



De-identification and Re-identification of Protected Health Information and Limited Data Sets # 1660.140

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 1, 2009	August 6, 2025	Office of Compliance and Integrity

POLICY STATEMENT

Each Florida International University (FIU) Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Health Care Component (hereinafter facility and program) must determine whether health information is protected health information (PHI) and whether de-identification must occur when there is no "need to know" the identity of the patient. This determination will be made on a case-by-case basis and depend on the nature of the request for the use or disclosure of PHI.

NOTE: HIPAA does not apply to de-identified data.

FIU health care practitioners/providers licensed under Florida Statute chapter 457; chapter 458; chapter 459; chapter 460; chapter 461; chapter 462; chapter 463; chapter 464; chapter 465; chapter 466; chapter 467; part I, part II, part III, part V, part X, part XIII, or part XIV of chapter 468; chapter 478; chapter 480; part II or part III of chapter 483; chapter 484; chapter 486; chapter 490; or chapter 491 **WILL NOT** use or disclose PHI for statistical and scientific research, unless the medial records and the medial condition (information) of the patient is abstracted in such a way as to protect the identity of the patient or provided written permission is first obtained from the patient or the patient’s legal representative. (Florida Statute §456.057)

Facility and program Administrative Officers, Privacy Coordinators, and/or Designees must verify the identity of a person or entity requesting de-identified PHI and the authority of any such person or entity to have access to the information, if the identity or authority of the person or entity is not known to the facility or program. The facility or program Administrative Officers, Privacy Coordinators, and/or designee must obtain any documentation, statements, or representations, whether oral or written, from the person or entity requesting the information when such documentation, statement, or representation is a condition of the disclosure. (FIU Policy and Procedure #1660.040) (Verification)

PHI used or disclosed for statistical and scientific research purposes must be approved by FIU Office of Research and Economic Development (ORED).

NOTE: See Use of Protected Health Information for Research Purposes (ORED Policy and Procedure #2370.520), Use of Decedent Protected Health Information (ORED Policy and

Procedure #2370.521), Limited Data Sets and Data Use Agreements (ORED Policy and Procedure #2370.522), Waiver or Modification of Authorization (ORED Policy and Procedure #2370.515), and Certification of Review Preparatory to Research (ORED Policy and Procedure #2370.510)

Facility and programs are expected to develop procedures or protocols supplementing this policy and procedure when facility and program-specific procedures are needed. As a University-wide policy and procedure approved by the HIPAA Steering Committee, Facility and program Privacy Coordinators, the Office of Compliance and Integrity, and the Office of General Counsel, this policy and procedure takes precedence over any facility and program-specific policies, procedures, or protocols that conflicts with this policy and procedure, unless prior approval is obtained from the Office of Compliance and Integrity.

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, each facility and program Privacy Coordinator will be responsible for maintaining all HIPAA documentation relevant to his/her facility and 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 state law and regulation. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

SCOPE

The policy applies to FIU's HIPAA Health Care 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 Associates.



REASON FOR POLICY

To establish a policy and procedure necessary for the creation, use and disclosure of de-identified information, reidentification, Limited Data Sets and Date Use Agreements, Business Associate Agreements and the requirement for written patient permission as described in the HIPAA Privacy and Security Rules, federal law, Florida state statute, and FIU Associated Policies and Procedures.

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 facility and program must designate a Privacy Coordinator responsible for overseeing and ensuring the facility’s and 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 ePHI, including, but not limited to the creation of deidentified PHI, Limited Data Sets, and the use, and disclosure of PHI for research and non-research purposes.

Office of Research and Economic Development

Review and approve all research activities involving the use or disclosure of patient

RELATED RESOURCES

References

- 45 CFR §164.501
- 45 CFR §164.502
- 45 CFR §164.504
- 45 CFR §164.508
- 45 CFR §164.512
- 45 CFR §164.514
- 45 CFR §164.528
- 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 #1640.015 (Notice of Privacy Practices)
- FIU Policy and Procedure #1640.025 (Minimum Necessary)
- FIU Policy and Procedure #1660.015 (Business Associates)
- FIU Policy and Procedure #1660.020 (Authorization for Use and Disclosure of Patient Protected Health Information)
- FIU Policy and Procedure #1660.025 (Uses and Disclosures of Protected Health Information for which an Authorization or Opportunity for the Patient to Agree or to Object is NOT Required)
- FIU Policy and Procedure #1660.040 (Verification)
- 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)

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: September 1, 2009

Review Dates (*review performed, no updates*): n/a

Revision Dates (*review performed, updates made to document*): December 31, 2017; April 2021 (renumbered from 1640.040); August 31, 2021; February 29, 2024; August 6, 2025.



