFR §164.514 (Other Requirements Relating to Uses and Disclosures of PHI-Verification)

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.
Administrative Officer	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.
Administrative Safeguards	Are 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.
Authority	Refers to the basis upon which the person claims to have access to the protected health information. (Also see **Identity**)

Authorization (HIPAA Authorization)	Means a specific type of permission given by the client to use and/or disclose protected health information about the client. Workforce members must use the FIU Authorization Form for client requests.
Availability	Means the property that data or information is accessible and useable upon demand by an authorized person.
Business Associate	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). **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 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.
Breach	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.
Code of Federal Regulations	Also known as CFR

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.
Designated Record Set	Means: 1. A group of records maintained by or for a covered entity that is: a. The medical records and billing records about clients maintained by or for a covered health care provider; b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or c. Used, in whole or in part, by or for the covered entity to make decisions about clients. 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.
Disclosure	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.
Electronic Protected Heath Information (ePHI)	PHI in electronic form. See also: PHI.
Emancipated Minor	Means a minor who is to be treated as an adult for purposes of this policy. An emancipation order allows a minor to consent to "medical, dental or psychiatric care, without parental consent, knowledge or liability."
Florida Statutes	Also known as F.S.

Health Care	Means the care, services, or supplies related to the health of a patient, including: 1. preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of a patient or that affects the structure or function of the body; and 2. sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
Health Care Component	See "Component"
Health Care Operations	Means any of the following activities: 1. quality assessment and improvement activities, including case management and care coordination; 2. competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; 3. conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; 4. specified insurance functions, such as underwriting, risk rating, and reinsuring risk; 5. business planning, development, management, and administration; and 6. business management and general administrative activities of the entity, including but not limited to: a. de-identifying protected health information, b. creating a limited data set, and c. certain fundraising for the benefit of the covered entity.
Health Care Provider	Means a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
U.S. Department of Health and Human Services	Also known as HHS.
Health Information	Means any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an patient; the provision of health care to an patient; or the past, present, or future payment for the provision of health care to an patient.

HIPAA	Means the Health Insurance Portability and Accountability Act of 1996.
Hybrid Covered Entity	Means a single legal entity that performs both covered and non-covered functions. The entity has a defined health care component that engages in HIPAA electronic transactions.
In loco parentis	Means a person or institution acting in lieu of a parent.
Identity	Refers to who the person is. (Also see **Authority**).
Individually Identifiable Health Information	Means information that is a subset of health information, including demographic information collected from an individual, and 1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and 2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and a. That identifies the individual; or b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Integrity	Means the property that data or information have not been altered or destroyed in an unauthorized manner.
Law Enforcement Official	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: 1. Investigate or conduct an official inquiry into a potential violation of law; or 2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
Legally Authorized Representative	Means person authorized either by state law or by court appointment to make decisions, including decisions related to health care, on behalf of another person, including someone who is authorized under applicable law to consent on behalf of a prospective subject to the subject's participation in the procedure involved in the research.
Patient	The person who is the subject of the PHI.
Person	Means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.
Personal Representative	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.
Physical Safeguards	The physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
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 (PHI)	Means any individually identifiable health information collected or created in the course of the provision of health care services by a covered entity, in any form (written, verbal or electronic). PHI relates to the past, present, or future physical or mental health or condition of an individual or the past, present, or future payment for the provision of health care to an individual. Protected Health Information however specifically excludes: 1. Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g ("FERPA"); 2. Records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and 3. Employment records held by a covered entity in its role as an employer.
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.
Record	Means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or on behalf of a Component.

Subcontractor	Means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
Technical Safeguards	Means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
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.
Secretary	Means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.
Standard	Means a rule, condition, or requirement: 1. Describing the following information for products, systems, services, or practices: a. Classification of components; b. Specification of materials, performance, or operations; or c. Delineation of procedures; or 2. With respect to the privacy of protected health information.
Treatment, payment, and healthcare operations	Also known as TPO
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.
Unemancipated Minor	Means a person under 18 years of age and not previously married; not in the Armed Services; not previously emancipated by court proceedings initiated by the parents or the State and in the care and control of the parents.
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 and procedures.
    - 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 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 verifying the identify and authority of an individual or entity seeking to use or disclose a patient's PHI.

