FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Verification #1660.040

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 13, 2020	August 6, 2025	Office of Compliance and Integrity

POLICY STATEMENT

Florida International University (FIU) Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Components (hereinafter facilities and programs) 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 facility or program 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 facility and program-specific policies, procedures, or protocols that conflict 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)

Facility and programs may maintain HIPAA documentation in either paper or electronic form, provided that any format is sufficiently protected to ensure it will be retrievable throughout the required retention period. Unless otherwise indicated in FIU Privacy or Security Rule Policy and Procedure, the facility and program Privacy Coordinators are responsible for maintaining all HIPAA documentation relevant to his/her facility or program. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

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

Facility and program Workforce members who fail to adhere to this policy and procedure may be subject to civil and criminal penalties as provided by law, and/or administrative and disciplinary action. (FIU Policy and Procedure #1660.085) (Sanctions)

FIU reserves the right to amend, change or terminate this policy and procedure at any time, either prospectively or retroactively, without notice. Any ambiguities between this policy and

procedure and the other policies and procedures should be accordingly made consistent with the requirements of HIPAA, federal law, and Florida state statutes. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

SCOPE

This policy applies to FIU Components (facilities and programs) contained within FIU's HIPAA Hybrid Designation (FIU Policy and Procedure #1610.005), its Workforce members and Business Associates as defined in this policy and FIU Policy and Procedure #1660.015 regarding Business Associate Agreements.

REASON FOR POLICY

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

DEFINITIONS

Please refer to the following link for a complete list of definitions pertaining to all HIPAA policies.

HIPAA Policies Definitions

ROLES AND RESPONSIBILITIES

Compliance Oversight:
The Director of Compliance and Privacy for Health Affairs:

- Evaluates all federal and state healthcare privacy laws, regulations, rules and ordinances (Rules) to ensure compliance with the Rules.
- Develops and maintains all required University-wide Privacy Rule policies and procedures.
- Develops and maintains HIPAA health care Privacy Rule training modules.
- Performs audits and assessments of the facilities and programs to ensure their compliance with the Privacy Rules and associated FIU Policies and Procedures.
- Partners with the Division of Information Technology HIPAA Security Officer to ensure compliance with all federal and state healthcare privacy and security laws, regulations rules, and ordinances.

HIPAA Components (Facilities and Programs):

- Each FIU HIPAA Hybrid Designated Component (facility and program) must designate a Privacy Coordinator responsible for overseeing and ensuring the facility's or program's implementation and compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable 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
- Florida Statute §456.057
- Florida Statute §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 Director of Compliance and Privacy for Health Affairs at (305) 348-0622 or hipaaprivacy@fiu.edu, or contact the appropriate Component Privacy Coordinator.

HISTORY

Initial Effective Date: October 13, 2020
Review Dates *(review performed, no updates)*: n/a
Revision Dates *(review performed, updates made to document)*: October 13, 2020; February 29, 2024, August 6, 2025.

FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

Verification #1660.040a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 13, 2020	August 6, 2025	Office of Compliance and Integrity

PROCEDURE STATEMENT

I. Verification

The facility and program Privacy Coordinators are responsible for overseeing and ensuring the facility's and program's implementation and compliance with the HIPAA Privacy Rule, federal law, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable Florida state statutes 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 or entity 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, Workforce members 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 facility or program 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 facility and program 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, federal law, and/or Florida state statutes, Workforce members shall utilize the following methods of verification:

1. <u>Verification of Identity When a Patient is Requesting their PHI in Person</u>

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

B. If the person is <u>not known</u> to the Workforce member, then the Workforce member <u>must</u> verify the identity of the person. (FIU Policy and Procedure #1660.050) (Access)

    1. The Workforce member <u>must</u>:
        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 Workforce member <u>must</u>:
        a. Make a photocopy of all identification and documentation provided,
        b. Record in the patient's medical records:
            1. The date, name, and title of the Workforce member 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 medical records,
d. Properly secure the copied identification or other documentation received in the patient's medical records.

