Physical Safeguards Policy
July 19, 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
FAU shall implement physical safeguards to prevent, detect, contain, and correct any HIPAA Security Rule violations in accordance with this policy.

REASON FOR POLICY
To establish physical safeguards to comply with the HIPAA Security Rule.

DEFINITIONS
Refer to Glossary and Terms.

PROCEDURE

1. Facility Access Controls

a. To ensure that only authorized individuals have access to FAU's datacenter or server room facilities and electronic information systems, access is controlled and validated by:

   i. ID badges;

   ii. Magnetic card readers or physical key;

   iii. A minimum of two doors physically controlling access to the datacenter; or

   iv. Receptionists or police.

   At no time are server rooms or datacenters to be left unsecured allowing access by unauthorized personnel. All personnel must be validated and approved prior to access to server rooms or datacenters.

b. Visitors to the facility are required to sign a log that records the time of arrival and departure.

c. Visitors to the facility must be escorted as appropriate and, if working near or with

electronic protected health information ("e-PHI"), have appropriate authorization and/or supervision.

d. A log must be kept to document all facility repairs or modifications that are related to security.

e. Temporary authorization to access FAU's facility and electronic information systems may be granted to repair personnel or technicians for the purpose of restoring lost data or repairing damaged equipment as long as proper supervision is provided.

2. Workstation Use and Workstation Security

a. Guidelines for the acceptable use of workstations (including desktops, laptops, and hand-helds) that contain or have access to e-PHI are provided to workplace members.

b. Training is provided to workplace members on the guidelines for acceptable use of workstations.

c. Additional training is provided as needed to ensure authorized users understand necessary procedures for compliance with the guidelines (for example, enabling password-protected screensavers or log-off procedures).

d. Physical safeguards for workstations that are implemented to restrict access to authorized users include:

i. Secure locations

ii. Locking devices

iii. Password protection

iv. Screen time-outs and

v. Shielding monitors from plain view

3. Device and Media Controls

<u>General Security</u>

a. All FAU workforce members and FAU network and systems users must adhere to best practices concerning the physical security of their computing devices.

b. The general recommendations for physical security are the same for all devices, particularly smaller devices like laptops, hard disks, smartphones, music players,

and flash drives:

i. Never leave your laptop or small device unattended, even for a moment, even in your office. Most laptops are stolen from their owners' offices, while the owner is away on a quick break or at a meeting.

ii. If you must leave your laptop in a car, stow your bag in the trunk before you reach your destination, so potential thieves don't see you doing so. Make sure your car is locked.

iii. Do not leave portable electronic equipment unattended when traveling. Monitor equipment closely while checking in at an airport or hotel counter and while passing through airport security checkpoints. If you must leave the equipment briefly unattended in a hotel room, secure it to a desk or table with a cable lock or keep it in a hotel-provided safe if available.

iv. When leaving your office space, lock your computing resources in a desk or an office that can be locked.

v. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location near the computer.

vi. Printouts containing protected health information should be immediately removed from the printer.

vii. Whiteboards containing PHI should be erased.

<u>Device Controls and Data Removal</u>

a. An accurate inventory of FAU's devices, hardware, and electronic media housing PHI shall be maintained and updated by the Office of Information Technology ("OIT") or the responsible IT group.

b. A log is maintained by OIT or the responsible IT group of the movement of known hardware that contain e-PHI into, out of, and within the facility.

c. A retrievable, exact backup copy of e-PHI is created before moving equipment that may result in damage or the loss of data.

d. E-PHI that is stored on the hard drives of computers or other electronic media shall be removed or otherwise rendered unreadable before the disposal or re-use of the hardware or electronic media.

e. Unencrypted e-PHI data must be destroyed or completely and securely removed from computers, devices, and electronic media (including backups) before disposal,

repair, or re-assignment of such equipment. OIT or the responsible IT group is responsible for removing e-PHI from such devices through scrubbing, purging, or other commercially reasonable method approved by the University Information Security Officer.

f. The effective removal of e-PHI from hardware or electronic media must be verified by OIT prior to disposal or re-use.

4. Printers, Scanners, Copiers, Fax, Shredders

a. Document Security: Every time you scan, copy, or email a document, an image of the original document may remain in storage on the device. Without any additional protective measures such as encrypting the document while in storage or securely wiping the data, individuals with some technical capability can recover such information.

All faculty and staff using a desktop, multifunction printer (MFP), or multifunction device (MFD) that incorporates the functionality of multiple devices (e.g., printer, scanner, photocopier, fax, email) used to manage unencrypted data must contact OIT for help in protecting the data stored in these devices.

b. Tracking and Analytics: All network printers utilized for printing PHI must be password protected and firmware updates applied on a regular basis.

c. Destruction of Documents containing PHI: All printed documents containing PHI must be destroyed using a shredder.

5. Safe and Secure File Sharing and Storage

a. Acceptable Services: All services used to allow the secure collaboration and document/file transfers must be approved by the University Information Security Officer. The following are examples of tools that are already approved to allow secure collaboration and document/file transfers:

- Microsoft OneDrive for Business — When logging in with FAU authorized account
- Network Share Drives — Non-sensitive information only
- ANDISEC Share Drives — Storing PHI requires the written approval of the University Information Security Officer and is applicable only to the approved drive share
- SharePoint sites — Non-sensitive information only
- OIT Filelocker

b. Prohibited Services: Any cloud storage provider not listed under the above acceptable services list or otherwise approved by the University Information Security Officer (e.g., Google Drive, Box.net, Dropbox, Amazon, etc.) **shall not** be used for document/file transfers containing any type of confidential, protected, or

sensitive information.

c. All FAU workforce members and network and systems users must adhere to any applicable FAU and OIT acceptable use policies on cloud storage and cloud services.

6. OIT Cyber Security

- All FAU workforce members and network and systems users must adhere to OIT's Cybersecurity and Information Security processes which include, but are not limited to:

    - Acceptable operating systems, software, and version numbers
    - Enforced password complexity and strength audits
    - Enforced password resets
    - Electronic filing and protection of passwords
    - Intrusion detection / scanning
    - Network and Wi-Fi standards
    - Banned 'rogue' devices
    - Penetration (Pen) testing standards and remediation
    - Identity theft and phishing protection
    - Illegal file sharing policies
    - VOIP encryption requirements for e-PHI — Applicable to VoIP services not provided through the Communication Infrastructure department.

REFERENCE

University Policy 12.2 Acceptable Use of Technology Resources.