RELATED RESOURCES

References

- 45 CFR §164.502
- 45 CFR §164.508
- 45 CFR §164.510
- 45 CFR §164.514
- 45 CFR §164.522
- 45 CFR §164.524
- 45 CFR §164.530
- F.S. §456.057
- F.S. §95.11

Related Policies

- FIU Policy # 1610.005 (Designated Health Care Components of FIU Community)
- 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 #1660.085 (Sanctions)
- FIU Policy and Procedure #1610.020 (Business Associate Agreements)
- FIU Policy and Procedure #1660.080 (Policies and Procedures, Changes to Policies and Procedures, and Documentation)
- FIU Policy and Procedure #1640.025 (Minimum Necessary)
- FIU Policy and Procedure #16460.020 (Authorization for Use and Disclosure of Patient Protected Health Information)
- FIU Policy and Procedure #1660.030 (Use and Disclosure of Patient Protected Health Information Requiring an Opportunity for the Patient to Agree or Object)
    - Use and Disclosure for Facility Directory and to the Clergy
    - Use and Disclosure to Individuals Involved in the Patients Case and for Notification Purposes
- FIU Policy and Procedure #1660.025 (Uses and Disclosures of Protected Health Information for Which an Opportunity to Agree or to Object is NOT Required)
- FIU Policy and Procedure #1660.045 (Right of Patients to Request Restrictions Regarding the Use and Disclosure of Their Protected Health Information)
- FIU Policy and Procedure #1660.050 (Patient Access to Protected Health Information)

CONTACTS

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

HISTORY

Initial Effective Date: October 13, 2020
Review Dates (review performed, no updates): n/a
Revision Dates: October 13, 2020

Verification #1660.040a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 13, 2020	October 13, 2020	Office of Compliance and Integrity

PROCEDURE STATEMENT

I. Verification

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 state laws and/or regulations governing the confidentiality, integrity and availability of Protected Health Information (PHI) and electronic PHI (ePHI), including, but not limited to verifying the identity and authority of the person requesting access to and/or disclosure of Protected Health Information (PHI). Privacy Coordinators may delegate and share duties and responsibilities with Workforce members 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)

NOTE: Identity refers to who the person is; Authority refers to the basis upon which the person claims to have access to the PHI.

A. Prior to providing access to and/or the disclosure of PHI, the Privacy Coordinator must verify:
   1. The identity of the person requesting access to and/or the disclosure of patient PHI,
   2. The authority of such person to access, receive, and/or request disclosure of patient PHI,
   3. Whether the patient has requested restriction(s) on the disclosure of his/her PHI which the Component has approved (FIU Policy and Procedure #1660.045) (Right of Patients to Request Restrictions Regarding the Use and Disclosure of Their protected Health Information) (Restrictions),
   4. Whether the patient has requested confidential communications which the Component has approved, (FIU Policy and Procedure #1660.005) (Right of Patients to Request Confidential Communications Regarding the Use and Disclosure of Their Protected Health Information) (Confidential Communications)
   5. Review the Minimum Necessary Standards regarding access and disclosure, (FIU Policy and Procedure #1640.025) (Minimum Necessary)
   6. Review the Use and Disclosure of Patient Protected Health Information Requiring an Opportunity for the Patient to Agree or Object

- Use and Disclosure for Facility Directory and to the Clergy
- Use and Disclosure to Individuals Involved in the Patients Case and for Notification Purposes (FIU Policy and Procedure #1660.030), and

7. Review the Uses and Disclosures of Patient Protected Health Information for Which and an Authorization or Opportunity to Agree or Object is NOT Required. (FIU Policy and Procedure #1660.025)

B. In situations, in which a particular form of verification is not prescribed by the HIPAA regulations or state law, the Privacy Coordinator or designee shall utilize the following methods of verification:

1. Verification of Identity When a Patient is Requesting their PHI in Person

A. If the patient is known to the Privacy Coordinator, then no further verification procedure need be undertaken.
   1. The Privacy Coordinator must:
      a. Record in the patient's Designated Record Set the identity of the patient requesting access to and/or the disclosure of his/her PHI and how the Privacy Coordinator verified the patient's identity. (i.e., personal knowledge) (FIU Policy and Procedure #1660.050) (Patient Access to Protected Health Information) (Access)

B. If the person is not known to the Privacy Coordinator, then the Privacy Coordinator must verify the identity of the person. (FIU Policy and Procedure #1660.050) (Access)

   1. The Privacy Coordinator must:
      a. Ask the person to provide a picture identification, such as a driver's license, passport, or other government issued identification, or an employment identification, and
      b. If the person does not have picture identification, ask the person for a Social Security card or birth certificate.

