FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Designated Record Set # 1660.110

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

POLICY STATEMENT

Under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, federal law, and Florida state statutes, patients have access to, may request copies of, and may request amendments of their protected health information (PHI) in their Designated Record Set (DRS). Florida International University (FIU) HIPAA Hybrid Designated Components (hereinafter facilities and programs) must specifically define, maintain and allow a patient who is the subject of the Protected Health Information (PHI) or their legal representative (FIU Policy and Procedure #1660.001) (Representatives) certain rights to a DRS per the procedure outlined below. The DRS will encompass information beyond the traditional medical record and billing record. Healthcare providers must include information received from another healthcare provider during the patient's visit in their DRS unless the healthcare provider has documented facts that the information was not used in whole or in part to make a decision about the patient.

As a University-wide policy and procedure, this policy and procedure takes precedence over any 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 and program Privacy Coordinators will be 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 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 the policy and FIU Policy and Procedure #1660.015 regarding Business Associate Agreements.

REASON FOR POLICY

The reason for this policy and procedure is to address what constitutes a Designated Record Set (DRS) and to provide guidance regarding the creation and maintenance of Designated Record Sets as required by HIPAA 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.

HIPAA Components (Facilities and Programs):

- Each FIU HIPAA Hybrid Designated Component (hereinafter facility and program) must designate a Privacy Coordinator responsible for overseeing and ensuring the facility's or program's implementation and compliance with the HIPAA Privacy Rule, FIU's associated HIPAA Privacy Policies and Procedures, and any applicable Florida state statutes governing the confidentiality, integrity and availability of PHI and ePHI.
- Creating and maintaining DRSs.

Compliance Oversight: The Division of Information Technology

- Evaluates all federal and state healthcare security laws, regulations, rules and ordinances (Rules) to ensure compliance with the Rules.
- Develops and maintains all required University-wide Security Rule policies and procedures.
- Develops and maintains HIPAA Security Rule training modules and ensures appropriate Workforce members complete the required training.
- Performs audits and assessments of the facilities and programs to ensure their compliance with the Security Rules and associated FIU Policies and Procedures.
- Partners with the Office of Compliance and Integrity Director of Compliance and Privacy for Health Affairs to ensure compliance with all federal and state healthcare privacy and security laws, regulations rules, and ordinances.

RELATED RESOURCES

References

- 45 CFR §164.501
- 45 CFR §164.502
- 45 CFR §164.504
- 45 CFR §164.524
- 45 CFR §164.526
- Florida Statute §95.11
- Florida Statute §456.057

Related Policies

- FIU Policy and Procedure # 1610.005 (Designated Health Components of FIU Community)
- FIU Policy and Procedure #1660.001 (Representatives)
- FIU Policy and Procedure #1660.015 (Business Associate Agreements)
- FIU Policy and Procedure #1660.045 (Right of Patients to Request Restrictions Regarding the Use and Disclosure of Their Protected Health Information)
- FIU Policy and Procedure #1660.050 (Patient Access to Protected Health Information)
- FIU Policy and Procedure #1660.055 (Amendment of Protected Health Information)
- 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: 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

Designated Record Set #1660.110a

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

PROCEDURE STATEMENT

I. Creation and Maintenance of Patient Designated Record Sets (DRS)

Component (hereinafter facility and program) Privacy Coordinators are responsible for overseeing and ensuring their facility's or program's implementation and compliance with the HIPAA Privacy Rule, federal law, Florida state statutes, and FIU's associated HIPAA Privacy Policies and Procedures governing the confidentiality, integrity and availability of patient Protected Health Information (PHI) and electronic PHI (ePHI), including, but not limited to, specifying in writing which forms and reports, when present in a patient's paper or electronic file, will be included in the Designated Record Set (DRS) based on the HIPAA definition of a DRS. 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 Facility and Program Privacy and Security Coordinators)

Each Healthcare facility or program must at a minimum include the following forms and reports in a patient's DRS. (See Attachment A)

II. Record Retention

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

III. Forms

- Attachment A (Examples of items that make-up a DRS)

Attachment A (Example of items that make-up a DRS)

