FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Right of Patients to Request Confidential Communications Regarding the Use and Disclosure of Their Protected Health Information #1660.005

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 permit patients to request the Component communicate with the patient by alternative means or at an alternative location (e.g., other than their home address or telephone number).

Components may require the patient to make a request for a confidential communication in writing.

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 #1600.080) (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 #1600.080) (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 FIU HIPAA Hybrid Designated Component (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 #1600.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

SCOPE

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

REASON FOR POLICY

To ensure the patient's right to request that communications of their PHI be delivered by alternate means or at alternate locations (Confidential Communications) as required by the HIPAA Privacy Rule and state law and to identify the steps the Components must take to grant or deny a patient's right to Confidential Communications.

45 CFR §164.522 (Right to Request Privacy Protection for PHI)

DEFINITIONS

TERM	DEFINITIONS
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.
Alternative Communication	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.
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.
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 patients 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 patients.

	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.
Florida Statutes	Also known as F.S.
Health Care Component	See "Component"
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 Plan	Means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).
HIPAA	Means the Health Insurance Portability and Accountability Act of 1996.
Hybrid Covered Entity	Means a single legal entity that performs both covered and non-covered functions. The entity has a defined health care component that engages in HIPAA electronic transactions.
Incidental	A use or disclosure that occurs as a by-product of another permissible or required use or disclosure, as long as the covered entity or support unit has applied reasonable safeguards and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure. An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Privacy Rule. However, an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule.
Integrity	Means the property that data or information have not been altered or destroyed in an unauthorized manner.
Patient	The person who is the subject of PHI.
Payment	Means:

1. The activities undertaken by:
    a. Except as prohibited under §164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
    b. A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
    c. The activities in paragraph (1) of this definition relate to the client to whom health care is provided and include, but are not limited to:
        1. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
        2. Risk adjusting amounts due based on enrollee health status and demographic characteristics;
        3. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
        4. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
        5. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
        6. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
            a. Name and address;
            b. Date of birth;
            c. Social security number;
            d. Payment history;

	e. Account number; and f. Name and address of the health care provider and/or health plan.
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.
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.
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 receiving and processing requests by patients for Confidential Communications.

RELATED RESOURCES

References

- 45 CFR §164.502
- 45 CFR §164.504
- 45 CFR §164.514
- 45 CFR §164.524
- 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 #1660.070 (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)
- FIU Policy and Procedure #1660.085 (Sanctions)
- FIU Policy and Procedure #1660.075 (HIPAA Privacy and Security Rule Training)
- FIU Policy and Procedure #1660.015 (Business Associate Agreements)
- FIU Policy and Procedure #1600.080 (Policies and Procedures, Changes to Policies and Procedures, and Documentation)
- FIU Policy and Procedure #1660.040 (Verification)

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

FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

Right of Patients to Request Confidential Communications Regarding the Use and Disclosure of Their Protected Health Information #1660.005a

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

PROCEDURE STATEMENT

I. Requests for Confidential Communications

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 PHI and electronic PHI (ePHI), including, but not limited to receiving and processing requests by patients for confidential communications regarding the use and disclosure of their 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 makes a request for confidential communications, the Privacy Coordinator must accommodate reasonable requests to receive communications of their PHI by alternative means or at alternative locations (confidential communications), by having the patient complete and sign a Request for Communication of Protected Health Information Form. (Sample Communication Form attached) (hereinafter Communication Form) However, the Privacy Coordinator will accept any written request for confidential communications if the required information and signature are provided.

B. The patient must describe in writing specifically the alternate means and/or location the patient would like the Component to communicate with the patient. (Communication Form)

C. The Privacy Coordinator will assist the patient in completing the Communication Form, if necessary.

D. The Privacy Coordinator will honor requests for alternate means of making this request if reasonable accommodations (such as disability or illiteracy) are needed.

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

F. If a patient submits a request for the Component to communicate with him/her via electronic communication (i.e., email/facsimile/text message), the patient is required to complete the Communication Form and the Email/Text/Facsimile Message Confidential Communication Form (hereinafter Email Form) (hereinafter both forms are known collectively as the Communication Form(s)) which identifies the risk associated with using electronic communication, the conditions for using electronic communication, instructions, and an acknowledgement.

G. If after advising the patient of the risk associated with the use of electronic communications, the patient determines that the risk(s) is unacceptable as a means of confidential communications, the patient should be offered other more secured means of communication such as mail, the telephone, or other electronic methods of communication.

NOTE: Under the HIPAA Privacy Rule, healthcare providers may communicate with patients electronically, such as through email, provided they apply reasonable safeguards when doing so. (See 45 C.F.R. § 164.530(c)). For example, certain precautions must be taken when using email to avoid unintentional disclosures, such as checking an e-mail address for accuracy before sending the email or sending an email alert to the patient for address confirmation prior to sending the message.

