FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

University Community (faculty, staff and students)

SUBJECT (R*)	EFFECTIVE DATE (R*)	POLICY NUMBER (O*)
HIPAA SECURITY: ACCESS TO FACILITIES HOUSING ELECTRONIC PROTECTED HEALTH INFORMATION	September 1, 2009	1670.010

POLICY STATEMENT (R*)

Florida International University departments and units that create, maintain or transmit electronic protected health information shall comply with the facility access controls established by the University.

REASON FOR POLICY (O*)

With respect to electronic protected health information, the University needs to have in place physical safeguards to prevent unauthorized access, tamping or theft of this information or of the equipment and systems in which such electronic health information is stored.

RELATED INFORMATION (O*)

Physical safeguards, HIPAA Security Standards, 45 C.F.R. § 164.310(a)(1).

DEFINITIONS (R*)

"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.

"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.

"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.

"Physical safeguards" are 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" 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.

PROCEDURES (O*)

Facility access controls established by the University consist of the following requirements:

1. Develop a documented master plan for safeguarding the facility and premises from unauthorized physical access, tampering, or theft, including the equipment contained therein (the "Facility Security Plan").

2. All repairs and modifications to the physical components of a facility, such as walls, doors and locks, shall be documented and maintained by a designated building facility manager.

3. The Facility Security Plan shall be reviewed and updated at least once a year by the department's or unit's designated HIPAA Security Administrator.

4. All installation, repairs, and maintenance to hardware and software shall be documented and maintained by the designated HIPAA Security Administrator.

5. The designated HIPAA Security Administrator shall conduct review of the security attributes of all hardware and software at least once per year.

The designated HIPAA Security Administrator shall conduct a review of all maintenance occurring on hardware and software on a bi-annual basis.

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**