FAU
FLORIDA ATLANTIC UNIVERSITY

Information Access Management 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

As one administrative safeguard designed to prevent, detect, correct and contain security violations, access to electronic protected health information ("e-PHI") is authorized, established, maintained and modified based on the minimum amount of e-PHI necessary for individual members of the workforce to perform their jobs effectively.

REASON FOR THE POLICY

To ensure that FAU gives workforce members access to e-PHI on a need to know basis and only to the extent necessary to perform their job functions. To establish a process to grant, restrict, and terminate access to e-PHI based on the members' change in status with FAU.

DEFINITIONS - Refer to Glossary and Terms

PROCEDURE

User Access to Computer Resources

1. Standard Access- All FAU workforce members, staff, students, researchers, personnel, and any other persons who are given access to computing resources, applications systems and the FAU network will be granted 'standard access.' Individual passwords and access to these information systems may not be shared, copied or distributed with others for any purpose.

2. Remote Access- VPN and other remote access to systems will be based on the established Office of Information Technology ("OIT") approval processes and managed by OIT. Any change in the user status related to access rights will be managed by the OIT workflow process. Devices used for remote access must conform to the security and privacy requirements in this policy document.

3. Access Reports- OIT or departmental IT staff will review user access reports on a periodic basis on systems which store (or can access) e-PHI, PHI, or other confidential information to determine if the appropriate need-to-know standards have been applied

and if policies and procedures are adhered to. Annual reviews will be conducted on network information resources to verify access rights.

4. Need to Know Checklist- All FAU workforce members, students, and anyone else accessing FAU's networks must complete an OIT checklist to determine required access to systems. OIT will work with administrative staff during the onboarding process to determine the level of access based on necessity.

5. Portable Media Access– Any user who accesses any FAU system which stores (or can access) e-PHI, PHI or other confidential information is prohibited from using unencrypted portable media devices, such as USB or CD/DVD to store such information.

Changing System Access

1. Authorization to access e-PHI is consistent with FAU's policy on minimum necessary use.

2. The Office of Information Technology or responsible departmental IT staff is responsible for granting, changing, and removing systems access. After access privileges have been authorized, a user account is established that enables a workplace member to access e-PHI and FAU's information systems as appropriate to his or her job function.

3. The Office of Information Technology and responsible departmental IT staff maintains documentation of all user accounts and authorized access privileges.

4. Each department shall ensure that reviews of access rights and user accounts for its assigned workforce members are conducted no less than quarterly to ensure continued appropriateness of accounts and levels of access. Any changes shall be immediately reported to the Office of Information Technology and responsible departmental IT staff.

5. FAU revokes access privileges when a user's employment or relationship with FAU is terminated for any reason. This revocation will occur on the effective date of the user's termination or sooner if circumstances warrant. Department leaders and the Human Resources Department are responsible for notifying the Office of Information Technology immediately upon a termination event.

6. Access privileges will be modified or revoked whenever a workforce member's job function or access needs change. Modifications to user accounts are made with appropriate authorization from the terminated workforce member's department in conjunction with the Office of Information Technology. Such modifications will include, but are not limited to disabling the terminated workforce member from accessing e-mail and software accounts and changing any passwords to common systems to which the terminated workforce member may have had access.

7. This policy and procedure is designed and implemented: (a) to ensure that all members of the workforce have appropriate access to e-PHI; and (b) to prevent those workforce

members who should not have access from obtaining access to e-PHI.

User and Administrator Permissions

1. Standard User Permissions- All FAU workforce members and system or network users will be granted standard user permissions by default to their approved computing resources. These users will be restricted from installing software or altering their secured computer configuration settings. All installations of new software applications, software patches or plugins will be managed through OIT or responsible departmental IT staff.

2. Administrator Permissions- OIT staff or responsible departmental IT staff will be the only authorized group of users with Administrator rights to any desktop or laptop. A valid business justification for granting administrator rights to any faculty or staff must be submitted to the Information Security Officer or the director of the responsible departmental IT group.