INCLUDES	EXAMPLES
Medical Practice (Clinical)	• Advanced Directives • Allied Health Reports (OT/PT, Speech Therapy, Nutrition, etc.) • Anesthesia records • Authorization forms • Cardiology reports • Care plans • Consent forms (i.e., Informed Consent and General Consent for Treatment) • Consultation reports • Copies from physician offices or other healthcare facilities used to make health care decisions, such as a history and physical examination or surgical records • Correspondence (i.e., referral letters, record requests, etc.) • Discharge reports (i.e., summary, progress note, instructions) • Documentation of miscellaneous services, including social service, case management, food and nutrition, physical therapy, speech therapy, occupational therapy, respiratory treatments, arterial blood gas reports, and ventilator sheets • Documented communications between provider and patient • Face-sheet • History and Physical Examination Report or Prenatal Record • Informed consent forms for items such as surgery, blood, and dialysis • Interdisciplinary education record • Immunization records • Laboratory Reports/Results, including blood typing or crossmatching (not requisitions for lab tests) • Medication Administration Records • Nursing documentation, including items such as vital sign graphics, intake and output records, neurocheck, medication sheets, intravenous fluid flow sheets, shift assessments, nursing notes, telemetry, admission history, care plan, discharge instructions, and release of body form. • Operative/Procedure records • Order or prescription for a test/treatment

	• Other Diagnostic Reports (i.e., EEG, EKG, EMG, NCV, Echo, etc.) • Pathology reports • Patient education records/discharge instructions • Peri-operative documentation, including items such as surgery checklist, anesthesia records, intraoperative nursing forms, and recovery room forms • Problem list • Progress notes (including medical student notes that are co-signed by the supervising physician (with or without an addendum)) • Provider Orders • Imaging/Radiology reports • Registration Record • Selected photographs • Transfer Records • Transport Records
Billing Records	• Coding summary • Complete statement of account containing billing history • Open balance statement • Receipt for service (per encounter date) • Financial agreement w/private patients • Requests/Denials for amendments/corrections • Financial payment arrangement • Encounter forms • Paper claims • Other Patient specific claims, remittance, eligibility response and claim status response, charge screen, statement of account balance, payment agreement
Business Associate Records	• Records held by a Business Associate that meet the definition of DRS.
DRS DOES NOT INCLUDE	**EXAMPLES**
Source Documentation	The following information is usually considered part of the source data of the DRS. In most cases, patients cannot interpret source data, so such data is meaningless. There may be times, however, when a patient has a legitimate need to access source data. When such a need arises, the health care facility or program Unit will want to provide the patient with greater rights of access, allowing the patient access to or copies of the source data when possible. A specific request, authorization or subpoena is required to produce the original or to obtain a copy (if retained and/or able to copy) of this information: • Endoscopy photographs

	• Photographs that taken in the operation/emergency room and are not maintained as part of the medical record. • All release of information related correspondence (e.g., requests for copies from insurance companies, authorization forms, interdepartmental requests for records, and fax cover sheets) as long as the documents are not maintained in the EMR • Psychotherapy Notes as defined by the Standards for Privacy of Individually Identifiable Health Information (§164.501) • Peer review information • Incident reports • Infection control reports • Administrative, attorney-client privileged and any other protected reports • Medical student notes not co-signed by the supervising physician • Temporary notes or worksheets, reminders, and concurrent coding worksheets • Incomplete record coversheets, • clarification notes to/from physicians, etc.
Related to Risk Management, Quality Improvement	• Quality Improvement/Peer review records • Risk Management records • Information compiled in reasonable anticipation of, or for use in civil, criminal, or administrative action or proceeding (e.g., Incident Reports- used to identify problems and implement corrective action, attorney notes)
Employment Related	• Results of HIV tests maintained by the employee health nurse for employees who incur needle stick injuries while at work • Employer records
Student Health Records	• Student education records (e.g., records protected under the Family Educational Rights and Privacy Act ("FERPA")
Health Information Generated, Collected, or Maintained for Purposes that do not include decision-making about the patient.	• Birth and Death Registers • Cancer Registry • Trauma Registry • Diagnostic or Operative Indexes • Copies of reports/documentation/forms, i.e. "shadow files", wherein the originals are maintained in an 'official' record maintained by the healthcare Facility or program. • Appointment and surgery schedules
Laboratory/Clinical	• Administrative records created or maintained by FIU administrative personnel and offices/units that perform support functions on behalf of other Health Care Facility or programs as

	defined in FIU Policy and Procedure #1610.005 (Designated Health Care Facility or programs of FIU Community)
Business Associates	Business associate records that meet the definition of DRS but are merely duplicate information maintained by the organization, e.g., dictated notes
Research	Data collected and maintained for research
External/Outside Medical Records	Medical records created by treating entities or providers other than the FIU Unit that have not been used to make a decision about the patient.