FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

HIPAA Security: Access Controls to Systems Containing Electronic Protected Health Information # 1670.005

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
December 31, 2017	May 17, 2024	Division of Information Technology/IT Security Office

POLICY STATEMENT

1. Florida International University departments and units that create, maintain or transmit electronic protected health information including, without limitation, the University's health care components, shall allow access to systems that maintain electronic protected health information only to those persons who require such access in order to perform their job duties.
2. Access to systems shall be based on principle of least privilege.
3. Workforce members are required to complete HIPAA Training, IT Security Training and Application specific training.
4. Third Parties storing ePHI must be vetted through the Technology Evaluation Group (TEG) process.
5. For third party user access, a Business Associate Agreement (BAA) must be in place. A Person of Interest (POI) must be completed for the third party user.Each department or unit employee who requires access to electronic protected health information shall be assigned a unique name and/or number for identifying and tracking user identity.
6. The University HIPAA Security Officer in collaboration with the designated HIPAA Security Administrators for each department or unit shall develop an emergency access procedure that will allow access to electronic protected health information during an emergency.
7. Specific times must be defined for electronic sessions to be automatically locked and terminated after periods of inactivity.
8. Electronic protected health information shall be encrypted prior to transmission and the procedures for doing so shall be documented by each department or unit.

SCOPE

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

REASON FOR POLICY

With respect to electronic protected health information, the University must have in place access controls to prevent unauthorized access to such information.

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: o Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g ("FERPA"); o 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.
Transaction	The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: • Health care claims or equivalent encounter information. • Health care payment and remittance advice. • Coordination of benefits. • Health care claim status. • Enrollment and disenrollment in a health plan. • Eligibility for a health plan. • Health plan premium payments. • Referral certification and authorization. • First report of injury. • Health claims attachment. Other transactions that the Secretary of Health and Human Services may prescribe by regulation.

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

Physical and technical safeguards, HIPAA Security Standards, 45 C.F.R. § 164.312(a)(2).
Technology Evaluation Group, https://it.fiu.edu/teg/

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 17, 2024