FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

# HIPAA Security: Inventory of Hardware and Software Containing Electronic Health Information # 1670.030

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

## POLICY STATEMENT

Florida International University departments and units that create, maintain or transmit electronic protected health information ("EPHI") are required to:

1. Maintain a master inventory list of all hardware and software that contain ePHI. For hardware, the list must include all relevant serial numbers and tags necessary to identify the device, its exact location and, where appropriate, the employee(s) who are assigned to work on the device.
2. Ensure that all ePHI accessible devices are accounted for by periodically updating the master inventory against the actual devices.
3. Ensure that devices that create, store or maintain EPHI are not moved or disposed of prior to notifying the HIPAA Security Administrator for the department or unit and the University IT Security Officer.
4. Ensure that prior to disposing of any devices containing ePHI, appropriate and retrievable backup copies are made in order to meet or exceed records retention requirements.
   Ensure that all hardware and media containing ePHI are sanitized based on University's Media Sanitation guideline, https://security.fiu.edu/sanitation.

University departments and units shall coordinate efforts required by this Policy with the designated HIPAA Security Administrator for the department or unit, the HIPAA Privacy Officer and the University IT Security Officer.

The departments or unit's designated HIPAA Security Administrator shall periodically review the inventories of hardware and software and shall report any significant finding to the HIPAA Privacy Officer and the University IT Security Officer.

## SCOPE

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

| REASON FOR POLICY |
|---|
| HIPAA Security Standards require that the covered entity implement policies and procedures to tract the movement, removal and final disposition of hardware and media containing electronic protected health information. The procedures must specify who is accountable for tracking this information within the institution. |

| 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<br>• 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; |

| | |
|---|---|
| | • Transmitted or maintained in any other form or medium.<br>• Protected health information specifically excludes:<br>  ○ Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g ("FERPA");<br>  ○ 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. |
| 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. |
| Workforce or workforce member | 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 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.
HIPAA Security Administrator or IT Administrator shall maintain a comprehensive inventory of assets.

**RELATED RESOURCES**

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

IT Asset Management: Complete Guide (https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0011571)

**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; December 31, 2017
**Review Dates** (*review performed, no updates*): N/A
**Revision Dates** (*updates made to document*): May 27, 2021; May 20, 2024