Electronic Protected Health Information Breach Policy
May 18, 2026

SCOPE

This policy applies to Florida Atlantic University's Covered Components and those working on behalf of the Covered Components (collectively "FAU") for purposes of complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), including applicable amendments and requirements established under the Health Information Technology for Economic and Clinical Health (HITECH) Act.

POLICY STATEMENT

FAU restricts access to protected health information (PHI), including electronic protected health information (e-PHI), to the minimum necessary to perform assigned job functions. All workforce members are required to take immediate action upon the discovery of a confirmed or suspected breach of e-PHI to ensure timely containment, investigation, and remediation in accordance with the Security Incident Procedures Policy and the Security Incident Response Plan.

REASON FOR THE POLICY

To establish reasonable procedures for individual workforce members to follow in the event of a suspected breach of e-PHI information.

DEFINITIONS

Breach: An event that generally involves an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of PHI.

RELATED INFORMATION SECURITY POLICIES

The policies, standards, and procedures documented herein are implemented in reference to the FAU Information Security Policies listed below. In the event of any discrepancy between this document and the referenced FAU Information Security Policies, the more restrictive requirement shall apply.

IS-POL-12 Incident Response
IS-POL-16 Reporting Security Incidents

PROCEDURE

1. If a breach of e-PHI information is suspected by a workforce member, the workforce member must immediately report any details to the University Chief Compliance and Ethics Officer and the University Information Security Officer, using approved methods, and adhere to IS-POL-12 Incident Response and IS-POL-16 Reporting Security Incidents as applicable.

2. The University Chief Compliance and Ethics Officer and University Information Security Officer or their designees will immediately review the supplied information and take direct action if necessary for any initial containment activities.

3. Further breach investigation, containment, remediation and reporting will occur in accordance with the Security Incident Procedures Policy and Security Incident Response Plan established by the University Information Security Officer.

4. Any necessary communication or reporting of breach details will be initially advised by the University Chief Compliance and Ethics Officer in accordance with applicable laws, regulations, and University policies and procedures.