FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Destruction/Disposal of Protected Health Information # 1660.115

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
August 31, 2021	February 29, 2024	Office of Compliance and Integrity

POLICY STATEMENT

Florida International University (FIU) strives to ensure the privacy and security of all patient protected health information (PHI) in the maintenance, retention, and eventual destruction/disposal of such information. Destruction/disposal of this information in whatever form and format shall be carried out as described in applicable records' retention schedules of FIU based on federal law and Florida state statutes and in a manner that leaves no possibility for reconstruction of the information. This policy and procedure describes how records shall be disposed of/destroyed. Also see https://security.fiu.edu/uploads/docs/Media-Sanitation-Guideline.pdf

As a University-wide policy and procedure, this policy and procedure takes precedence over any FIU Health Insurance and Portability and Accountability Act (HIPAA) Hybrid Designated Healthcare Component (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 and Security 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 and a HIPAA Security Coordinator. (FIU Policy and Procedure #1660.070) (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)

FIU reserves the right to amend, change or terminate this policy and procedure at any time, either prospectively or retroactively, without notice. Any ambiguities between this policy and procedure and the other policies and procedures should be harmonized consistent with the requirements of HIPAA and state law and regulation. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

SCOPE

This policy applies to FIU's HIPAA Components 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

To explain retention, destruction and disposal of PHI as described in the HIPAA Privacy and Security Rules and Florida state statutes.

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 ePHI and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
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 PHI on behalf of a covered entity (such as claims processing, case management, utilization review, quality

	assurance, billing) or provides services for a covered entity that require the disclosure of PHI (such as legal, actuarial, accounting, accreditation). **NOTE:** A business associate relationship exists when an individual or entity, acting on behalf of an FIU HIPAA Component(s), assists in the performance of a function or activity involving the creation, use, disclosure, or access of PHI. This includes, but not limited to, claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management or repricing. **NOTE:** A Business Associate may include any individual or entity that receives PHI from a HIPAA Component in the course of providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, software support, or financial services. A Business Associates does not, however, include HIPAA Component workforce members.
Business Associate Agreement	Means a contract or other written arrangement with a business associate which must describe the permitted and required uses of PHI by the business associate; Provide that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law; and Require the business associate to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the contract.
Code of Federal Regulations	Also known as CFR is the codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the Federal Government. It is divided into 50 titles that represent broad areas subject to Federal regulation.
Component	Means a component or combination of components of a hybrid entity designated by the hybrid entity (Florida International University). Those programs designated by FIU that must comply with the requirements of the Health Insurance Portability and Accountability Act of 1996, hereinafter referred to as "Components". Components of FIU are required to comply with the Administrative Simplification provisions of HIPAA because the Components perform a covered function.
Confidentiality	Means data or information is not made available or disclosed to unauthorized persons or processes.

Covered Entity	An entity that is subject to HIPAA. 1. a health plan; 2. a health care clearinghouse; and/or 3. a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
Degauss	Using a magnetic field to erase (neutralize) the data bits stored on magnetic media.
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 PHI 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 PHI outside of the entity holding the information.
Electronic Protected Heath Information (ePHI)	PHI in electronic form. See also: PHI.
Florida Statutes	Also known as F.S. is a permanent collection of state laws organized by subject area into a code made up of titles, chapters, parts, and sections. The Florida Statutes are updated annually by laws that create, amend, transfer, or repeal statutory material.
Form and Format	The terms refer to how the PHI is conveyed to the individual (e.g., on paper or electronically, type of file, etc.)
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 is a cabinet-level executive branch department of the U.S. federal government created to protect the health of the U.S. people and providing essential human services.

Health Information	Means any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an patient/client; the provision of health care to an patient/client; or the past, present, or future payment for the provision of health care to an patient/client.
HIPAA	Means the Health Insurance Portability and Accountability Act of 1996.
Hybrid Covered Entity	Means a single legal entity that performs both covered and non-covered functions. The entity has a defined health care component that engages in HIPAA electronic transactions
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.
Patient Health Information Media	Any record of patient health information, regardless of medium or characteristic that can be retrieved at any time. This includes all original patient records, documents, papers, letters, billing statements, x-rays, films, cards, photographs, sound and video recordings, microfilm, magnetic tape, electronic media, and other information recording media, regardless of physical form or characteristic, that are generated and/or received in connection with transacting patient care or business.
Payment	Means: 1. The activities undertaken by: Except as prohibited under §164.502(a)(5)(i), a. 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 patients to whom health care is provided and include, but are not limited to: i. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; ii. Risk adjusting amounts due based on enrollee health status and demographic characteristics;