   2. The Privacy Coordinator must:
      a. Make a photocopy of all identification and documentation provided,
      b. Record in the patient's Designated Record Set:
         1. The date, name, and title of the Privacy Coordinator who responded to the request,
         2. The method and manner used to verify the person's identification,
         3. The type of identification or other documentation provided, and
      c. Compare, verify, and document the accuracy of the information and documentation provided with the information contained within the patient's Designated Record Set,

d. Properly secure the copied identification or other documentation received in the patients Designated Record Set.

3. If the Privacy Coordinator has any concerns or reservation with the accuracy of the information provided and the information contained within the Designated Record Set, the Privacy Coordinator must:
   a. Inform the person that some or all of the information provided is inconsistent with the some or all of the information contained within the Designated Record Set,
   b. Provide the person and opportunity to explain the reason for the inconsistency, and
   c. If the person does not provide a satisfactory reason for the inconsistency, the Privacy Coordinator will:
      1. Delay granting the person access to and/or the disclosure of the requested PHI,
      2. Immediately contact the Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity, for guidance and instructions on how to proceed, and
      3. Document in the patient's Designated Record Set:
         a. The reason for the concern or reservation,
         b. The response(s) the person provided, and
         c. The request for assistance and guidance from the Office of Compliance and Integrity.

NOTE: Do not send email or other electronic communications/questions containing patient PHI to the Office of Compliance and Integrity.

2. Verification of Identity When a Patient is Requesting Their PHI via the Telephone

A. Prior to disclosing PHI over the telephone, including appointment reminders, the Privacy Coordinator must make reasonable efforts to verify the identity of the person with whom he/she is speaking by:
   1. Ask the person for their name, home address, phone number, date of birth, and dates of treatment, and/or medical record number.

B. The Privacy Coordinator must:
   1. Document in the patient's Designated Record Set:
      a. The date, name, and title of the Privacy Coordinator who spoke with the person claiming to be the patient,
      b. The reasonable efforts made to verify the identity of the person claiming to be the patient,

c. The specific information provided in response to the questions asked by the Privacy Coordinator or designee, and

2. Compare, verify, and document the accuracy of the information provided with that contained in the patients Designated Record Set.

C. If the Privacy Coordinator has any concerns or reservation with the accuracy of the information provided and the information contained within the Designated Record Set, the Privacy Coordinator or designee must:

1. Inform the person that some or all of the information provided is inconsistent with the some or all of the information contained within the Designated Record Set.
2. Provide the person and opportunity to explain the reason for the inconsistency.
3. If the person does not provide a satisfactory reason for the inconsistency, the Privacy Coordinator or designee will:
   a. Delay granting the person access to or disclosing any PHI,
   b. Immediately contact the Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity, for guidance and instructions on how to proceed, and
   c. Document in the patient's/patient's Designated Record Set:
      1. The reason for the concern or reservation,
      2. The responses the person provided, and
      3. The request for assistance and guidance from the Office of Compliance and Integrity.

NOTE: Do not send email or other electronic communications/questions containing patient PHI to the Office of Compliance and Integrity.

4. Verification of Identity When a Patient Provides a Copy of an Authorization, or the Authorization is Received via Facsimile, or other Electronic Means

A. The Privacy Coordinator may use or disclose PHI pursuant to a copy of a valid and signed Authorization, including a copy that is received via facsimile or other electronic means.

1. The Privacy Coordinator or designee must:
   a. Record in the patient's Designated Record Set:
      1. The date, time, name and title of the Privacy Coordinator or designee who received the Authorization,
      2. The manner in which it was received,
      3. Compare, verify, and document the accuracy of the information contained within the Authorization and the information contained within the patient's Designated Record Set, and

b. Properly secure the Authorization in the patient's Designated Record Set.

