



Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators #1660.070

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 13, 2020	February 29, 2024	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 designate a HIPAA Privacy Coordinator responsible for overseeing and ensuring the Component’s implementation and compliance with the HIPAA Privacy Rule, federal laws, Florida state statutes, and FIU’s associated HIPAA Privacy Policies and Procedures governing the confidentiality, integrity and availability of PHI and electronic PHI (ePHI).

Each Component must designate a HIPAA Security Coordinator responsible for overseeing and ensuring the Component’s implementation and compliance with the HIPAA Security Rule, FIU’s associated HIPAA Security Policies and Procedures, and any associated or applicable state laws and/or regulations governing the administrative, physical, and technical safeguards of PHI and ePHI.

The Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity, is the designated privacy official responsible for the development and implementation of the HIPAA Privacy Rule policies and procedures for Florida International University (FIU).

Each HIPAA Component must notify the Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity (Designated HIPAA Privacy Officer), and the HIPAA Security Officer, Division of Information Technology, of the names and titles of their designated HIPAA 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 #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)

SCOPE

The policy applies to the FIU’s Health Care Components that are contained within FIU’s HIPAA Hybrid Designation (FIU Policy and Procedure #1610.005) and its Workforce members as defined in this policy and policy # 1610.005.

REASON FOR POLICY

To ensure that FIU Workforce members understand the critical significance of complying with FIU’s HIPAA Privacy and Security Rules Policies and Procedures and applicable federal laws 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 <u>system</u> 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 <u>security measures</u> to protect electronic protected health information 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 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

	<p>PHI. This includes, but not limited to, claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management or repricing.</p> <p>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.</p>
Business Associate Agreement	Means a contract or other written arrangement with a business associate which must describe the permitted and required uses of protected health information by the business associate; provide that the business associate will not use or further disclose the protected health information 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 protected health information other than as provided for by the contract.
Breach	Means the unauthorized acquisition, access, use, or disclosure of Protected Health Information (PHI) that compromises the security or privacy of the data and poses a significant risk of financial, reputational, or other harm to the client.
Code of Federal Regulations	Also known as CFR is the codification of the general and permanent regulations promulgated by the executive departments and agencies of the federal government of the United States.
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. <ol style="list-style-type: none"> 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.
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 Health Information (ePHI)	PHI in electronic form. See also: <u>PHI</u> .
Florida Statutes	Also known as F.S. are the codified, statutory laws of Florida.
Health Care	Means the care, services, or supplies related to the health of a patient, including: <ol style="list-style-type: none"> 1. preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of a patient or that affects the structure or function of the body; and 2. sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
Health Care Component	See "Component"
Health Care Operations	Means any of the following activities: <ol style="list-style-type: none"> 1. quality assessment and improvement activities, including case management and care coordination; 2. competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; 3. conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; 4. specified insurance functions, such as underwriting, risk rating, and reinsuring risk; 5. business planning, development, management, and administration; and 6. business management and general administrative activities of the entity, including but not limited to: <ol style="list-style-type: none"> a. de-identifying protected health information, b. creating a limited data set, and c. certain fundraising for the benefit of the covered entity.
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; the provision of health care to an patient; or the past, present, or future payment for the provision of health care to an patient.
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.
Individually Identifiable Health Information	Means information that is a subset of health information, including demographic information collected from an individual, and <ol style="list-style-type: none"> 1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and 2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and <ol style="list-style-type: none"> a. That identifies the individual; or b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
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 the PHI.
Physical safeguards	The physical measures, policies, and procedures to protect a covered entity's or business associate's electronic <u>information systems</u> 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

	<p>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.</p>
Protected Health Information (PHI)	<p>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:</p> <ol style="list-style-type: none"> 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	<p>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.</p>
Technical safeguards	<p>Means the technology and the policy and procedures for its use that protect electronic protected health information and control <u>access</u> to it.</p>
Secretary	<p>Means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.</p>
Standard	<p>Means a rule, condition, or requirement:</p> <ol style="list-style-type: none"> 1. Describing the following information for products, systems, services, or practices: <ol style="list-style-type: none"> a. Classification of components; b. Specification of materials, performance, or operations; or c. Delineation of procedures; or 2. With respect to the privacy of protected health information.
Treatment, payment, and healthcare operations	<p>Also known as TPO</p>

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 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 Administrative Officer 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).

