FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

University Community (faculty, staff and students)

SUBJECT (R*)	EFFECTIVE DATE (R*)	POLICY NUMBER (O*)
HIPAA SECURITY: INVENTORY OF HARDWARE AND SOFTWARE CONTAINING ELECTRONIC PROTECTED HEALTH INFORMATION	September 1, 2009	1670.030

POLICY STATEMENT (R*)

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.
5. Ensure that all hardware and media containing EPHI are scrubbed before they are made available for re-use by another department or unit.

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 department's 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.

REASON FOR POLICY (O*)

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.

RELATED INFORMATION (O*)

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

DEFINITIONS (R*)

"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" or "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.

RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)	
Division of Information Technology Florida International University	The University Policies and Procedures Library is updated regularly. In order to ensure a printed copy of this document is current, please access it online at http://policies.fiu.edu/.
RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)	
FIU IT Security Officer Biscayne Bay Campus, LIB 328 3000 N.E. 151st Street North Miami, Florida 33181 Telephone Number: (305) 919-4299	For any questions or comments, the "Document Details" view for this policy online provides complete contact information.

***R = Required *O = Optional**