FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

University Community (faculty, staff and students)

SUBJECT (R*)	EFFECTIVE DATE (R*)	POLICY NUMBER (O*)
HIPAA SECURITY: DUTY TO REPORT SECURITY INCIDENTS INVOLVING PROTECTED HEALTH INFORMATION	September 1, 2009	1670.020

POLICY STATEMENT (R*)

Florida International University workforce members shall immediately report any and all suspected and actual breaches of information security involving protected health information to one of the following University representatives: the designated HIPAA Security Administrator for the department or unit, the University IT Security and HIPAA Security Officer, the University HIPAA Privacy Officer, or the University Compliance Officer.

The department or unit, through its designated HIPAA Security Administrator and the University HIPAA Security Officer, shall mitigate, to the extent practicable, harmful effects of security incidents that are known to the department or unit. The department or unit involved shall take immediate proactive steps to prevent further unauthorized intrusion and to document security incidents and their outcomes.

RELATED INFORMATION (O*)

Administrative safeguards, HIPAA Security Standards, 45 C.F.R. § 164.308(a)(6).

DEFINITIONS (R*)

"Administrative safeguards" are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage workforce conduct in relation to the protection of that information.

"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.

"Security incidents" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

"Workforce" or "workforce member" means part-time, full-time or temporary faculty and staff, students, volunteers, trainees, and other persons whose conduct, in the performance of work for the University, is under the direct command of the University (regardless of whether or not they are paid by the University).

RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)	
Division of Information Technology Florida International University	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.
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	For any questions or comments, the "Document Details" view for this policy online provides complete contact information.

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