RELATED RESOURCES

References

- 45 CFR §164.502
- 45 CFR §164.504
- 45 CFR §164.506
- 45 CFR §164.508
- 45 CFR §164.510
- 45 CFR §164.512
- 45 CFR §164.514
- 45 CFR §164.520
- 45 CFR §164.522
- 45 CFR §164.524
- 45 CFR §164.526
- 45 CFR §164.528
- 45 CFR §164.530
- Florida Statute §456.057(11)
- Florida Statute §95.11

Related Policies

- FIU Policy # 1610.005 (Designated Health Care Components of FIU Community)
- 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 #1660.120 (Minimum Necessary)
- FIU Policy and Procedure #1660.080 (Policies and Procedures, Changes to Policies and Procedures, and Documentation)
- FIU Policy and Procedure #1660.020 (Authorization for Use and Disclosures of Patient Protected Health Information)
- FIU Policy and Procedure #1640.015 (Notice of Privacy Practices)
- FIU Policy and Procedure #1660.030 (Uses and Disclosures of Patient Protected Health Information Requiring an Opportunity for the Patient to Agree or to Object)
 - Use and Disclosure for Facility Directory and to the Clergy.
 - Use and Disclosure to Individuals Involved in the Patients Case and for Notification Purposes.
- FIU Policy and Procedure #1660.025 (Uses and Disclosures of Patient Protected Health Information for Which an Authorization of Opportunity to Agree or to Object is NOT Required)
- FIU Policy and Procedure #1660.140 (De-identification and Reidentification of Protected Health Information, Use of Limited Data Sets, and Data Use Agreements.
- FIU Policy and Procedure #1660.005 (Right of Patients to Request Confidential Communications Regarding the Use and Disclosure of Their Protected Health Information)
- FIU Policy and Procedure #1660.040 (Verification)

- FIU Policy and Procedure #1660.060 (Accounting of Disclosures of Protected Health Information)
- FIU Policy and Procedure #1660.035 (Use and Disclosure of Patient Protected Health Information for Fundraising Purposes)
- 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 #1660.060 (Accounting of Disclosure of Protected Health Information)
- FIU Policy and Procedure #1660.065 (Complaints Under the HIPAA Privacy Rule, Mitigation, Refraining from Intimidating or Retaliatory Acts, and Waiver)
- FIU Policy and Procedure #1660.095 (Reporting of HIPAA Incidents and Notification in Case of a Breach)
- FIU Policy and Procedure #1660.090 (HIPAA Component Privacy Review and Audit)

CONTACTS

For further information concerning this policy, please contact the FIU Office of Compliance and Integrity at (305) 348-2216, compliance@fiu.edu, hipaaprivacy@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 (*review performed, updates made to document*): October 13, 2020; February 29, 2024.



Designation of HIPAA Privacy Officer and Component Privacy and Security Coordinators #1660.070a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
October 13, 2020	February 29, 2024	Office of Compliance and Integrity

PROCEDURE STATEMENT

Each Florida International University (FIU) Health Insurance Portability and Accountability Act (HIPAA) Hybrid Designated Health Care Component (Component) must designate a HIPAA Privacy Coordinator responsible for overseeing and ensuring the Component’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 PHI and electronic PHI (ePHI).

Each Component must designate a HIPAA Security Coordinator responsible for overseeing and ensuring the Component’s implementation and compliance with the HIPAA Security Rule, federal law, Florida state statutes, and FIU’s associated HIPAA Security Policies and Procedures governing the administrative, physical, and technical safeguards of PHI and ePHI.

Each HIPAA Component must notify the Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity (Designated HIPAA Privacy Officer), and the HIPAA Security Officer, Division of Information Technology, the name and title of their designated HIPAA Privacy and Security Coordinators.

I. Designation of HIPAA Privacy Officer

A. HIPAA Privacy Officer: The Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity, is the designated privacy official responsible for the development and implementation of the HIPAA Privacy Rule policies and procedures for Florida International University (FIU).

