FIU | FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

University Community (faculty, staff and students)

SUBJECT (R*)	EFFECTIVE DATE (R*)	POLICY NUMBER (O*)
HIPAA SECURITY: AUTHENTICATION AND AUDIT CONTROLS FOR ELECTRONIC PROTECTED HEALTH INFORMATION	September 1, 2009	1670.015

POLICY STATEMENT (R*)

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

REASON FOR POLICY (O*)

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.

RELATED INFORMATION (O*)

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

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.

RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)

Division of Information Technology
Florida International University

RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)

FIU IT Security Officer
Biscayne Bay Campus, LIB 328
3000 N.E. 151st Street
North Miami, Florida 33181
Telephone Number: (305) 919-4299

The University Policies and Procedures Library is updated regularly. In order to ensure a printed copy of this document is current, please access it online at www.policies.fiu.edu.

For any questions or comments, the “Document Details” view for this policy online provides complete contact information.

***R = Required *O = Optional**