



THE UNIVERSITY OF TEXAS AT DALLAS

SECURITY OF ELECTRONIC HEALTH CARE INFORMATION

Section 4.3: Workstation Security	Page: 1 of 3
Effective Date: March 21, 2005	

POLICY

UTD shall implement physical safeguards to restrict access to workstations that access electronic protected health information (“PHI”) only to authorized users. UTD personnel who have access to any UTD workstation (“workstations”) that are a part of the health care operations-related information systems shall be required to be familiar with this policy and shall follow the procedures below.

PERSONNEL

Security Officer

Privacy Officer

System Administrator

Facilities Manager

Director-on-call

End User

Management

IMPACTED SYSTEMS

This workstation use policy shall apply to electronic computing devices that have access to PHI, including personal computers, laptop computers, personal digital assistants (“PDAs”), tablet computers, or other devices that perform similar functions, and electronic media stored on electronic computing devices.

PROCEDURES

1. Locations of Workstations.
 - a. To the extent possible, Director-on-call shall locate non-portable workstations that access PHI in areas restricted to authorized UTD workforce members.
 - b. Director-on-call shall locate workstations that contain or access PHI in areas that are continuously monitored by UTD Security and/or UTD workforce members, where practicable. Areas containing workstations, if possible, shall be securely locked when the workstation is unattended.
 - c. For workstations located in non-secure areas, Users shall face the computer monitors away from public view in order to protect PHI or other data from being observed where possible, else use monitor privacy filters .
2. Portable Devices.
 - a. Portable computing devices, including laptop computers, personal digital assistants (PDAs), portable storage devices, etc., while at UTD's facilities, shall be locked up at the end of each workday.
 - b. Users shall secure portable computing devices when such devices are used outside of UTD facilities.
 - c. If a User accesses PHI from a portable computer device, the device shall be password-protected so that Users must enter a password before access is granted. The PHI data on the portable computer device must be encrypted using UTD-approved digital encryption methodology.
 - d. If accessing PHI from portable computing devices, Users shall prevent the information from being viewed by others.
3. Screen Savers. Workstations for use by UTD workforce members or any workstations that are located in areas accessible by persons outside UTD shall be secured with password-protected screensavers.
 - a. System Administrator shall ensure that workstations from which PHI is accessible have screen savers set to turn on following not more than ten (10) minutes of inactivity. Users shall not be authorized to change this default setting.
 - b. The screensaver shall require Users to enter an assigned unique User ID and a password to gain access to the workstation.

4. Servers. Director-on-call shall locate servers in areas that can be securely locked and physical access controlled in accordance with the Facility Access Controls Policy (*see* Section 4.1 of this Manual).

Date Approved: _____

Date Revised/Reviewed: _____

Approved By: _____

Title: _____

Signature: _____