II. Designation of Privacy and Security Coordinators

A. Privacy Coordinator: Each FIU HIPAA Hybrid Designated Component (Component) must designate a Workforce member to be the Component’s Privacy Coordinator. The Privacy Coordinator’s responsibilities include, but are not limited to the following:

1. Ensuring that his/her Component has developed applicable Component specific privacy policies and procedures to ensure compliance with the HIPAA Privacy Rule, federal law, and Florida state statutes.
2. Serving as the first point of contact for Workforce members within the Component regarding issues related to FIU HIPAA Privacy Policies and Procedures, the HIPAA Privacy Rule, state law and regulatory compliance.
3. Serving as the initial point of contact for patient complaints that arise from activities within the Component. (FIU Policy and Procedure #1660.065) (Complaints Under the HIPAA Privacy Rule, Mitigations, Refraining From Intimidating or Retaliatory Acts, and Waiver).
4. Serving as the Component's liaison with the Director of Compliance and Privacy for Health Affairs regarding issues related to privacy, the HIPAA Privacy Rule , federal law, and Florida state statute compliance.
5. Ensuring that each Workforce member within the Component has completed and passed the appropriate level of privacy and HIPAA Privacy Rule training by the applicable deadline. (FIU Policy and Procedure #160.075) (HIPAA Privacy and Security Rule Training)
6. Working with the Director of Compliance and Privacy for Health Affairs to ensure 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 Protected Health Information (PHI) and electronic PHI (ePHI), including, but not limited to:
 - Treating a representative as the patient with respect to the HIPAA Privacy Rule and state law. (FIU Policy and Procedure #1660.001) (Representatives)
 - Ensuring that required Business Associate Agreements (BAAs) are obtained prior to allowing Business Associates to create, use, disclose, or access PHI and must ensure BAAs are maintained during the course of the contract or other written agreement. (FIU Policy and Procedure #1660.015) (Business Associate Agreements)
 - Obtaining a written authorization for uses and disclosures of patient PHI. (FIU Policy and Procedure #1660.020) (Authorization for Uses and Disclosures of Patient Protected Health Information)
 - The use and disclosure of patient PHI to individuals involved in the patient's care and for notification purposes. (FIU Policy and Procedure

- #1660.030) (Use and Disclosure of Patient Protected Health Information Requiring an Opportunity for the Patient to Agree or Object)
 - (Use and Disclosure for Facility Directory and to the Clergy)
 - (Use and Disclosure to Individuals Involved in the Patients Case and for Notification Purposes)
- The permitted and required use and disclosure of patient PHI within their Designated Record Set. (FIU Policy and Procedure #1660.020) (Use and Disclosure of Patient Protected Health Information for Which an Authorization or Opportunity to Agree or Object is NOT Required)
- Receiving and processing requests for de-identified patient PHI. (FIU Policy and Procedure #1640.040) (De-identification and Re-identification of Protected Health Information and Use of Limited Data Sets and Data Use Agreements)
- Fundraising to patients. (FIU Policy and Procedure #1660.035) (Use and Disclosure of Patient Protected Health Information for Fundraising Purposes)
- Verifying the identity and authority of the person requesting access to and/or disclosure of PHI. (FIU Policy and Procedure #1660.040) (Verification)
- Receiving and processing requests by patients for restrictions on the use and disclosure of their PHI within their Designated Record Set. (FIU Policy and Procedure #1660.045) (Right of a Patient to Request Restriction Regarding the Use and Disclosure of Their Protected Health Information)
- Receiving and processing requests by patients for confidential communications regarding the use and disclosure of their PHI contained within their Designated Record Set. (FIU Policy and Procedure #1660.045) (Right of a Patients to Request Confidential Communications Regarding the Use and Disclosure of their Protected Health Information)
- Receiving and processing requests by patients for access to the PHI contained within their Designated Record Set. (FIU Policy and Procedure #1660.050) (Patient Access to Protected Health Information)
- Receiving and processing requests by patients for an amendment of their PHI within their Designated Record Set. (FIU Policy and Procedure #1660.055) (Amendment of Protected Health Information)
- Receiving and processing requests by patients for an accounting of disclosures of their PHI. (FIU Policy and Procedure #1660.060) (Accounting of Disclosures of Protected Health Information)
- Ensuring Workforce members and students complete all required Privacy and Security Rule training. (FIU Policy and Procedure #1660.075) (HIPAA Privacy and Security Rule Training)
- Ensuring that any administrative and/or disciplinary action taken against Workforce members found responsible for having committed a

violation(s) and/or a breach(es) is properly administered, documented, and reported to the Director or Compliance and Privacy for Health Affairs and the HIPAA Security Officer with the Information Technology Division. (FIU Policy and Procedure #1660.085) (Sanctions)

