FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

# HIPAA Security: Access to Facilities Housing Electronic Protected Health Information # 1670.010

| INITIAL EFFECTIVE DATE: | LAST REVISION DATE: | RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT |
|---|---|---|
| December 31, 2017 | May 20, 2024 | Division of Information Technology |

## POLICY STATEMENT

Florida International University departments and units that create, maintain or transmit electronic protected health information shall comply with the facility access controls established by the University.

## SCOPE

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

## REASON FOR POLICY

With respect to electronic protected health information, the University needs to have in place physical safeguards to prevent unauthorized access, tamping or theft of this information or of the equipment and systems in which such electronic health information is stored.

## 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:<br>• 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<br>1. That identifies the individual; or<br>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:<br>• Transmitted by electronic media;<br>• Maintained in electronic media;<br>• Transmitted or maintained in any other form or medium.<br>• Protected health information specifically excludes:<br>o Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g ("FERPA");<br>o Records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and<br>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. |
| 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:<br>• Health care claims or equivalent encounter information.<br>• Health care payment and remittance advice.<br>• Coordination of benefits.<br>• Health care claim status.<br>• Enrollment and disenrollment in a health plan.<br>• Eligibility for a health plan. |

| | |
|---|---|
| | • Health plan premium payments.<br>• Referral certification and authorization.<br>• First report of injury.<br>• Health claims attachment.<br>Other transactions that the Secretary of Health and Human Services may prescribe by regulation. |

**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.

**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**

Physical safeguards, HIPAA Security Standards, 45 C.F.R. § 164.310(a)(1).

**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*): N/A
**Revision Dates** (*updates made to document*): December 31, 2017; May 24, 2021; May 20, 2024

FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

# HIPAA Security: Access to Facilities Housing Electronic Protected Health Information # 1670.010a

| INITIAL EFFECTIVE DATE: | LAST REVISION DATE: | RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT |
|---|---|---|
| December 31, 2017 | May 20, 2024 | Division of Information Technology/ IT Security Office |

## PROCEDURE STATEMENT

Facility access controls established by the University consist of the following requirements:

1. Develop a documented master plan for safeguarding the facility and premises from unauthorized physical access, tampering, or theft, including the equipment contained therein (the "Facility Security Plan").
2. All repairs and modifications to the physical components of a facility, such as walls, doors and locks, shall be documented and maintained by a designated building facility manager.
3. The Facility Security Plan shall be reviewed and updated at least once a year by the departments or unit's designated Facility Manager.
4. All installation, repairs, and maintenance to hardware and software shall be documented and maintained by the designated Facility Manager.
5. The designated Facility Manager shall conduct review of the security attributes of all hardware and software at least once per year.

The designated Facility Manager shall conduct a review of all maintenance occurring on hardware and software on a bi-annual basis.