FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

HIPAA Security: Technical Security Measures for the Transmission of Electronic Protected Health Information #1670.045

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 1, 2009	May 21, 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 must comply with the following transmission security policy:

1. The HIPAA Security Officer and the departments or unit's designated HIPAA Security Administrator must implement technical security measures to ensure that electronically transmitted protected health information is not improperly accessed, altered or destroyed.
2. The technical security measures to be implemented may include, without limitation, firewalls, intrusion detection systems, encryption of ePHI, where appropriate, and other security devices and techniques to ensure the network is secure against all eminent threats.

SCOPE

This policy applies to all departments and Units that create, maintain, or transmit electronic protected health information.

REASON FOR POLICY

Florida International University departments and units that maintain electronic protected health information must implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

DEFINITIONS

TERM	DEFINITIONS

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.
Individually identifiable health information	means 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.

ROLES AND RESPONSIBILITIES

HIPAA Security Officer and the departments or unit's designated HIPAA Security Administrator must implement technical security measures to ensure that electronically transmitted protected health information is not improperly accessed, altered or destroyed.

HIPAA Security Administrator must be an active member of the HIPAA Committee and participate in the committee meetings.

HIPAA Security Administrator will be the liaison between the department or unit and the IT Security Office. They will work with the Chief Information Officer to make sure all security controls are in place, documented, and validated.

RELATED RESOURCES

Technical safeguards, HIPAA Security Standards, 45 C.F.R. § 164.312(e)(1).

CONTACTS

Division of Information Technology/IT Security Office
11200 SW 8 ST, PC534a
Miami, FL 33199
305-348-1366
security@fiu.edu

HISTORY

Initial Effective Date: September 1, 2009
Review Dates (*review performed, no updates*): May 23, 2024
Revision Dates (*updates made to document*): May 21,2021