- Accepting and processing patient complaints, mitigating, to the extent practicable, any harmful effect that is known to the Component of a use or disclosure of PHI/ePHI in violation of the HIPAA Privacy Rule and FIU's associated HIPAA Privacy Rule Policies and Procedures, ensuring Workforce members and Business Associates refrain from intimidating and retaliatory acts against individuals for exercising any right established under the HIPAA Privacy Rule and FIU's associated HIPAA Privacy Rule Policies and Procedures, or for participation in any process provided by the HIPAA Privacy Rule and FIU's associated HIPAA Privacy Rule Policies and Procedures, including the filing of a complaint, and that individual are not required to waive their right to file a complaint with the Secretary of the federal Department of Health and Human Services (HHS) as a condition of the provision of treatment, payment or eligibility for benefits. (FIU Policy and Procedure #1660.065) (Complaints Under the HIPAA Privacy Rule, Mitigation, Refraining From Intimidating or Retaliatory Acts, and Waiver)
 - Assisting with the development and maintenance of FIU HIPAA Privacy Rule Policies and Procedures and the creation and maintenance of required documentation. (FIU Policy and Procedure #1660.080) (Policies and Procedures, Changes to Policies and Procedures, and Documentation)
 - Receiving and forwarding to the Director of Compliance and Privacy for Health Affairs with the Office of Compliance and Integrity, and/or the HIPAA Security Office with the Division of Information Technology (IT), suspected or known violations and/or breaches. (FIU Policy and Procedure #1660.095) (Reporting of HIPAA Incidents and Notification in the Case of a Breach)
 - Conducting quarterly HIPAA Privacy Rule compliance assessments and assisting with the annual HIPAA Privacy Rule Audit. (FIU Policy and Procedure #1660.090) (HIPAA Component Privacy Review and Audit)
7. Performing other functions as designated in FIU policies and procedures implementing the HIPAA Privacy Rule, federal law, Florida state statutes, and
 8. Making reports to the Director of Compliance and Privacy for Health Affairs, or the Office of Compliance and Integrity as requested, in items #1-7, above.

B. Security Coordinator. Each FIU Component that creates or maintains protected health information in electronic form (ePHI) must designate a Workforce member or Workforce members to act as the Component's Security Coordinator. The Security Coordinator's responsibilities include, but are not limited to the following:

1. Ensuring that his/her Component has developed security policies and procedures where FIU has been silent or does not have applicable HIPAA Hybrid Designated-wide policies and procedures to ensure compliance with the HIPAA Security Rule and state law and/or regulations.
2. Acting as the first point of contact for faculty, staff, and students within the Component regarding issues related to security, HIPAA Security Rule, federal law, and Florida state statutes.
3. Acting as the Component's liaison with the FIU HIPAA Security Officer with the Division of Information Technology regarding issues related to security, the HIPAA Security Rule, federal law, and Florida state statutes.
4. Ensuring that each Workforce member within the Component has taken completed the appropriate level of security and HIPAA Security Rule training by the applicable deadline, and
5. Making reports to the FIU HIPAA Security Officer, or Information Technology Division, as requested, in items #1-4, above.

III. Notification of Designated Privacy and Security Coordinators

1. The Administrative Officer of each Component shall designate the Component's Privacy and Security Coordinators and shall notify the Director of Compliance and Privacy for Health Affairs, Office of Compliance and Integrity, and the HIPAA Security Officer, Division of Information Technology, in writing of the designations and promptly upon any change(s).

NOTE: A Component may designate the same person to act as more than one of its Coordinators.