HIPAA Policy – Mobile Devices
July 16, 2021

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).

POLICY STATEMENT

FAU Covered Health Care 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

The ubiquity of mobile devices and their ability to access, store and transmit PHI requires that security measures be actively enacted to protect PHI from unauthorized disclosure.

PROCEDURES

1. FAU Covered Health Care Components shall purchase, configure, maintain and issue mobile devices utilizing the best practices identified below (as may be reasonably implemented for each of the Covered Health Care Components) for mobile devices likely to access, store or transmit PHI:

    - Full disk/memory encryption
    - Password (or other authentication) mediated login
    - Remote wiping capacity
    - Disable file sharing applications
    - Install/enable firewall
    - Install/enable security software
    - Update security/operating software regularly
    - Maintain physical control of device
    - Educate users that when not using secure FAU network directly, they should use the University's virtual private network (VPN) application for sensitive data and at a minimum use ensure they are using secure websites ("https") for non-sensitive data
    - Prevent and prohibit backups to the cloud unless an applicable active business associate agreement is in place with FAU

2. University owned and issued mobile devices and laptops following current policies and procedures should be sufficiently protected. This is monitored through the installation of mobile device management (MDM) or hypervisor software on the mobile devices.

3. For users who want to BYOD (bring their own device) to work (i.e. use a personally owned mobile device for business purposes) the following are required:

    a. To access any Electronic Medical Record (EMR) system (most sensitive level of access), install MDM (user must bring device to college/university IT personnel to install) which will:

        - ensure device is encrypted;
        - allow remote wiping; and
        - enforce password/other authentication to sign in.

        EMR must implement multifactor authentication (for example Duo). VPN must be used to access EMR via non-university networks laptops. To access EMR on cellphones, users must use the EMR's native app. Whenever users replace their personnel mobile devices, they must have MDM on the new device.

    b. To access FAU email (least sensitive level of access), the Outlook app shall be the exclusive method for access (pending implementation date from OIT).

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

4. Mobile device users must report lost or stolen devices to the Chief Information Security Officer (CISO) immediately.

5. Mobile device users may not share devices, passwords or User IDs with other persons, including family members.

6. Mobile device users are obligated to maintain the latest operating system (OS) and/or anti-virus software on their mobile devices and laptops.

7. Mobile device users must also comply with the requirements of any applicable clinics or hospitals in which they are providing services or undergoing training (e.g., using required applications such as HIPAA Bridge, HIPAA Chat or other applications required by the facility), as well as any applicable College, School or Department policies.

CONTACT

Contact FAU's Chief Privacy Officer at 561-297-3004 with any questions or comments.