



HIPAA Security: Duty to Report Security Incidents Involving Protected Health Information # 1670.020

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
December 31, 2017	May 24, 2021	Division of Information Technology/IT Security Office

POLICY STATEMENT

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.

FIU’s Incident Response Plan will be followed.

SCOPE

This policy applies to all faculty, staff, and students.

REASON FOR POLICY

HIPAA Security Standards require that departments and units that create, maintain or transmit electronic protected health information protect it from unauthorized access, improper alteration or destruction. They also have a duty to report security incidents involving protected health information.

DEFINITIONS

TERM	DEFINITIONS
Covered entity	A health plan, health care clearinghouse, or health care provider who transmits health information in electronic form in connection with a health care transaction.

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: <ul style="list-style-type: none"> • 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 <ol style="list-style-type: none"> 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.
Information system	An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people.
Physical safeguards	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)	Individually identifiable health information that is: <ul style="list-style-type: none"> • Transmitted by electronic media; • Maintained in electronic media; • Transmitted or maintained in any other form or medium. • Protected health information specifically excludes: <ul style="list-style-type: none"> ○ Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g (“FERPA”); ○ Records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and Employment records held by a covered entity in its role as an employer.
Technical safeguards	The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.



Administrative safeguards	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.
---------------------------	---

ROLES AND RESPONSIBILITIES

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.

The HIPAA Security Officer or Chief Compliance Officer will activate the Incident Response Plan.

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.

RELATED RESOURCES

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

FIU Incident Response Plan Policy (<https://policies.fiu.edu/policy/862>)

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 20, 2024

Revision Dates (*updates made to document*): December 31, 2017; May 24, 2021