NOTE: Workforce members must ensure that any emails sent containing PHI are done in compliance with FIU HIPAA Security Policy and Procedure #_____. With limited exception, Workforce members must not communicate with patients through unencrypted email. Further, while the Privacy Rule does not prohibit the use of unencrypted email for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted email and patients must be advised of the risk of using encrypted and/or unencrypted email.

For example, a health care provider should accommodate an individual's request to receive appointment reminders via email, rather than on a postcard, if email is a reasonable, alternative means for that provider to communicate with the patient.

II. Incomplete Communication Form(s)

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

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

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 Communication Form, or other written document, and Designated Record Set 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.

C. If the patient is not available in-person, or via the telephone, and did not previously request and been approved for confidential communications, the Privacy Coordinator may notify the patient of the need for the missing information by sending the original incomplete Communication Form, or other written document, without unreasonable 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 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 of delivery

outlined in the **NOTE** and Section II.D.1, 2 and 3 immediately below shall apply.

NOTE: Any electronic communications (i.e., email/facsimile/text message) containing patient protected health information (PHI) must contain the following or similar confidentiality statement approved by the Office of Compliance and Integrity:

> The information contained in this transmission may contain privileged and confidential information, including patient information protected by federal and state privacy laws, including the Health Insurance Portability and Accountability Act Privacy Rule (HIPAA) (45 C.F.R. Part 164). It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution, or duplication of this communication is strictly prohibited and may be unlawful. If you are not the intended recipient, please contact the sender by reply email or call the sender at the telephone number include in their contact information and delete this e-mail from your system and destroy any and all copies of the original email message.

D. The Privacy Coordinator must:
   1. Document in the patient's Designated Record Set:
      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 Communication Form(s), or other written document, and Cover Letter (See Sample Cover Letter Requesting Complete or Additional Information) (hereinafter Cover Letter) in the patient's Designated Record Set, and
   3. If the delivery is accomplished via previously 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 Designated Record Set, 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 Designated Record Set.

III. Properly Completed Communication Form(s)

A. Upon receipt of a completed Communication Form(s), the Privacy Coordinator will:
   1. Date stamp receipt of the completed Communication Form(s), or other written document, on the day received,
   2. Complete the "For FIU Entities USE ONLY" section of the Communication Form,
   3. Promptly document in the patient's Designated Record Set:

a. Receipt of the Communication Form(s), or other written document, and
b. The date, name, and title of the Privacy Coordinator who received the properly completed Communication Form(s), or other written document.

4. Properly secure the Communication Form(s), or other written document, in the patient's Designated Record Set.

B. The Privacy Coordinator, along with appropriate and necessary Workforce members, will review the patient's request to receive communications of their PHI by alternative means or at an alternate location to determine if the Component will grant or deny the request.

C. The Privacy Coordinator, and the appropriate and necessary Workforce members responsible for reviewing the patient's request, must not require the patient to provide an explanation regarding his/her request for communications of their PHI by alternative means or at alternative location as a condition of providing communications on a confidential basis.

D. The Privacy Coordinator must condition and document in the patient's Designated Record Set when evaluating a patient's request to receive communications of his/her PHI by alternative means or at alternative locations on:
1. Information regarding how payment, if any, will be handled; and
2. Specification of an alternative address or other method of contact (i.e., email address, cellular telephone number verses home telephone number, mailing address verses P.O. Box address, etc.)

E. The Privacy Coordinator must within a reasonable time following receipt of the properly completed a Communication Form(s), or other written document, accept or deny the patient's request for confidential communications and complete the "FOR FIU INTERNAL USE ONLY" Section of the Communication Form.

IV. Confidential Communications Approved

A. If the Privacy Coordinator and the appropriate and necessary Workforce members approve the patient's request for confidential communications, FIU Workforce members must not communicate with the patient in a manner that violates the approved alternate means and/or location of confidential communication.

B. The Privacy Coordinator shall promptly send the patient an Approval Letter (See Sample Letter Accepting Patient's Request for Confidential Communications (hereinafter Approval Letter) via the approved method of confidential communication. The Approval Letter shall identify:
1. The request is approved,

2. The Component will communicate with the patient using the alternate means or location requested and approved,
3. The approval will remain in-place until such time as:
   a. The Component receives a written request from the patient to terminate or change the agreement, or
   b. The Component determines that it is no longer administratively possible to comply with the approved request.
4. That in an urgent or emergency situation, the Component will use whatever communication mechanism is necessary to contact the patient. (Approval Letter)