B. If the Privacy Coordinator has any concerns or reservation with the accuracy of the information contained within the Authorization and the information contained within the Designated Record Set, the Privacy Coordinator must:
   1. Contact the person through their preferred method of communication and inform them that some or all of the information provided is inconsistent with the some or all of the information contained within the Designated Record Set. Without providing details about the information contained within the Designated Record Set, the Privacy Coordinator will provide the person and opportunity to explain the reason for the inconsistency. If the person does not provide a satisfactory reason for the inconsistency, the Privacy Coordinator will:
   2. Delay granting the person access to or disclosing any PHI,
   3. Immediately contact the Office of Compliance and Integrity for guidance and instructions on how to proceed, and
   4. Document in the patient's Designated Record Set:
      a. The reason for the concern or reservation,
      b. The responses the person provided, and
      c. The request for assistance and guidance from the Office of Compliance and Integrity.

NOTE: Do not send email or other electronic communications/questions containing patient PHI to the Office of Compliance and Integrity.

5. Verification of the Identity and Authorization of a Personal Representative of an Adult or Emancipated Minor

A. If a person asserts that they are the patient's Personal Representative, but the person is not known to the Privacy Coordinator, then the Privacy Coordinator or designee must:
   1. Ask the person to provide a driver's license, passport, other government issued identification, employment identification, or
   2. If a picture identification is not available, ask for the person's Social Security card or birth certificate.

B. The Privacy Coordinator must:
   1. Make a photocopy of all identification and other documentation provided and record in the patients Designated Record Set:
      a. The date, name, and title of the Privacy Coordinator who verified the person's identity,

b. The method and manner in which the Privacy Coordinator verified the person's identity,
c. The type of identification or other documentation received, and

2. Properly secure the copied identification or other documentation in the patient's Designated Record Set.

C. Once the person's identity has been established, the Privacy Coordinator or designee may establish the person's authority to act on behalf of the patient by confirming that the person is named in the patient's Designated Record Set as the patient's Representative. (FIU Policy and Procedure #1660.001) (Representatives)

D. If the person is not listed in the patient's Designated Record Set as the Representative, the person may established authority by presenting an original or copy of a valid power of attorney for health care, an original or copy of a court order appointing the person guardian of the patient (guardian ad litem), or an Authorization signed by the patient. (FIU Policy and Procedure #1660.001) (Representatives)

E. If the person is not able to present a health care power of attorney for health care, an original or copy of a court order appointing the person guardian ad litem, or an Authorization signed by the patient, the person may establish a next-of-kin legally authorized representative relationship by representation, or providing a statement of the person's family relationship to the patient. (FIU Policy and Procedure #1660.001) (Representatives)

F. The Privacy Coordinator must:
1. Make a photocopy of all documentation provided and record in the patient's Designated Record Set:
   a. The date, name, and title of the Privacy Coordinator who viewed and made copies of all documentation provided,
   b. Whether a written and signed Authorization was already secured in the patient's Designated Record Set,
   c. The type of documentation received, and
2. Document any oral representation or statements that the person made to support their claim that they are authorized to be the patient's Representative.
3. Properly secure the copied identification or other documentation in the patient's Designated Record Set.

6. Verification of the Identity and Authorization of a Personal Representative of a Minor

A. If the Personal Representative is the child's parent or guardian and is with the child, then no further verification or authorization is required; otherwise verification of authorization must be requested by one of the means set forth for verification of the authorization of the personal representative of an adult or emancipated minor.

NOTE: The identity of the Personal Representative must be verified as set forth immediately above in #4.

7. **Verification of the Identity and Authorization of Law Enforcement Officials if Request is to Disclose PHI for Certain Law Enforcement Purposes**

A. Authority of the law enforcement official to have access to PHI should be established by a written statement from the law enforcement official of the legal authority under which the information is requested (or, if a written statement is impracticable, an oral statement of such authority).