3. If the Workforce member has any concerns or reservation with the accuracy of the information provided and the information contained within the medical records, the Workforce member 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 medical records,
   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 Workforce member 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 medical records:
         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 Workforce member 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 Workforce member must:
   1. Document in the patient's medical records:
      a. The date, name, and title of the Workforce member 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 Workforce member or designee, and

2. Compare, verify, and document the accuracy of the information provided with that contained in the patient's medical records.

C. If the Workforce member has any concerns or reservation with the accuracy of the information provided and the information contained within the medical records, the Workforce member 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 medical records.
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 Workforce member 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 medical records:
      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 Workforce member 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 Workforce member must:
   a. Record in the patient's medical records:
      1. The date, time, name and title of the Workforce member 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 medical records, and

b. Properly secure the Authorization in the patient's medical records.

B. If the Workforce member has any concerns or reservation with the accuracy of the information contained within the Authorization and the information contained within the medical records, the Workforce member 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 medical records. Without providing details about the information contained within the medical records, the Workforce member 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 Workforce member 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 medical records:
   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 Workforce member, then the Workforce member 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 Workforce member must:

1. Make a photocopy of all identification and other documentation provided and record in the patient's medical records:

a. The date, name, and title of the Workforce member who verified the person's identity,
b. The method and manner in which the Workforce member 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 medical records.

C. Once the person's identity has been established, the Workforce member may establish the person's authority to act on behalf of the patient by confirming that the person is named in the patient's medical records as the patient's Representative. (FIU Policy and Procedure #1660.001) (Representatives)

D. If the person is not listed in the patient's medical records 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 Representative of the patient, or an Authorization signed by the patient. (FIU Policy and Procedure #1660.001) (Representatives)

E. If the person is not able to present a document appointing as the Representative, or an Authorization signed by the patient, the person may establish a next-of-kin legally authorized representative relationship as limited by Florida state statute. (FIU Policy and Procedure #1660.001) (Representatives)

F. The Workforce member must:
1. Make a photocopy of all documentation provided and record in the patient's medical records:
a. The date, name, and title of the Workforce member who viewed and made copies of all documentation provided,
b. Whether a written and signed Authorization was already secured in the patient's medical records,
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 medical records.

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 the Director of Compliance and Privacy for Health Affairs with the 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 Workforce member 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 Workforce member must immediately contact via telephone the Office of General Counsel and the Office of Compliance and Integrity and advise them of the law enforcement request.

D. The Workforce member 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 Workforce member 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.

F. The Workforce member 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 medical records:
   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 Workforce member 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 Workforce member 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 medical records.

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 Workforce member 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 Workforce member 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 Workforce member may rely on an oral statement.

C. The Workforce member must immediately contact via telephone the Office of General Counsel and the Office of Compliance and Integrity and advise them of the public official's request.

D. The Workforce member 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 Workforce member 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 Workforce member 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 patient's medical records:
      a. The date, time, name, and title of the public official,
      b. The Workforce member'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 medical records.

G. The Workforce member 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 Workforce member 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 Workforce member 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 Workforce member 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 Workforce member must immediately contact via telephone the Office of General Counsel and the Office of Compliance and Integrity and advise them of the law enforcement request.

F. The Workforce member 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 Workforce member 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 Workforce member 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 patient's medical records:
      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 Workforce member 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 medical records.

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

A. The Workforce member 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 Workforce member 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 Workforce member 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 Workforce member or healthcare provider must document in the patient's medical records:
1. The date, name, and title of the Workforce member or healthcare provider 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 Workforce member 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 Workforce member 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 Workforce member or healthcare provider must:
   1. Document:
      a. The date, name, and title of the Workforce member who made the disclosure,
      b. The names of the patient 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. Record/Documentation Retention

A. If a communication, action, activity, or designation is required to be documented in writing, the document or record owner (The facility or program) 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)