HIPAA SECURITY: TECHNICAL SECURITY MEASURES FOR THE TRANSMISSION OF ELECTRONIC PROTECTED HEALTH INFORMATION

POLICY STATEMENT (R*)

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 department’s 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 PHI, where appropriate, and other security devices and techniques to ensure the network is secure against all eminent threats.

REASON FOR POLICY (O*)

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.

RELATED INFORMATION (O*)

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

DEFINITIONS (R*)

“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.
“Protected Health Information” or “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.

“Technical safeguards” means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.