FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

HIPAA Security: Operational Contingency Plan for Electronic Protected Health Information # 1670.035

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
September 1, 2009	May 17, 2024	Division of Information Technology/IT Security Office

POLICY STATEMENT

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 business impact analysis must be created to document the impact of a disruption to business functions and provide strategies to mitigate and minimize the risk of the impact.
2) A data backup plan must be created to maintain retrievable exact copies of electronic protected health information.
3) A disaster recovery plan must be established, tested and documented. The plan must include methods for restoring data loss during a disaster. This plan should be reflected in the FIU Continuity of Operations Plan (COOP), FIU Ready.
4) 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.

SCOPE

This policy applies to all faculty, staff, students, person of interest, and affiliates which create, store, or maintain protected health information.

REASON FOR POLICY

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.

DEFINITIONS	
TERM	**DEFINITIONS**
COOP	Continuity of Operations Plan
FIU Ready	Is the main**ontinuity planning tools** used by the Department of Emergency Management to maintain normal University operations in the face of disruptive events.
Business Impact Analysis	Is a detailed **study** of business activities, dependencies, and infrastructure. It reveals how critical products and services are delivered and examines the potential **impact** of a disruptive event over time.
Disaster Recovery Plan	Is a formal document that contains detailed instructions on how to respond to an unplanned incident such as a natural disaster, power outage, cyber-attack, and any other disruptive events.
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 (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

	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.

ROLES AND RESPONSIBILITIES

Business Units or departments that create, store, transmit, and maintain protected health information must perform a risk assessment to determine the impact of a disruption of services to their information systems that house this data. A business impact analysis must be maintained to document the impact of such disruptions. A disaster recovery plan, backup plan, and emergency mode plan must also be maintained.

RELATED RESOURCES

Administrative safeguards, HIPAA Security Standards, 45 C.F.R. §164.308(a)(7).
FIU Ready: https://dem.fiu.edu/resources/fiu-ready/index.html

CONTACTS

Division of Information Technology/IT Security Office
11200 SW 8 ST, PC534A
Miami, FL 33199
305-348-1366
security@fiu.edu
security.fiu.edu

HISTORY

Initial Effective Date: September 1, 2009
Review Dates (*review performed, no updates*): N/A
Revision Dates (*updates made to document*): May 21, 2021; May 17, 2024