	iii. 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; iv. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; v. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and vi. Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: a. Name and address; b. Date of birth; c. Social security number.
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	Means any individually identifiable health information collected or created in the course of the provision of health care services by a covered entity, in any form (written, verbal or electronic). PHI

	relates to the past, present, or future physical or mental health or condition of an individual or the past, present, or future payment for the provision of health care to an individual. PHI, however, specifically excludes: 1. Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g ("FERPA"); 2. Records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and 3. Employment records held by a covered entity in its role as an employer.
Privacy Rule	The regulations at 45 CFR 160 and 164, which detail the requirements for complying with the standards for privacy under the administrative simplification provisions of HIPAA.
Sanitization	Removal or the act of overwriting data to a point of preventing the recovery of the data on the device or media that is being sanitized. Sanitization is typically done before re-issuing a device or media, donating equipment that contained sensitive information or returning leased equipment to the lending company.
Technical Safeguards	Means the technology and the policy and procedures for its use that protect ePHI and control access to it.
Treatment, Payment, and Healthcare Operations	(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.
Use	With respect to patient/client identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
Workforce	Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity (FIU HIPAA Component) or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

ROLES AND RESPONSIBILITIES

1. **Compliance Oversight:** The Office of University Compliance and Integrity (University Compliance)

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

2. Division of Information Technology HIPAA Security Officer:

- See the Division of Information Technology "Media Sanitation Guideline".
- The Information Security Office will be responsible for performance and documentation of all media sanitation.

3. HIPAA Components:

- Each FIU HIPAA Hybrid Designated Component must designate a Privacy and a Security Coordinator responsible for overseeing and ensuring the Component's implementation and compliance with the HIPAA Privacy Rule and Security Rule, FIU's associated HIPAA Privacy and Security Policies and Procedures, and any applicable state laws and/or regulations governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to the retention, destruction and disposal of PHI.

RELATED RESOURCES

References

- 45 CFR §164.502
- 45 CFR §164.504
- 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 #1660.015 (Business Associate Agreements)
- FIU Policy and Procedure #1660.070 (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)
- FIU Policy and Procedure #1660.075 (HIPAA Privacy and Security Rule Training)

- FIU Policy and Procedure #1660.080 (Policies and Procedures, Changes to Policies and Procedures, and Documentation)
- FIU Policy and Procedure #1660.085 (Sanctions)
- FIU Policy and Procedure #1660.110 (Designated Record Set)
- The Division of Information Technology "Media Sanitation Guideline"

CONTACTS

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

HISTORY

Initial Effective Date: August 31, 2021
Review Dates (*review performed, no updates*): n/a
Revision Dates (*review performed, updates made to document*): August 31, 2021; February 29, 2024.

Destruction/Disposal of Protected Health Information # 1660.115a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
August 31, 2021	February 29, 2024	Office of Compliance and Integrity

PROCEDURE STATEMENT

I. **Destruction/Disposal of Protected Health Information**

Each Component must designate a Privacy Coordinator responsible for overseeing and ensuring the Component's implementation and compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable federal laws and Florida state statutes governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to the retention, destruction and disposal of patient protected health information (PHI). Privacy Coordinators may delegate and share duties and responsibilities as necessary and appropriate but retain oversight responsibility. (See FIU Policy and Procedure #1660.070) (Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators)

A. The Division of Information Technology through the Information Security Office will be responsible for performance and documentation of all media sanitation. (See Division of Information Technology "Media Sanitation Guideline" at https://security.fiu.edu/uploads/docs/Media-Sanitation-Guideline.pdf

B. All destruction/disposal of PHI will be done in accordance with applicable federal laws, Florida state statutes, and any applicable records' retention schedule of FIU. Records that have satisfied the period of retention may be destroyed/disposed of by an appropriate method as described in III.A. below.

C. Records involved in any open investigation, public records request, audit or litigation must not be destroyed/disposed of if an FIU Component receives notification that any of the above situations have occurred, or there is the potential for such. The record retention schedule shall be suspended for those records until such time as the situation has been resolved.

D. When the record retention schedule for the destruction/disposal of identified record(s) is suspended, the Privacy Coordinator or designee must document:
   1. the name and title of the Privacy Coordinator or designee who suspended the destruction/disposal;
   2. the date the Privacy Coordinator or designee suspended the destruction/disposal;

3. the reason for the suspension (i.e., receipt of a public records request, audit, or litigation), and
4. the date, if known, when the records may be destroyed/disposed of.

