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	August 6, 2025	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 Component (hereinafter facility or 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)

Facilities 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 or program Privacy and Security Coordinator 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 harmonized consistent with the requirements of HIPAA 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 the FIU Components (hereinafter 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

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

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.

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.

HIPAA Components (Facilities and Programs):

- Each FIU HIPAA Hybrid Designated Component (hereinafter facility and program) must designate a Privacy and a Security Coordinator responsible for overseeing and ensuring the facility's or program'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 statutes, 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 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: 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; August 6, 2025.

FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

Destruction/Disposal of Protected Health Information # 1660.115a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
August 31, 2021	August 6, 2025	Office of Compliance and Integrity

PROCEDURE STATEMENT

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

Facility and program Privacy Coordinator are responsible for overseeing and ensuring their facility's or program'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 the 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 facility or program 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/ePHI. 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/ePHI or when the destruction of patient PHI/ePHI is unfeasible. (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/ePHI,
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/ePHI 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 Facility or Program (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

Facility or Program 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 or Program

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

Facility or Program 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.