UNIVERSITY OF OKLAHOMA

HIPAA Policies

Subject: Safeguards - Technical	**Approved:** January 2, 2014
Effective Date: January 2, 2014	**Last Revised:** 4/1/2018, 7/22/22

I. PURPOSE

To describe the Technical Safeguards that must be in place to protect each Health Care Component's ePHI from unauthorized Access and Use. (See also HIPAA *Protecting ePHI from Improper Alteration or Destruction* policy.)

II. POLICY*

Each Health Care Component, in coordination with Information Technology and the HIPAA Security Officer, shall have in place Technical access and audit controls, including encryption of portable electronic devices used to access, create, or store PHI outside of the University's VDI environment or secure data center, to protect the ePHI it maintains on its Information Systems from unauthorized Access or Use.

III. PROCEDURE

A. As part of its Technical Safeguards, each Health Care Component shall comply with or provide for the following:

1. Computer Logoff/Lock Policy - HCC administration and the HCC's assigned Tier 1 or IT Representative shall enforce both of the following requirements for computer lock and logoff:
   a. Lock – Workforce Members must manually lock or log off a computing device or application when leaving that device or application unattended, even for brief periods.
   b. Automated Lock or Logoff – All computing devices and applications must be secured with either a password-protected screen saver or automatic log off that will take effect after the time period established by IT Security, currently no more than 15 minutes of inactivity.

2. Encryption and Decryption of ePHI, as described in the HIPAA *Protecting ePHI from Improper Alteration or Destruction* policy.

Workforce Members must comply with the HIPAA policies regarding emailing PHI to patients (See HIPAA *Emailing and Transmitting PHI* policy), as well as with the policy or practice of their HCC. For OU Physicians, for example the preferred method for

communicating electronically with patients is through a secure patient portal.

B. Each HCC shall, in coordination with Information Technology and the HIPAA Security Officer, configure or enable its hardware, software, and/or procedural mechanisms to record for examination the User activity in its Information Systems that contain ePHI to the extent technology is available. Reviews of the records shall be handled in accordance the HIPAA *HCC Review of Access to ePHI Systems* policy and related University audit policies. If improper access is observed by the HCC manager, it shall be immediately reported to the University Privacy Official or HIPAA Security Officer.

C. IT representatives and Tier 1s who put University-owned, University-leased, or personally-owned** portable devices into service must encrypt the device prior to releasing it for use. Workforce Members who put such devices into service for University Business without the assistance of IT must have their Tier 1 or IT Representative encrypt the device prior to using the device to access, create, or store PHI outside of the University's VDI environment or secure data center.

D. Health Care Components, with assistance from their Tier 1 or IT Representative, must comply with all Information Technology and related policies designed to protect Information Systems that maintain ePHI, including but not limited to maintaining anti-virus software on all devices and equipment that create, transmit, or store PHI.

IV. REFERENCES

A. 45 CFR 164.312(a) – (b)
B. Information Technology Password Management Policy and Standards
C. Information Technology Transmission of Sensitive Data Policy
D. Information Technology Computer Logoff/Lock Policy
E. Information Technology Activity (Log) Review Policy
F. HIPAA Audits Policy
G. HIPAA Compliance Audit Program policy
H. HIPAA Administrative and Physical Safeguards policy
I. HIPAA Protecting ePHI from Improper Alteration or Destruction policy

** Full disk encryption is not required on Personally-owned portable devices in which the Workforce Member is only going to access ePHI through the Virtual Desktop Infrastructure ("VDI") and will only store ePHI to a secure file share that is saved in OU's secure data center through VDI. If a Workforce Member is going to access ePHI through systems outside of the VDI or anticipates they will need to store or download ePHI to their device locally, the device will need to be encrypted.

For more information visit https://apps.ouhsc.edu/hipaa/faqs/HIPAACompliantVDIVPNuse.asp or contact the HIPAA security officer.

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.