Name of Standard: Clinical Workstation Security.

Standard Number: IT – 12-002

Approving Officer: Vice President of Information Technology

Responsible Agent: Director, Health Information Technology and Healthcare Informatics; Information Security Officer

Scope: all University campuses

| X | New standard proposal | ☐ | Minor/technical revision of existing standard |
| ☐ | Major revision of existing standard | ☐ | Reaffirmation of existing standard |

(A) Purpose

This standard is intended to define specific requirements for university-owned clinical workstations used to create, receive, maintain, or transmit ePHI through the use of approved clinical applications to enforce security controls in accordance with HIPAA requirements and provide for common clinical workstation capabilities.

(B) Associated Policy

Workstation policy, 3364-65-12.

(C) Standard

This standard defines specific requirements for clinical workstations in addition to requirements identified in Workstation Policy, 3364-65-12.

Security Controls

(1) Physical security. All clinical workstations not intended to be mobile will be physically secured at the deployed location (e.g. Kensington lock or industry anti-theft grade lock, permanently affixed, or otherwise locked in place to prevent theft.)

(2) Encryption. All clinical workstations will be encrypted using currently approved enterprise encryption methods.

(3) Antivirus. In addition to antivirus requirements identified in the Workstation policy, Clinical workstations should employ anti-malware protections available through the UT web filter to the maximum extent possible. Where not possible due to subscription licensing constraints (i.e. licensing based on IP address) efforts should be made to update licensing to allow for the added protections provided by the web filter.

(4) Timeouts. All clinical workstations will enforce appropriate locking screensaver timeouts. Maximum screensaver timeouts for clinical workstations are:

(a) Imprivata enabled workstations – 5 minutes.
(b) Non-Imprivata enabled workstations – 15 minutes (maximum.)

Shorter timeouts should be enabled based on risk.
(c) Training environment – 30 minutes (maximum) provided that security awareness training concerning the necessity to lock computers prior to leaving them unattended is provided.

(D) Definitions

(1) Clinical Workstations; any university-owned workstations used to create, receive, maintain, or transmit ePHI through the use of provided clinical applications.

(2) ePHI (electronic Protected Health Information); PHI is information that will lead to the identification of an individual, either by itself or in combination with other available information.