FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

HIPAA Security: Authentication and Audit Controls for Electronic Protected Health Information # 1670.015

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
December 31, 2017	May 20, 2024	Division of Information Technology/IT Security Office

POLICY STATEMENT

Florida International University departments and units that create, maintain or transmit electronic protected health information (ePHI) must designate a HIPAA Privacy Officer to perform data authentication checks in order to ensure the data is not improperly altered or destroyed. The designated HIPAA Privacy Officer must report any suspicious findings to the University HIPAA Security Officer.

Software used to store electronic protected health information must have the ability to audit the access to, and integrity of this information. In addition, departments and units that create, maintain or transmit ePHI must enable all system and software auditing functions that may be used to track system activity. The University will continuously perform monitoring, inspection, testing and auditing of such systems and software access logs in order to ensure the confidentiality, integrity and availability of ePHI.

SCOPE

This policy applies to all faculty, staff, and students.

REASON FOR POLICY

HIPAA Security Standards require that departments and units that create, maintain or transmit electronic protected health information protect it from unauthorized access, improper alteration or destruction.

DEFINITIONS

TERM	DEFINITIONS
Covered entity	A health plan, health care clearinghouse, or health care provider who transmits health information in electronic form in connection with a health care transaction.
Health care component	A component or combination of components of a hybrid entity that has been specifically designated by the covered entity

	because it either performs covered functions; or activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.
Individually identifiable health information	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.
Information system	An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people.
Physical safeguards	Physical measures, policies and procedures that protect electronic protected health information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.
Protected health information (PHI)	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: ○ Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g ("FERPA"); ○ Records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and Employment records held by a covered entity in its role as an employer.
Technical safeguards	The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

ROLES AND RESPONSIBILITIES

HIPAA Security Officer:
Is the individual designated by the University to assist in the implementation of the HIPAA Security Standards, 45 C.F.R. Parts 160, 162 and 164, and to oversee and monitor the University's compliance with the required technical, administrative and physical safeguards as these relate to protected health information created, maintained or transmitted via electronic means. The University Information Technology Security Officer is designated as the HIPAA Security Officer.

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.

RELATED RESOURCES

Technical safeguards, HIPAA Security Standards, 45 C.F.R. §§ 164.310(d) and 164.312(b).

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*): N/A
Revision Dates (*updates made to document*): December 31, 2017; May 24, 2021; May 20, 2024