FAU

FLORIDA ATLANTIC UNIVERSITY

Information Access and Security Policy
June 7, 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 limits access to PHI and e-PHI and requires that workforce members use reasonable measures to protect against unauthorized disclosure or access to PHI, e-PHI and other confidential information

REASON FOR THE POLICY

To establish reasonable procedures for individual workforce members to follow to reduce the risk of compromising the security of e-PHI, PHI, and other confidential information.

DEFINITIONS- Refer to Glossary and Terms

PROCEDURE

1. Workforce members with a need to utilize FAU's electronic systems containing e-PHI will be given access on a need to know basis in accordance with FAU's Information Access Management Policy.

2. The Office of Information Technology will assign new workforce members a unique, individual user identification and password.

3. Workforce members must immediately change their initial systems access passwords.

4. Workforce members should change their access passwords at least once every ninety (90) days unless other password protections are in place (e.g., dual factor authentication). Where possible, the Office of Information Technology will establish reminders and other procedures if passwords are not regularly changed to ensure compliance with this provision.

5. Where possible, workforce members should position their computer screens away from public or third party view or implement the use of screen protectors.

6. Workforce members must log off of their computers or lock their screen when they are not at their computer. This includes absences for lunch, breaks, etc. Where possible, the Office

of Information Technology or department IT staff will enable settings that automatically logs a user off the computer or locks the screen when it is not in use for a set amount of time (e.g., 5 minutes).

7. Workforce members may not send or download e-PHI to personally owned devices or accounts (i.e. personal e-mail accounts, download on personal iPad, send e-PHI via text, etc.) without the express permission of the department leader and the Office of Information Technology. Personal devices that are used to maintain, create, store, or transmit e-PHI will be subject to inspection at the request of FAU to ensure the devices have adequate security and are being used appropriately.

8. Filing cabinets containing PHI will remain locked, and only those with a need to know will have access to the keys.

9. Papers containing PHI should be placed in folders, placed face-down on desks, or otherwise shielded from public or third party view.

10. Workforce members transmitting PHI or e-PHI must take precautions to protect the confidentiality of such information. For instance:

    - Fax: Only send faxes if another transmission method is not available. Verify the fax number is correct before sending the information.
    - Mail: Send PHI in the mail via a method where you can track delivery.
    - E-Mail: Send via an encrypted method.

11. FAU will train its workforce members on at least an annual basis regarding privacy and security measures that can be taken by individuals to facilitate FAU’s privacy and security policies and procedures.