De-identification and Re-identification of Protected Health Information and Limited Data Sets # 1660.040a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 1, 2009	August 6, 2025	Office of Compliance and Integrity

PROCEDURE STATEMENT

I. De-identification and Reidentification of Patient Protected Health Information (PHI)

Component (hereinafter facility and program) Privacy Coordinators are 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 Florida state statutes governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI), including, but not limited to receiving and processing requests for de-identified protected health information and Limited Data Sets for research and non-research purposes. 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. Privacy Coordinators may determine that PHI is not individually identifiable PHI (de-identified) in the following two ways:

1. Removal of Identifiers. The facility or program Privacy Coordinator **MUST** remove the following identifiers of the patient and the patient’s relatives, employers or household members:
 - a. Names;
 - b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geographic codes. However, the initial three digits of a zip code may remain on the information if, according to current publicly-available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic unit containing 20,000 or fewer people is changed to 000;
 - c. All elements of dates (except year) for dates directly relating to a patient, including birth date, dates of admission and discharge from a health care facility, and date of death. For patients age 90 and older, all elements of

dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of "age 90 or older,"

- d. Telephone numbers;
- e. Fax numbers;
- f. Electronic mail addresses;
- g. Social security numbers;
- h. Medical record numbers;
- i. Health plan beneficiary numbers;
- j. Account numbers;
- k. Certificate or license numbers;
- l. Vehicle identifiers and serial numbers, including license plate numbers;
- m. Device identifiers and serial numbers;
- n. Web Universal Resource Locators (URLs);
- o. Internet Protocol (IP) address numbers;
- p. Biometric identifiers, including fingerprints and voiceprints;
- q. Full face photographic images and any comparable images; and
- r. Any other unique identifying number, characteristic, or codes.

NOTE: This method requires that the facility or program Privacy Coordinator **DOES NOT** have actual knowledge that the remaining information could be used alone or in combination with other information to identify the patient.

2. Statistical Method. The facility and program Privacy Coordinator may employ a designated entity or individual with knowledge and experience of generally accepted statistical and scientific principles and methods for rendering information not individually identifiable PHI, if the entity or individual applies such methods and determines that the risk is very small that the information could be used alone, or in combination with other available information, by an anticipated recipient of such information to identify the patient(s).
 - a. The Privacy Coordinator **MUST** document the selected designated entity's or individual's knowledge and experience necessary to perform the de-identification prior to disclosing any PHI to the designated entity or individual.
 - b. The Privacy Coordinator **MUST** ensure the designated entity or individual selected documents the method and results of the analysis that justify the determination.
 - c. The Privacy Coordinator **MUST** ensure the de-identification will be

performed at the data source, or, in the case of the de-identification is made by the designated entity or individual named in (I)(A)(2), immediately above, where such designated entity or individual is located, as appropriate.

B. Reidentification. The facility or program Privacy Coordinator, designated entity or individual performing the de-identification may assign a code or other means of record identification to allow information de-identified under this policy and procedure to be reidentified by the facility or program Privacy Coordinator, except that:

1. The code or other means of record identification is not derived from or related to information about the patient(s), and
2. Cannot otherwise be translated to identify the patient(s); and
3. The designated entity or individual does not use or disclose the code or other means of record identification for any other purpose, and
4. The designated entity or individual does not disclose the mechanism for reidentification to anyone other than the facility or program Administrative Officer, Privacy Coordinator, or Designee.

1. The facility or program Privacy Coordinator, designated entity or individual **MUST** document and secure the code or other means of record identification to allow information de-identified under this policy to be reidentified by the facility or program Privacy Coordinator.

NOTE: The facility or program Privacy Coordinator, designated entity, or individual may de-identify hardcopy PHI by obliterating (making unreadable and unrecognizable) the 18 identifiers.

NOTE: Regardless of the method by which de-identification is achieved, the Privacy Rule does not restrict the use or disclosure of de-identified PHI, as it is no longer considered PHI.