NOTE: Local law enforcement officials (e.g., city police, county sheriff) are not generally entitled to PHI without a court order or written authorization. There are exceptions for reporting and investigation of child abuse/neglect and for reporting gunshot wounds, certain other wounds and burns to local law enforcement officials. (FIU Policy and Procedure #1660.025) (Use and Disclosure of Patient Protected Health Information for Which an Authorization or Opportunity to Agree or Object is NOT Required)

NOTE: When in doubt about the authority of law enforcement official to obtain PHI, contact with the Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity.

For example:

A law enforcement official unknown to staff members requests patient PHI. The official's identity may be established by presentation of his/her badge and the official's authority to have access may be established by the official's written (or oral) statement of the legal authority under which the information is requested, such as investigation of suspected child abuse (which, under state law, permits a police officer access to PHI without patient authorization).

B. The Privacy Coordinator must ask to see the Law Enforcement Official's official identification and must also request the subpoena, summons, request for records, civil or authorized investigative demand, or similar legal process by which the patient PHI is being requested.

C. The Privacy Coordinator or designee must immediately contact via telephone the Office of General Counsel and the Office of Compliance and Integrity (Offices) and advise them of the law enforcement request.

D. The Privacy Coordinator or designee must not take any further action, unless specifically instructed to do so by either Office.

NOTE: Do not send email or other electronic communications/questions containing PHI to the Office of General Counsel or the Office of Compliance and Integrity.

E. The Privacy Coordinator or designee must immediately forward all requests for access to, receipt or disclosure of PHI from a Law Enforcement Official, or any legal requests such as subpoenas, court or administrative orders to the Office of General Counsel for review and approval prior to the disclosure of any PHI.

A. The Privacy Coordinator or designee must, unless instructed to do otherwise by the Office of General Counsel:
   1. Take possession of all original documents received and/or make a photocopy of all documentation presented, and
   2. Record in the patient's Designated Record Set:
      a. the date, time, name, and title of the Law Enforcement Official,
      b. The agency/department/office where the Law Enforcement Official is employed,
      c. The date, time, name, and title of the Privacy Coordinator who obtained the Law Enforcement of Public Official's request and documents,
      d. The date, time, and action taken to communicate with the Office of General Counsel and/or the Office of Compliance & Integrity,
      e. The name(s) of the Workforce member within the Office(s) with whom the Privacy Coordinator communicated,
      f. The instructions received from the Office(s), if any,
      g. The additional actions taken per the instructions received, if any, and
      h. The type of documentation received.
   3. Properly secure the original and/or copied identification and other documentation in the patient's Designated Record Set.

8. Verification of the Identity of a Public Official

A. If the public official is making the request for disclosure of patient PHI in person, the Privacy Coordinator or designee must ask to see the person's official governmental identification or credentials. If the public official is making the

request in writing, then verification must be made by checking with the Public Official's department, division, or office to make sure the request is on official letterhead.

B. After verifying the identity of the public official, the Privacy Coordinator or designee must request a written statement of the legal authority under which the PHI is being requested. If the request is made per legal process, then a warrant, subpoena, order or other legal process issued by a court, grand jury or administrative tribunal is presumed to constitute legal authority to disclose the PHI. If the disclosure is not being made pursuant to legal process, and if it is impractical to obtain a written statement of legal authority under the circumstances, then the Privacy Coordinator or designee may rely on an oral statement.

C. The Privacy Coordinator must immediately contact via telephone the Office of General Counsel and the Office of Compliance and Integrity (Offices) and advise them of the public official's request.

D. The Privacy Coordinator or designee must not take any further action, unless specifically instructed to do so by either Office.

NOTE: Do not send email or other electronic communications/questions containing PHI to the Office of General Counsel or the Office of Compliance & Integrity.

E. The Privacy Coordinator or designee must immediately forward all requests for disclosure of PHI from a public official or any legal requests such as subpoenas, court or administrative orders to the Office of General Counsel for review and approval prior to the disclosure of any PHI.

