FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

HIPAA Security: Responsibility for Conducting Risk Assessments with Regards to Electronic Protected Information # 1670.040

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 1, 2009	May 27, 2021	Division of Information Technology/IT Security Office

POLICY STATEMENT

Florida International University departments and units that create, maintain or transmit electronic protected health information shall perform an accurate and thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information maintained or transmitted through them. This risk assessment shall be updated periodically and shall demonstrate, at a minimum, the following information:

- The level of risk associated with each potential vulnerability exploitation.
- Steps to be taken to reduce the risk of vulnerability exploitation.
- Process for maintaining no more than the acceptable level of risk.

The designated HIPAA Security Administrator for the department or unit is responsible for conducting the risk assessment and implementing the necessary risk management procedures. All workforce members of the department or unit shall be trained regarding their appropriate responsibilities and duties to reduce the risk of security incidents.

SCOPE

This policy applies to all Florida International Departments and units that create, maintain or transmit electronic protected health information.

REASON FOR POLICY

Administrative safeguards, HIPAA Security Standards, 45 C.F.R. § 164.308(a)(1).

DEFINITIONS

TERM	DEFINITIONS
Administrative safeguards	Are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected

	health information and to manage workforce conduct in relation to the protection of that information.
HIPAA Security Administrator	Is the individual designated by each health care component to assist in the implementation and maintenance of systems and processes for the creation, maintenance and transmission of protected health information via electronic means and to work in collaboration with the HIPAA Security Officer, HIPAA Privacy Officer and other designated University representatives to ensure that the University creates and maintains an information technology environment that is compliant with applicable federal and state law governing health information privacy and confidentiality.
Individually identifiable health information	Is information that is a subset of health information, including demographic information collected from an individual, and: • Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and • 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 1. That identifies the individual; or 2. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Protected Health Information (PHI)	Means individually identifiable health information that is: • Transmitted by electronic media. • Maintained in electronic media. • Transmitted or maintained in any other form or medium. • Protected Health Information 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.
Workforce or Workforce Member	Means part-time, full-time or temporary faculty and staff, students, volunteers, trainees, and other persons whose conduct, in the performance of work for the University, is under the direct command of the University (regardless of whether or not they are paid by the University).

ROLES AND RESPONSIBILITIES

Florida International University departments and units that create, maintain or transmit electronic protected health information shall perform an accurate and thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information maintained or transmitted through them. The Risk Assessment must be shared with the IT Security Office.

RELATED RESOURCES

Administrative safeguards, HIPAA Security Standards, 45 C.F.R. § 164.308(a)(1).

CONTACTS

Division of Information Technology/IT Security Office
11200 SW 8 ST, PC534A
Miami, FL 33199
305-348-1366
security@fiu.edu
https://security.fiu.edu

HISTORY

Initial Effective Date: September 1, 2009
Review Dates (*review performed, no updates*): May 17, 2024
Revision Dates (*updates made to document*): May 27, 2021