NOTE: Disclosure of a code or other means of re-identification constitutes disclosure of PHI.

NOTE: De-identified information that is reidentified is subject to the HIPAA Privacy Rule.

C. Business Associates

1. If the designated entity or individual employed to create de-identified data is not a Workforce member of the FIU facility or program, the Privacy

Coordinator **MUST** ensure that a signed Business Associate Agreement is received from the designated entity or individual prior to disclosing any PHI to the designated entity or individual to create the de-identified data from a broader set of PHI. (FIU Policy and Procedure #1660.015) ((Business Associates Agreements)

II. Limited Data Sets, Business Associate Agreements and Memorandums of Understanding

- A. FIU facility and program Workforce members may use and disclose a Limited Data Set for non-research purposes when more information than is included in de-identified information is needed and without patient written authorization only for:
1. Public Health Activities when required or permitted by Federal and/or Florida state statutes,
 2. Healthcare Operations performed by FIU facility or program Workforce members or FIU HIPAA Hybrid Designated facilities or programs, unit Workforce members on behalf of a health care facility or program. Health Care Operations performed by FIU Workforce members who are not employed within an FIU HIPAA Hybrid Designated facility or program, or by an external individual or entity requires a Memorandum of Understanding (MOU) or Business Associate Agreement (BAA), as determined by the Office of Compliance and Integrity or the Office of General Counsel.
- B. Facility and program Privacy Coordinators, designated entities, and/or individuals who create Limited Data Sets **MUST** remove the following identifiers of the patient and the patient's relatives, employers or household members from the PHI in order to create a Limited Data Set:
- a. Names;
 - b. Street address (other than town or city, state, and zip code);
 - c. Telephone numbers;
 - d. Fax numbers;
 - e. Electronic mail addresses;
 - f. Social Security Numbers;
 - g. Medical record numbers;
 - h. Health plan beneficiary numbers;
 - i. Account numbers;
 - j. Certificate/License numbers;
 - k. Vehicle identifiers and serial numbers (including license plate numbers);
 - l. Device identifiers and serial numbers;
 - m. Web universal resource locators (URLs);
 - n. Internet protocol (IP) address numbers;
 - o. Biometric identifiers including finger and voice prints; and
 - p. Full face photographic images and any comparable images.

NOTE: The health information that may remain in the information disclosed in a Limited Data Set includes:

- a. Geographic data (town, city, state, and zip code, but no street address).
- b. All dates relating to the individual (e.g. birth date, admission, discharge or service date).
- c. Ages in years, months or days or hours.
Other unique identifiers (any unique number, characteristic or code other than those specified in the list of 16 identifiers that are expressly disallowed).

NOTE: It is important to note that Limited Data Set information is still PHI as defined by HIPAA. It is not de-identified information and is therefore subject to the requirements of the HIPAA Privacy Rules and Florida state statute. (See **NOTE** immediately below in II(C))

- C. The Privacy Coordinator must ensure the creation of the Limited Data Set will be performed at the data source, or, in the case of the Limited Data Set is made by an external designated entity or individual, where such designated entity of individual is located, as appropriate.
- D. If the designated entity or individual employed to create a Limited Data Set is not a Workforce member of the FIU health care facility or program, the Privacy Coordinator **MUST** ensure that a signed Business Associate Agreement is received from the designated entity or individual prior to disclosing any PHI to the designated entity or individual to create a Limited Data Set from a broader set of PHI. (FIU Policy and Procedure #1660.015) ((Business Associates Agreements)

NOTE: Once the Limited Data Set is created under the Business Associate Agreement for the FIU health care facility or program, all of the PHI, other than the PHI qualifying as the Limited Data Set must be returned to the FIU health care facility or program.

NOTE: Health Care Providers/Practitioners as identified in Florida Statute Chapter §456.057 MAY disclose PHI for statistical and scientific research, provided the information is abstracted in such a way as to protect the identity of the patient or provided written permission is received from the patient or the patient's legal representative. (Florida Statute §456.057) Because a Limited Data Set does not protect the identity of the patient, written permission (Authorization) **MUST** be obtained from the patient.

- E. For Limited Data Sets for research purposes see the FIU Office of Research and



Economic Development (ORED) Policy and Procedure #2370.522 and ORED Policy and Procedure #2370.520 (Use of Protected Health Information for Research Purposes).

III. 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)