F. The Privacy Coordinator or designee must, unless instructed to do otherwise by the Office of General Counsel or the Office of Compliance and Integrity:
   1. Take possession of all original documents received and/or make a photocopy of all documentation provided,
   2. Request a written statement of the legal authority under which the PHI is being requested and record in the patients Designated Record Set:
      a. The date, time, name, and title of the public official,
      b. The Privacy Coordinator or designee's request for a written statement of legal authority,
      c. The Public Official's response to the request,
      d. The agency/office/department where the public official is employed,
      e. The date, time, name, and title of the Workforce member who received the Public Official's request and documents,

f. The method used the verify, and the verification that the request is on official letterhead,
g. The date, time, and action taken to communicate with the Office General Counsel's and the Office of Compliance and Integrity,
h. The name(s) of the Workforce member within the two Offices with whom communication occurred,
i. The instructions received from the two Offices, if any,
j. The additional actions taken per the instructions, if any, and
k. The type of documentation received.

3. Properly secure the copied identification or other documentation in the patient's Designated Record Set.

G. The Privacy Coordinator or designee must immediately forward all requests for Disclosure of PHI from a Government Official, i.e., FBI, CIA, DCF or any legal requests such as subpoenas, court or administrative orders to the Office of General Counsel and the Office of Compliance and Integrity for review and approval prior to the disclosure of any PHI.

9. Verification of the Identity of a Person Acting on Behalf of a Public Official

A. When the Requester is a person acting on behalf of a Public Official (e.g., law enforcement officers, state or federal surveyors, medical examiners, coroners) and the request is made in person, verification of the identity of a person acting on behalf of the public official should be accomplished by the presentation of an agency identification badge, other official credentials or proof of government status.

B. The Privacy Coordinator must also ask for a written statement on official letterhead of the person acting on behalf of a public official or governmental agency for whom the person is acting identifying that the person is acting on behalf of the governmental agency.

C. When the Requester is a person acting on behalf of a Public Official or governmental agency (e.g., law enforcement officers, state or federal surveyors, medical examiners, coroners) and the request a person acting on behalf of a Public Official or governmental agency is making is in writing, then the Privacy Coordinator must verify with the governmental agency to make sure the request is on official letterhead. Alternatively, a contract, memorandum of understanding or purchase order that shows the person is acting on behalf of a public official or the government agency can be used for verification.

D. After verifying the identity of person acting on behalf of a Public Official, the Privacy Coordinator or designee must request a written statement of the legal authority under which the PHI is being requested. If the request is made per legal process, then a warrant, subpoena, order or other legal process issued by a court, grand jury or administrative tribunal is presumed to constitute legal authority to disclose the PHI. If the disclosure is not being made pursuant to legal process, and if it is impractical to obtain a written statement of legal authority under the circumstances, then the Privacy Coordinator may rely on an oral statement.

E. The Privacy Coordinator must immediately contact via telephone the Office of General Counsel and the Office of Compliance and Integrity (Offices) and advise them of the law enforcement request.

F. The Privacy Coordinator must not take any further action, unless specifically instructed to do so by either Office.

NOTE: Do not send email or other electronic communications/questions containing patient PHI to the Office of General Counsel or the Office of Compliance and Integrity.

G. The Privacy Coordinator must immediately forward all requests for disclosure of PHI of a person acting on behalf of a Public Official or any legal requests such as subpoenas, court or administrative orders to the Office of General Counsel.

H. The Privacy Coordinator or designee must, unless instructed to otherwise by the Office of General Counsel:
   1. Take possession of all original documents received and/or make a photocopy of all documentation provided, and
   2. Record in the patients Designated Record Set:
      a. The person's verbal response to a request for a written statement of legal authority of the person acting on behalf of a Public Official,
      b. The date, time, name, and title of the person acting on behalf of a Public Official,
      c. The agency/office/department where the person is acting on behalf of a Public Official is employed,
      d. The date, time, name, and title of the Privacy Coordinator who received the person acting on behalf of a Public Official's request and documents,
      e. The method used the verify the request of the person acting on behalf of a Public Official is on official letterhead,
      f. The date, time, and action taken to communicate with the Office of General Counsel and the Office of Compliance and Integrity,

g. The name(s) of the Workforce member within the Offices with whom communication occurred,
h. The instructions received from the Office of General Counsel and the Office of Compliance and Integrity, if any,
i. The additional actions taken per the instructions, if any, and
j. The type of documentation received.

