FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

HIPAA Security: Workforce Security Regarding Protected Health Information # 1670.055

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
December 31, 2017	May 21, 2021	Division of Information Technology/IT Security Office

POLICY STATEMENT

University departments performing HIPAA transactions must comply with the following workforce security policy:

1. Workforce members shall access only those areas and the applicable health information contained therein to which they are authorized according to their appropriate personnel clearance levels.
2. The procedures herein shall be referenced to and coordinated with the policies and procedures for INFORMATION ACCESS MANAGEMENT FOR ELECTRONIC PROTECTED HEALTH INFORMATION POLICY.
3. The designated HIPAA Security Administrator, in collaboration with the HIPAA Security Officer and HIPAA Privacy Officer are the University representatives responsible for determining the appropriate personnel clearance levels. The HIPAA Security Administrator shall maintain a list detailing the level(s) of clearance for each person.
4. Within 24 hours of an employee's official Notice of Termination or inter-departmental transfer, the designated HIPAA Security Administrator must be notified. Upon notification the HIPAA Security Administrator shall determine the extent, including the appropriate time, to which the employee's personnel clearance level and access authorizations will be eliminated and/or modified.
5. All employees shall be trained regarding appropriate personnel clearance levels.

Personnel security clearance policies and procedures may be amended from time to time as necessary to comply with all applicable business associate agreements.

SCOPE

This policy applies to all University departments performing HIPAA transactions.

REASON FOR POLICY

HIPAA Security Standards, 45 C.F.R. §164.308(3)(i).

DEFINITIONS	
TERM	**DEFINITIONS**
Health Care Component	A component or combination of components of a hybrid entity that has been specifically designated by the covered entity because it either performs covered functions; or activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.
Individually Identifiable Health Information	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 (PHI)	Is 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.
Secretary	Means the Secretary of the U.S. Department of Health and Human Services.
Transaction	The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: • Health care claims or equivalent encounter information. • Health care payment and remittance advice. • Coordination of benefits. • Health care claim status. • Enrollment and disenrollment in a health plan.

	• Eligibility for a health plan. • Health plan premium payments. • Referral certification and authorization. • First report of injury. • Health claims attachment. • Other transactions that the Secretary of Health and Human Services may prescribe by regulation.
Workforce or Workforce Member	Part-time, full-time and 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

1. The designated HIPAA Security Administrator, in collaboration with the HIPAA Security Officer and HIPAA Privacy Officer are the University representatives responsible for determining the appropriate personnel clearance levels.
2. The HIPAA Security Administrator shall maintain a list detailing the level(s) of clearance for each person.
3. The designated HIPAA Security Administrator shall provide training or access to training for appropriate personnel clearance levels.

RELATED RESOURCES

HIPAA Security Standards, 45 C.F.R. §164.308(3)(i).

CONTACTS

Division of Information Technology/IT Security Office
11200 SW 8 ST, PC534a
Miami, FL 33199
305-348-1366
security@fiu.edu
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*): December 31, 2017; May 21, 2021.