C. The Privacy Coordinator must:
1. Document in the patient's Designated Record Set:
   a. The date, name(s), and title of the Workforce members involved in the review and approval of the requested confidential communication(s),
   b. The specific approved alternate means and/or location of confidential communication(s),
2. Prepare and deliver to the patient the Approval Letter.
3. Document in the patient's Designated Record Set:
   a. The date, name, and title of the Privacy Coordinator who completed delivery of the Approval Letter, and
   b. The method of delivery.
4. Ensure that appropriate Workforce members are notified of the approved confidential communication,
5. Document in the patient's Designated Record Set:
   a. The date, names, and titles of the Workforce member(s) who were notified of the approved confidential communication, and
   b. The manner in which the Workforce members were notified (i.e., in-person, memorandum, etc.)
6. Properly secure in the patient's Designated Record Set:
   a. The original Communications Form(s),
   b. A copy of the Approval Letter,
   c. The original written notification sent to Workforce members regarding the agreed upon confidential communication, (or copy when appropriate), and
   d. If delivery of the written notification sent to the Workforce members was made via electronic communication:
      1. Print a hardcopy of the electronic communication, and
      2. Properly secure it in the patient's Designated Record Set.

V. Termination of Agreement for Confidential Communications

A. The Component may terminate an agreement to communicate with the patient by confidential communications if:

1. The Privacy Coordinator and/or appropriate Workforce members determine the alternate means or location is not effective (e.g., Component is unable to contact the patient by the approved specific means and/or at the specified location); or
2. The Component can no longer accommodate the request because it is not reasonable.

B. When a Component terminates an agreement for confidential communication, the Privacy Coordinator must make a reasonable attempt to notify the patient in writing that the Component is terminating the agreement before resuming communication through the normal channels. (See Sample Letter Terminating Agreement for Confidential Communications) (hereinafter Termination Letter)

C. The Privacy Coordinator must:
1. First attempt to deliver the Termination Letter to the patient via the previously requested and approved alternate means or location;,
2. Document in the patient's Designated Record Set:
   a. The date, name, and title of the Privacy Coordinator who attempted delivery of the Termination Letter;
   b. The Form and Format ;of the attempted delivery, and
   c. If the delivery was successful:
      1. The date of deliver.
3. Properly secure a copy of the Termination Letter in the patient's Designated Record Set, and
4. If the delivery was made via electronic communication, print a hardcopy of the electronic communication (i.e., email/facsimile/text message) and properly secure it in the patient's Designated Record Set.

D. If the Privacy Coordinator is not able to accomplish or verify delivery of the Termination Letter, the Privacy Coordinator must:
1. Document in the patient's Designated Record Set:
   a. The date, name, and title of the Privacy Coordinator who attempted delivery, and
   b. The Form and Format of the attempted delivery.
2. Properly secure a copy of the Termination Letter in the patient's Designated Record Set;
3. If the attempted delivery was made via electronic communication, print a hardcopy of the electronic communication and properly secure it in the patient's Designated Record Set, and
4. Resume delivery through normal channels and document delivery in the same manner as described in V.D.1 and 2 of this Section.

VI. Confidential Communications Denied

A. If the Privacy Coordinator and the appropriate Workforce members denies the patient's request for confidential communications, the Privacy Coordinator must:
   1. Document in the patient's Designated Record Set:
      a. The date, name(s), and title of the Workforce member(s) involved in the review and denial of the requested confidential communication,
      b. The denial of requested confidential communication.
   2. Prepare a Denial Letter (See Sample Letter Denying Patient's Request for Confidential Communications) (hereinafter Denial Letter);
   3. Document in the patient's Designated Record Set:
      a. The date, name, and title of the Privacy Coordinator who completed delivery of the Denial Letter;
      b. The Form and Format of delivery, and
      c. Ensure that appropriate Workforce members are notified of the denial of the request for confidential communication.
   4. Document in the patient's Designated Record Set:
      a. The date, names, and titles of the Workforce member(s) who were notified of the denial of confidential communication, and
      b. The manner in which the Workforce members were notified (i.e., in-person, memorandum, etc.)
   5. Properly secure in the patient's Designated Record Set:
      a. The original Communications Form(s);
      b. A copy of the Denial Letter, and
      c. All original written notification(s) of the denial of confidential communication (or copy when appropriate) sent to the Workforce members, and
   6. If the deliver was made via electronic communication:
      a. Print a hardcopy of the electronic communication, and
      b. Properly secure it in the patient's Designated Record Set.

B. The Denial Letter shall identify:
   1. The request was denied,
   2. The reason(s) for the denial,
   3. A statement that if the patient disagrees with the denial, he/she may contact the Privacy Coordinator at the address and telephone number provided on the Denial Letter.

VII. 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)

VIII. Forms

- Sample Confidential Communication Request Form
- Sample Email/Text /Facsimile Message Confidential Communication Form
- Sample Cover Letter requesting Complete or Additional Information
- Sample Letter Accepting Patient's Request for Confidential Communications
- Sample Letter Denying Patient's Request for Confidential Communications
- Sample Letter Terminating Agreement for Confidential Communications