HIPAA SECURITY: OPERATIONAL CONTINGENCY PLAN FOR ELECTRONIC PROTECTED HEALTH INFORMATION

September 1, 2009 1670.035

POLICY STATEMENT (R*)

Florida International University departments and units that create, store or maintain electronic protected health information shall perform a data criticality analysis and document the acceptable level of down time expected if services are disrupted. Based on this risk assessment, the following plans must be established by each department/unit:

1) A data backup plan must be created to maintain retrievable exact copies of electronic protected health information.
2) A disaster recovery plan must be established. The plan must include methods for restoring data loss during a disaster.
3) An emergency mode operation plan must be developed to enable access to critical business processes for the continued security of electronic protected health information while operating in emergency mode.

The plans described above must be tested and revised at least once a year.

REASON FOR POLICY (O*)

The University must have in place adequate procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

RELATED INFORMATION (O*)

Administrative safeguards, HIPAA Security Standards, 45 C.F.R. §164.308(a)(7).

DEFINITIONS (R*)

“Administrative safeguards” are 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.

“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.

“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:
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

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) 91-4299

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 www.policies.fiu.edu.

For any questions or comments, the “Document Details” view for this policy online provides complete contact information.

*R = Required  *O = Optional