Physical and Technical Authentication Safeguards Policy

March 3, 2026

APPLICABILITY:

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 shall establish and maintain security controls to restrict physical and logical access to authorized users only. These controls apply to all computing devices and are particularly critical for portable and mobile devices, including laptops, external storage media, smartphones, tablets, media players, and flash drives.

REASON FOR POLICY:

To establish physical and technical safeguards to comply with HIPAA Physical Safeguard requirements and institutional standards governing the physical protection of computing devices that access, store, or process electronic protected health information (ePHI).

PROCEDURES:

Device Security Controls

1. These controls apply to all computing devices and are particularly critical for portable and mobile devices, including laptops, external storage media, smartphones, tablets, media players, and flash drives.

2. Computing devices that store or access ePHI must employ encryption for data at rest. Encryption mechanisms must be approved by the Information Security Officer and implemented in a manner that renders ePHI unusable, unreadable, or indecipherable to unauthorized individuals in the event of loss, theft, or unauthorized physical access.
3. When an office or workspace is left unattended, computing devices and associated storage media must be secured in a locked desk, cabinet, or room that provides physical

access control. Passwords must not be written down or displayed on sticky notes affixed to or placed near computing devices or stored in an accessible or unsecured location in proximity to a workstation.

4. When a computing device must be left inside a vehicle, the device or carrying case must be concealed from view prior to arrival at the destination and secured in a locked trunk or equivalent compartment.

5. Portable electronic equipment must be continuously supervised while traveling. Devices must be closely monitored during airport and hotel check-in, transportation security screening, and similar transit activities.

6. Additional guidelines governing the acceptable use of workstations are documented and communicated through the FAU "Workstation and Network Appropriate Use" Policy.

User Access Controls

1. Workforce members authorized to access electronic protected health information ("e-PHI") are assigned a unique User ID that enables FAU's information system to identify, authenticate and track user identity and access to FAU's information systems and e-PHI.

2. Workplace members may not allow anyone to use their User ID or use another person's User ID to gain access to FAU's information systems under any circumstance.

3. Workplace members are required to follow password management policies and procedures to create and safeguard their User ID to prevent unauthorized access to FAU's information systems.

4. Access control lists are maintained and updated as needed, and technical modifications to user accounts are provided in a timely manner when access privileges are terminated or changed.

Emergency Access Controls

1. Temporary access to e-PHI or FAU's information systems may be provided in emergencies.

2. FAU's "Contingency Plan" policy describes the emergency access procedures.

File Storage Controls

1. All file sharing, document collaboration, and electronic storage services used to store, transmit, or access protected health information (PHI or ePHI), or other confidential or sensitive University information, must be formally approved by the FAU Information Security Officer (ISO). Only services that meet FAU security, privacy, and regulatory compliance requirements may be used.

2. Approved services for secure collaboration and document or file transfer include the following, subject to applicable data classification and usage restrictions:

    a. FAU network share drives, limited to non-sensitive information only;

    b. ANDISEC share drives, where storage of PHI or ePHI is permitted only with prior written approval from the ISO and restricted to the specifically approved drive share;

    c. FAU-managed SharePoint sites, limited to non-sensitive information only; and

    d. Microsoft OneDrive for Business, when accessed using an FAU-authorized account

E-PHI Transmission Controls

1. E-PHI may only be transmitted to authorized parties.

2. When e-PHI must be transmitted in email communications, only the minimum amount of protected health information needed to achieve the purpose of the communication should be transmitted and only in an encrypted state consistent with officially approved procedures or mechanisms defined by the FAU HIPAA Taskforce.

3. When transmitting e-PHI in email communications, the following statement should be included in the email as an extra precaution:

    a. The information contained in this transmission may contain privileged and confidential information, including patient information protected by federal and state privacy laws. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution, or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender by reply email, report the error to FAU's Chief Compliance Officer, and destroy all copies of the original message.

4. The use of unapproved cloud storage providers or file sharing services for the storage, transmission, or collaboration of confidential, protected, or sensitive information is strictly prohibited. This prohibition includes, but is not limited to, services such as Google Drive, Box, Dropbox, Amazon-hosted storage services, or any other cloud service not explicitly approved by the University Information Security Officer.

5. All third-party service providers that create, receive, maintain, or transmit PHI or ePHI on behalf of FAU must have a fully executed Business Associate Agreement (BAA) in place prior to the use of such services. The BAA must be reviewed and approved by the appropriate FAU authorities and must, at a minimum:

    a. Establish the vendor's responsibility to safeguard PHI in accordance with HIPAA requirements;

    b. Prohibit the unauthorized use or disclosure of PHI;

    c. Require implementation of appropriate administrative, physical, and technical safeguards; and

    d. Address breach notification, reporting obligations, and subcontractor compliance.

6. Cloud services or file sharing platforms that do not support or execute a HIPAA-compliant BAA are not authorized for the storage, processing, or transmission of PHI or ePHI under any circumstances.

Data Removal and Destruction Controls

1. An accurate and up-to-date inventory of all FAU devices, hardware, and electronic media that store or process protected health information (PHI or ePHI) must be maintained. Inventory management responsibilities rest with the designated responsible IT group and must be reviewed and updated in accordance with FAU asset management standards.

2. The use of unencrypted portable storage media to store, process, or transmit ePHI, PHI, or other confidential information is strictly prohibited. This prohibition applies to, but is not limited to, USB drives, optical media (CD/DVD), external hard drives, and similar removable storage devices.

3. Prior to the relocation, transport, or movement of equipment that may result in damage, loss, or compromise of data, a retrievable and encrypted backup copy of all ePHI must

be created and securely maintained. Backup processes must comply with FAU information security and data protection standards.

4. Electronic protected health information stored on computers, storage devices, or other electronic media must be removed or rendered unreadable prior to the disposal, reuse, reassignment, or repurposing of such hardware or media. The removal of ePHI from hardware or electronic media must be verified and documented by the responsible IT group prior to disposal or reuse. Verification activities must ensure that ePHI cannot be recovered using reasonable technical means.

5. Unencrypted ePHI must be securely destroyed or completely and irreversibly removed from all computers, devices, and electronic media, including backup media, before disposal, repair, or reassignment. The responsible IT group is required to perform data removal using scrubbing, purging, destruction, or other commercially reasonable methods approved by the University Information Security Officer.

Facility Access Controls

1. Physical access to FAU datacenters, server rooms, and facilities housing electronic information systems that store or process electronic protected health information (ePHI) must be restricted to authorized personnel only. Access to these facilities must be controlled and validated through one or more of the following mechanisms:
    a. University-issued identification badges;
    b. Magnetic card readers or physical keys;
    c. A minimum of two physical barriers (e.g., dual locked doors) controlling access to the datacenter or server room; or
    d. Physical oversight by authorized personnel, including reception staff or FAU Police.

2. Server rooms and datacenters must not be left unsecured at any time. Unauthorized access to these facilities is strictly prohibited.

3. All personnel must be formally authorized and approved prior to being granted access to server rooms or datacenters. If visitors are required to work near or with systems that store, process, or transmit ePHI, appropriate authorization to access the relevant electronic information systems must be granted in advance and documented in accordance with FAU security policies. Authorization must be based on documented business need and reviewed in accordance with FAU access control procedures.

4. All Visitors must be escorted and continuously supervised while within restricted facilities. Visitors to server rooms or data centers must be logged. Visitor logs must, at a minimum, record the visitor's name, affiliation, purpose of the visit, time of arrival, and time of departure. Logs must also be maintained to document facility repairs, maintenance activities, or physical modifications that may impact the security of the environment.