3. Properly secure the copied identification and other documentation received in the patient's Designated Record Set.

10. Verification Requirements for Disclosures Made to Persons Involved in the Patients Care and Treatment and in Emergency Circumstances

A. The Privacy Coordinator and/or healthcare provider must exercise its professional judgment to determine whether it is in the best interest of the Patient to make a disclosure of the patient's PHI to family members, close friends, an adult acting on behalf of a child, or others in situations, including emergency situations, in which the Patient is unavailable or unable to give his/her authorization for the disclosure. (FIU Policy and Procedure #1660.030) (Use and Disclosure of Patient Protected Health Information Requiring an Opportunity for the Patient to Agree or Object) and (Policy and Procedure #1640.025) (Minimum Necessary).

B. The Privacy Coordinator and/or healthcare provider must ask the patients family members, close friends, an adult acting on behalf of a child, or others, in situations, including emergency situations, about the nature of their relationship with the patient prior to making any disclosures.

11. Verification Requirements for Disclosures Made to Avert a Serious Threat to Health and Safety

A. The Privacy Coordinator and/or healthcare provider may rely on the exercise of professional judgement in making a use or disclosure or act on a good faith belief that making a disclosure to a person or entity that he/she believes will be able to help avert or substantially lessen a threat to health or safety.

B. The Privacy Coordinator or healthcare provider must document in the patient's Designated Record Set:
1. The date, name, and title of the Privacy Coordinator who made the disclosure, and
2. The name and title of the person or entity to whom the disclosure was made.

12. Verification Requirements for Disclosures Made to Researchers

A. The Privacy Coordinator must request from the researcher written assurances that are specified in the FIU HIPAA Policy Regarding Disclosure and Use of PHI for Research Purposes and the Role of the FIU Institutional Review Board.

B. If a disclosure is conditioned on particular documentation, statements, or representations from the individual or entity (researcher) requesting the PHI, the Privacy Coordinator may rely, if reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

C. The documentation required (e.g., an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law, and adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted) may be satisfied by one or more written statements signed by the chair or other member, as designated by the chair, of the Institutional Review Board (IRB) or the privacy board, as applicable.

D. The Privacy Coordinator or healthcare provider must:
   1. Document:
      a. The date, name, and title of the Privacy Coordinator who made the disclosure,
      b. The names of the patients whose PHI was disclosed, and
      c. The extent of the patient PHI disclosed, and
      d. The method(s) used to verify the documentation, statements, or representations provided in order to meet the verification requirements.
   2. Make a copy of any and all documents provided.

II. Documenting/Recording

A. Prior to making or denying access to and/or disclosure of PHI, the Privacy Coordinator must:
   1. Document in the patients Designated Record Set the relevant information collected and the applicable actions taken as required above in each verification process. This may include, but is not limited to:
      a. The date, name, and title of the Workforce member who completed the verification,
      b. The verification procedure(s)/method(s) used,

c. The reasonable efforts made to verify the identity of the individual with whom he/she spoke if the communication was via the telephone,
d. The type of document(s) received, and if it/they are original or a photocopy,
e. How documents were received (i.e. via facsimile, hand delivered, US. Postal Services, etc.),
f. Any verbal representations or statements made by the individual asserting that they are the patient's Personal Representative,
g. Any statements of the person's family relationship to the patient,
h. How the identity of a law enforcement official, public official, or person acting on behalf of a public official was verified,
i. The visual verification of an individual's official governmental identification or credentials,
j. The receipt of a public official's written request and verification procedure used to ensure that the written request is on official letterhead,
k. The verification of a public officials' legal authority under which PHI is being requested via a written statement,
l. The visual verification of a person's identity and official governmental identification or credentials,
m. The receipt of a warrant, subpoena, order or other legal process issued by a court, grand jury or administrative tribunal, or if the disclosure is not being made pursuant to legal process, and if it is impractical to obtain a written statement of legal authority under the circumstances, then documenting the oral statements the Privacy Coordinator or designee relied on in making the disclosure,
n. The receipt of any contracts, memorandums of understanding, or purchase orders used to verify that a person is acting on behalf of an identified government agency, and
o. The date and type of documents forwarded to the Office of General Counsel and/or the Office of Compliance and Integrity.

2. Properly secure all documents received in the patient's/patient's Designated Record Set.

III. 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) 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)