UNIVERSITY OF OKLAHOMA

HIPAA Policies

Subject: Workstation Policy	**Approved:** January 2, 2014
Effective Date: January 2, 2014	**Last Revised:** 4/1/2018, 7/22/22

I. PURPOSE

To ensure that computers that access, store, or transmit electronic Protected Health Information (ePHI) are used in a secure and appropriate manner.

II. POLICY*

Each Health Care Component and its Workforce Members who use computers that access, store, or transmit ePHI ("Users"), such as University-Owned, University-Leased, Personally-Owned desktops, laptops, smart phones, flash drives, medical devices, and, tablets ("Workstations") must comply with the following policies.

A. Proper Use of Workstations

1. Users shall observe the Minimum Necessary Rule at all times (i.e., use Workstations to Access only that PHI that they need to Access to perform a job-related function).
2. Users shall not attempt to exceed their approved Access or attempt to Access any network, system, application, or data to which they have not been granted access.
3. Users understand that Workstation use may be audited at the discretion of the HIPAA Security Officer, University Privacy Official, or University administration to confirm compliance with University policies.

B. Workstation Locations

1. Users shall secure Workstations or shall locate them in areas that can be secured when they are not attended.
2. Users shall position Workstation monitors away from view of those in common areas or install privacy screens to prevent unauthorized observation.
3. Users must return the screens on Workstations to a password-protected screen saver or login screen when the Workstation will be unattended.

C. Storing PHI on Workstations

1. Users shall not store ePHI on unencrypted Workstations.
2. Users may store ePHI only on encrypted Workstations or on servers located in a secure enterprise data center.
3. Each User is responsible for the security of his/her Workstation and the ePHI stored on

NOTE: Clinical work performed by dually-employed Workforce Members at the affiliated institution, OU Medicine, Inc. (d/b/a OU Health and OU Health Physicians) must be done in compliance with OU Medicine, Inc. (d/b/a OU Health and OU Health Physicians) policies and procedures.

the Workstation.

4. Users must comply with all relevant IT and University policies concerning protecting ePHI stored on portable computing devices, such as encryption and password protection policies.
5. Portable computing devices used to access, create, transmit, or store PHI outside of the University's VDI environment or secure data center, regardless of whether the device is owned or leased by the University or by the User, must be encrypted.

NOTE: The Office for Civil Rights has stated that it considers storing ePHI on unencrypted portable devices to be an act of deliberate indifference with regard to the protection of PHI.

Users should Contact IT or the HIPAA Security Officer if they believe they have circumstances that warrant special encryption consideration.

D. Theft or Loss

1. Users must immediately report the theft or loss of <u>any</u> Workstation used for University Business (including those owned by the individual or a vendor) to the University Privacy Official and HIPAA Security Officer, as well as to their Tier 1/IT Representative or IT Security, so that mitigation and reporting options can be considered and implemented as soon as possible. (See HIPAA *Breach of Unsecured PHI/ePHI* policy.) It is expected that a police report will be filed with local law enforcement and that IT's *Lost/Stolen Device* form will be completed and submitted.
2. Users must cooperate with those individuals who are investigating the theft or loss of Workstations containing PHI and/or mitigating any related harm.

E. Updates and Security

1. Users shall cooperate with Tier 1s/IT Representatives to ensure Workstations are part of a patch or vulnerability management system that requires the application of regularly scheduled antivirus software updates.
2. Users shall comply with Information Technology password management policies and standards, such as those that require each User to have a unique User authentication.
3. Health Care Components and their Tier 1s/IT Representatives shall encrypt all portable computing devices before putting them into service.
4. Health Care Components shall require their Workforce Members to register their devices that connect to the Health Care Component or University network or other system containing PHI, as required by the Health Care Component's campus IT Security policy and other applicable policy.
5. Tier 1/IT Representatives shall maintain a current Device Inventory of all devices, regardless of whether the device is owned or leased by the University or by the User, used to create, store, or maintain PHI, including but not limited to medical devices, desktops, laptops, tablets, smart phones, external storage and flash drives, in accordance with the HIPAA *Tracking, Returning, and Disposing of Device and Media* policies.

III. REFERENCES

A. HIPAA Regulations, 45 CFR 164.308(a)(1)(ii)(B)
B. HIPAA Regulations, 45 CFR 164.310
C. HIPAA Administrative and Physical Safeguards policy
D. HIPAA Breach of Unsecured PHI/ePHI policy
E. HIPAA Minimum Necessary Rule policy
F. Relevant Information Technology and IT Security policies

NOTE: Clinical work performed by dually-employed Workforce Members at the affiliated institution, OU Medicine, Inc. (d/b/a OU Health and OU Health Physicians) must be done in compliance with OU Medicine, Inc. (d/b/a OU Health and OU Health Physicians) policies and procedures.