



e-PHI Breach Policy
September 12, 2016

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).

POLICY STATEMENT

FAU takes immediate action upon the discovery of a breach or suspected breach of e-PHI in order to contain and remediate any suspected breach of e-PHI consistent with the Security Incident Procedures Policy and 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- Refer to Glossary and Terms

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 Officer and the University Information Security Officer and adhere to the Security Incident Procedures Policy and Security Incident Response Plan as applicable.
2. The University Chief Compliance Officer and University Information Security Officer or their designees will immediately review the supplied information and take direct action if necessary for any needed 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 Officer in accordance with applicable laws, regulations and University procedures.