E. The Privacy Coordinator or designee must ensure that records containing PHI scheduled for destruction/disposal will be secured against unauthorized or inappropriate access until the destruction/disposal of the PHI is complete.

F. The Privacy Coordinator or designee must ensure that a record of all destruction/disposal of original patient records/media contained within the patient's Designated Record Set or other original documents containing PHI will be made and retained **permanently** regardless of whether the destruction/disposal is done by FIU or by a contractor (Business Associate). Permanent retention of the destruction/disposal record is required because the records of destruction/disposal may be needed to demonstrate that the records containing PHI were destroyed/disposed of in the regular course of business.

G. The Privacy Coordinator or designee must ensure that records of destruction/disposal include:
   1. date of destruction/disposal,
   2. method of destruction/disposal,
   3. description of the destroyed/disposed record series or medium,
   4. inclusive dates covered,
   5. a statement that the records containing PHI were destroyed/disposed of in the normal course of business, and
   6. the signatures of the Privacy Coordinator or designee supervising and witnessing the destruction/disposal.

   (See Attachment A: Component Verification of Destruction of Protected Health Information form)

H. Business Associate Agreements (BAA) must provide that, upon termination of the contract, the business associate will return or destroy/dispose of all PHI. If such return or destruction/disposal is not feasible, the BAA must limit the use and disclosure of the information to the purposes that prevent its return or destruction/disposal. (FIU Policy and Procedure #1660.015) (Business Associate Agreements)

I. Upon termination of the contract, Business Associates must provide FIU with a Certificate of Destruction when the business associate has destroyed/disposed of patient PHI or when the destruction of patient PHI is infeasible. (FIU Policy and Procedure #1660.015) (Business Associate Agreements)

(See Attachment B: Sample Certificate that Protected Health Information Maintained by Business Associate Has Been Destroyed or Destruction is Infeasible form)

. **Destruction/Disposal Services Contracted to an Outside Vendor**

A. If the destruction/disposal services are contracted to an outside vendor (Business Associate), the contract and BAA must provide that the Business Associate will establish the permitted and required uses and disclosures of information by the Business Associate as set forth in federal and state law *(As outlined in FIU's HIPAA Business Associated Agreement)*. The BAA will set minimum acceptable standards for the sanitization of media containing PHI. The BAA or contract should include, but not be limited to the following:

1. specify the method of destruction/disposal (such method must be consistent with those set forth in Section III(A) below),
2. specify the time that will elapse between acquisition and destruction/disposal of data/media containing PHI,
3. establish safeguards against unauthorized disclosures and breaches in confidentiality,
4. indemnify FIU from loss due to unauthorized disclosure, and
5. provide proof of destruction/disposal (i.e., Certificate of Destruction)

(See FIU Policy and Procedure #1660.015 regarding Business Associate Agreements)

III. **PHI will be Destroyed/Disposed of Using a Method That Ensures the PHI Cannot be Recovered or Reconstructed.**

A. Any media containing PHI should be destroyed/disposed of using a method that ensures the PHI could not be recovered or reconstructed. Some appropriate methods for destruction/disposal are outlined in the following table.

Medium	Recommendation
Audiotapes	Methods for destroying/disposing of audiotapes include recycling (tape over) or pulverizing.
Computerized Data/Computers & Hard Disk Drives (including within some fax machines and copiers)	Methods of destruction/disposal should destroy/dispose of data permanently and irreversibly. Methods may include overwriting data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy/dispose of the data, but merely deletes the filename from the

	directory, preventing easy access and making the sector available on the disk so it may not be overwritten. Total data destruction/disposal does not occur until back-up computerizes data used or created for redundancy purposes have been overwritten or destroyed.
Computer Data/ Magnetic Media or devices including USB drives or SD cards	Methods of destruction may include overwriting data with a series of characters or reformatting the tape (destroying everything on it). Total data destruction does not occur until back-up media or devices used or created for redundancy purposes have been overwritten or destroyed. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. Shredding or pulverization should be the final disposition of any removable media when it is no longer usable.
Handheld devices including cell phones, smart phones, PDAs, tablets and similar devices	Software is available to remotely wipe data from handheld devices. This should be standard practice. Any removable FIU issued/owned media that is used by these handheld devices should be handled as specified in the previous paragraph. When a handheld device is no longer reusable it should be totally destroyed by recycling in a manner specified in FIU Security Policy and Procedure.
Optical Media	Optical disks cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.
PHI Labeled Devices, Containers, Equipment, Etc.	Reasonable steps should be taken to destroy or de-identify any PHI information prior to disposal of this medium. Removing labels or incineration of the medium would be appropriate. Another option is to obliterate the information with a heavy permanent

