Mobile Device Policy
August 10, 2026

SCOPE
This policy applies to Florida Atlantic University's Covered Components and those working on behalf of the Covered Components for purposes of complying with the privacy provisions of 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 Covered Components will implement security measures on mobile devices which may have or could reasonably expect to access, contain or transmit protected health information (PHI). The security measures are designed to protect PHI from unauthorized disclosure.

REASON FOR THE POLICY
Mobile devices present an increased risk of unauthorized access or disclosure of protected health information due to their portability and widespread use. This policy exists to ensure that such risks are addressed in a manner consistent with the University's HIPAA compliance obligations and overall information security governance.

DEFINITIONS
Mobile Device - Any portable computing device or portable electronic media capable of accessing, storing, or transmitting electronic protected health information (e-PHI). This includes, but is not limited to, laptops, smartphones, tablets, USB flash drives, external drives, and CD/DVD/Blu-ray media.

RELATED INFORMATION SECURITY POLICIES
The policies, standards, and procedures documented herein are implemented in reference to the Florida Atlantic University (FAU) Information Security Policies listed below. In the event of any discrepancy between this document and the referenced FAU Information Security Policies, the more restrictive requirement shall apply and must be observed.

IS-POL-1 Protecting Electronic University Data

IS-POL-3 Virtual Private Network (VPN) and Remote Access Policy
IS-POL-12 Incident Response
IS-POL-16 Reporting Security Incidents
IS-POL-17 Encryption Standards

PROCEDURES

1. FAU Covered Components shall purchase, configure, issue, and maintain mobile devices in accordance with the best practices identified below for devices that access, store, or transmit PHI, consistent with applicable operational and technical requirements.:

a. Full-device and storage encryption for all mobile devices that access, store, or transmit PHI.

b. Authentication-mediated login using an approved mechanism (e.g., password, PIN, passcode, or gesture-based authentication).

c. Remote wipe capability to support prompt data removal in the event of loss, theft, or unauthorized access.

d. Installation and activation of device-level firewall or equivalent operating system network protection controls.

e. Installation and activation of University-approved security software or operating system–provided security protections, including malware protection.

f. Regular updating of operating systems and security software to address known vulnerabilities.

g. Maintenance of physical control over mobile devices at all times to prevent unauthorized access or loss.

h. Use of secure network connections when accessing sensitive data, including use of the University's virtual private network (VPN) when not connected directly to a secure FAU network, and use of secure websites ("https") for non-sensitive data.

i. Disabling or restricting unapproved file-sharing, backup, synchronization, or cloud-based applications for PHI, unless an applicable, active Business Associate Agreement is in place with Florida Atlantic University.

University owned or managed mobile devices that access, store, or transmit PHI are required to be protected in accordance with applicable University policies and procedures. Compliance with these requirements is to be enforced and monitored using mobile device management (MDM) services.

2. For users who want to use a personally owned mobile device for business purposes the following is required:

a. To access Electronic Medical Record (EMR) systems, workforce members must bring their personal device to university IT personnel to install MDM software which will:

- Ensure the device is encrypted;
- Allow remote wiping of the device;
- Enforce the use of passwords or other approved authentication methods for sign-in.

b. The Outlook app or Office web site are the exclusive methods for accessing University email.

c. Cellphone users must install and enable a “Find my iPhone” or “Find My Device” type application on their device.

3. Workforce members may not share their mobile devices, passwords, or User IDs with other persons, including family members.

4. Workforce members must also comply with the mobile device requirements of any applicable clinics or hospitals in which they are providing services or undergoing training, as well as applicable University policies.

5. Lost or stolen mobile devices must be reported to the University Information Security Officer immediately.