FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

University Community (faculty, staff and students)

SUBJECT (R*)	EFFECTIVE DATE (R*)	POLICY NUMBER (O*)
HIPAA PRIVACY AND SECURITY: RESPONSIBILITIES OF UNIVERSITY IT SECURITY OFFICER AND HIPAA SECURITY ADMINISTRATORS	December 31, 2017	1610.010

POLICY STATEMENT (R*)

Florida International University departments and units that create, maintain or transmit electronic protected health information ("EPHI") shall each designate a HIPAA Security Administrator. The designated HIPAA Security Administrator shall work closely with the University IT Security Officer who shall also serve as the University's HIPAA Security Officer and with the University Privacy Officer to ensure that only those members of the workforce who require access to electronic protected health information have that access and to prevent unauthorized individuals from gaining such access.

The University Privacy Officer and the University IT Security Officer shall have primary responsibility for the development and implementation of HIPAA security policies at the institutional level. The University Privacy Officer, IT Security Officer and designated HIPAA Security Administrators shall perform a periodic technical and non-technical evaluation in response to environmental or operational changes affecting the security of electronic protected health information in order to ensure that the University's HIPAA Security policies and procedures continue to be viable.

RELATED INFORMATION (O*)

Administrative safeguards, HIPAA Security Standards, 45 C.F.R. §164.308(a)(2) and (8).

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.

"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.)

HISTORY (R*)

Initial Effective Date: September 1, 2009; December 31, 2017

RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*) Division of Information Technology Florida International University **RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)** 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**