	marker pen. Ribbons used to print labels may contain PHI and should be disposed of by shredding or incineration.
Computer Diskettes	Methods for destroying/disposing of diskettes include reformatting, pulverizing, or magnetic degaussing.
Laser Disks	Disks used in "write once-read many" (WORM) document imaging cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.
Microfilm/Microfiche	Methods for destroying/disposing of microfilm or microfiche include recycling and pulverizing.
Paper Records	Paper records should be destroyed/disposed of in a manner that leaves no possibility for reconstruction of information. Appropriate methods for destroying/disposing of paper records include: burning, shredding, pulping, and pulverizing. If shredded, use crosscut shredders which produce particles that are 1 x 5 millimeters or smaller in size.
Videotapes	Methods for destroying/disposing of videotapes include recycling (tape over) or pulverizing.

IV. **Additional Information on Disposal of Discarded Paper Containing PHI**.

A. On occasion, when copying or faxing documents containing PHI, additional copies are made which are not subject to a retention schedule (because they are copies, not originals) and which may be disposed of immediately after the purpose for which they were made has been fulfilled. Such paper copies may be disposed of in recycle bins or waste receptacles only as described below:

1. Unsecured recycle bins/waste receptacles should be located in areas where the public will not be able to access them.

2. When possible, dispose of paper waste containing PHI in receptacles that are secured by locking mechanisms or that are located behind locked doors after regular business hours. Locked containers must be used with copy machines located in insecure or unattended areas.

3. Paper documents containing PHI may be placed in recycle bins/waste receptacles as described above in Section IV(A) only if the paper in such bins or receptacles will be disposed of in a manner that leaves no possibility for reconstruction of the information as described in the chart in Section III(A). above.

B. The Director of Compliance for Health Affairs and the HIPAA Security Officer will ensure that the methods of destruction/disposal are (re)assessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction/disposal services.

V. **Documentation Requirements**

A. A record of all destruction/disposal of original medical/patient records or other original documents containing PHI will be made and retained permanently as described above in Section I(F) and (G) using the attached form or a form substantially similar to the attached form available at compliance@fiu.edu.

VI. **Forms**

- Attachment A: Sample Component Verification of Destruction of Protected Health Information form
- Attachment B: Sample Certificate that Protected Health Information Maintained by Business Associate Has Been Destroyed or Destruction is Infeasible form

Attachment A

Sample

Component Verification of Destruction of Protected Health Information

The information described below was destroyed in the normal course of business pursuant to a proper retention schedule and destruction processes as defined by FIU policies and procedures.

Facility/Component
Name:_____

Date of destruction:_____

Description of records or record series disposed of:
_____
_____
_____

Inclusive dates covered:_____

Method of destruction:
( ) Burning ( ) Shredding ( ) Pulping ( ) Demagnetizing
( ) Overwriting ( ) Pulverizing ( ) Other: _____

Records destroyed by:_____
Name Title

Witness signature:_____
Name Title

Component manager: _____
Name Title

Attachment B

Sample

Certification that Protected Health Information Has Been Destroyed or Destruction is Infeasible

Effective _____, Business Associate and Florida International University (FIU) entered into a Business Associate Agreement.

Such Agreement has terminated, and Business Associate hereby certifies with respect to the protected health information (PHI) that Business Associate received as part of the Agreement that Business Associate has:

- ☐ Destroyed the original and all copies of the protected health information
- ☐ In conjunction with FIU, determined that returning or destroying the protected health information is infeasible. **In this case, Business Associate agrees that it may continue to use such PHI for those purposes that make the return or destruction infeasible and shall continue to protect such PHI as required under this Agreement for so long as the Business Associate maintains such PHI. Business Associate further agrees that it will either return PHI to FIU or attest to its proper destruction if, at any time, the circumstances that made return or destruction of the information infeasible are no longer present.**

On Behalf of Business Associate:

_____
Signature

_____
Printed Name

_____
Title

_____
Date

Filing Instructions: A copy of this form should be filed with the FIU Office of University Compliance & Integrity, Modesto Maidique Campus, PC 429, 11200 S.W. 8th Street, Miami, Florida 33199. Please keep a copy for your own records, as you may be asked by FIU to verify that you have received the certification.