FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

HIPAA Security: Use and Security of Workstations with Access to Electronic Protected Health Information # 1670.050

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 1, 2009	May 27, 2021	Division of Information Technology/IT Security Office

POLICY STATEMENT

Florida International University departments and units that create, maintain or transmit electronic protected health information must comply with the following workstation use and security measures:

1. Workforce members shall use workstations in the appropriate manner considering the sensitivity of the information contained therein, and minimizing the possibility of unauthorized access to such information.
2. Physical safeguards will be implemented for all workstations that access electronic protected health information, to restrict access to authorized users.
3. All persons who engage in use of these workstations shall be trained on the proper functions to be performed and the manner in which those functions are to be performed, in accordance with the University's policies and procedures implementing the HIPAA Privacy and Security regulations.

Staff members are not allowed to grant access to their workstations to non-staff members, unless approved by the designated HIPAA Security Administrator for the department or unit. In the event the designated HIPAA Security Administrator is not available, authorization shall be obtained from the supervisor for that department or unit and the University Privacy Officer or the University HIPAA Security Officer.

SCOPE

This policy applies to Florida International University departments and units that create, maintain or transmit electronic protected health information.

REASON FOR POLICY

The University must have in place safeguards to ensure that only authorized personnel use workstations containing electronic protected health information.

DEFINITIONS	
TERM	**DEFINITIONS**
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 (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).

ROLES AND RESPONSIBILITIES

HIPAA Security Administrator: review and approve access to workstations for non-staff members. Maintain security controls on the workstations and physical safeguards to restrict access to authorized users.

Department or Unit Supervisor: provide authorization if HIPAA Security Administrator is not available.

University Privacy Officer or University HIPAA Security Officer: provide authorization if HIPAA Security Administrator or Department Supervisor is not available.

RELATED RESOURCES

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

CONTACTS

Division of Information Technology/IT Security Office
11200 SW 8 ST, PC534A
Miami, FL 33199
305-348-1366
security@fiu.edu
https://security.fiu.edu

HISTORY

Initial Effective Date: September 1, 2009
Review Dates (*review performed, no updates*): May 17, 2024
Revision Dates (*updates made to document*): May 27, 2021