



THE UNIVERSITY OF TEXAS AT DALLAS

SECURITY OF ELECTRONIC HEALTH CARE INFORMATION

Section 4.2: Workstation Use	Page: 1 of 5
Effective Date: March 21, 2005	

POLICY

UTD shall implement procedures that specify the proper functions to be performed on workstations, the manner in which those functions shall be performed, and the physical attributes of workstations that can access electronic protected health information (“PHI”). UTD personnel who have access to any UTD workstation that is a part of the health care operations-related information systems shall be familiar with this policy and shall follow the procedures below.

PERSONNEL

Security Officer

Privacy Officer

Director-on-call

System Administrator

End Users

Management

Human Resources

IMPACTED SYSTEMS

This Workstation Use policy shall apply to all workstations that contain or have access to PHI, which include electronic computing devices, such as personal computers, laptop computers, personal digital assistants (“PDAs”), tablet computers, or devices that perform similar functions, and electronic media stored on electronic computing devices.

PROCEDURES

1. Proper Functions to Be Performed.
 - a. UTD shall provide workstations to UTD's workforce members for the purpose of performing their job functions for UTD. Users of UTD workstations shall be responsible for using workstations appropriately in conformance with this Policy.
 - b. Users shall use workstations to perform the duties that are a necessary part of a workforce member's job function. Such functions may include, but are not necessarily limited to, data entry, charting, accessing medical records, updating medical records, storing PHI, accessing PHI, scheduling, researching, billing, corresponding for UTD health care operations-related purposes, printing, and faxing.
2. Functions That May Not Be Performed.
 - a. Users shall not use workstations to access any confidential patient information or any other confidential or proprietary information of UTD that they do not have a need to know to perform a job-related function for UTD.
 - b. Users shall not use workstations to transmit any confidential patient information or any other confidential or proprietary information of UTD to any third party unless authorized by Callier Center Management, the Privacy Officer, or the Security Officer.
 - c. Users shall not download PHI from UTD's information systems and store it on a workstation, except as necessary to perform job functions on behalf of UTD.
 - d. Users shall not attempt to evade the access rights granted to the User and shall not attempt to access any network, system, application, or data to which the User has not been granted access.
 - e. To protect against computer viruses from being transmitted onto workstations and into UTD's electronic information systems, Users shall not download from the Internet any unauthorized programs or applications and shall not upload any unauthorized external software or data. Before a workforce member downloads programs or applications from the Internet or uploads any external software to a workstation, the User shall receive the approval of the Director-on-call.

- f. Users of workstations shall not open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source and shall delete these attachments immediately because they may contain viruses, e-mail bombs, or Trojan Horse code.
- g. Users shall not install non-UTD hardware on any workstations unless approved by the Director-on-call or install unauthorized modems or other communications devices to the network.
- h. Users shall not use an UTD-owned workstation to engage in an activity prohibited by UTD's employee handbook, UTD's Information Resources Security or Human Resources policies and procedures.
- i. Users shall not engage in any activity that is illegal under local, state, federal, or international law while using UTD-owned workstations.
- j. Users shall not use UTD-owned workstations for personal gain or for business-related purposes or functions unrelated to the User's job function with UTD.
- k. Users shall not remove from UTD's facilities electronic media that contains PHI or confidential or proprietary UTD information unless such removal is authorized by a User's supervisor and the User signs out the media in accordance with the Device and Media Controls Policy (*see* Section 4.4 of this Manual).

3. Manner in Which Functions Are to Be Performed.

- a. *Entry of Assigned User ID.*
 - i. If the entry of a unique User ID and/or password is necessary to use a workstation, Users shall log onto the workstation using the User ID assigned to that User.
 - ii. Users shall not log onto a workstation using another person's User ID or password nor shall the User permit another person to log on with his or her User ID or password.
 - iii. Users shall not enter data under another User's unique User ID or password.
 - iv. Users shall not attempt to mask their identity while logged onto a workstation or UTD's network.

- v. Users shall be responsible for the security of their unique User ID's, passwords, and accounts.
 - vi. Users shall keep their User IDs and passwords confidential.
 - vii. Users shall change passwords in accordance with UTD Information Resources Security Policy and Procedures.
- b. Users shall keep their computer monitors away from public viewing during use, especially if the User is accessing PHI.
 - c. Users shall log off workstations or establish a password-protected screen saver before leaving the workstation unattended for more than 10 (ten) minutes (*see* Section 4.3 of this Manual) unless such workstation is located in a controlled physical environment.
 - d. Users shall not leave printers unattended when they are printing PHI or other confidential information. This procedure is especially important when two or more computers share a common printer or when the printer is located in an area where unauthorized personnel have access to the printer.
 - e. Hard-copy printouts of PHI shall only be made if needed for treatment or billing purposes or if access is requested by the patient or to respond to a valid authorization. Only the minimum necessary information shall be printed. The printouts shall be shredded and disposed of after use, if the printouts are not placed in a patient's file.
 - f. Users shall erase PHI from electronic media not contained in a patient's file or not used for back-up purposes.
4. Physical Attributes of Workstations and Surroundings.
- a. Facility Managers and/or Director-on-call shall, if possible, locate workstations only in areas that are physically secured and where access is limited to only authorized UTD workforce members.
 - b. System Administrator shall install on workstations a password-protected screensaver that requires Users to enter a User ID and password to access. The workstations shall have a time-out feature after a certain period of inactivity.

- c. *Anti-Virus Procedures.* UTD shall employ currently acceptable means by which to detect and prevent the spread of computer viruses, worms, Trojan Horses, or any other agents designed to alter or destroy data.
 - i. Workstations shall have anti-virus protection software that detects computer viruses, worms, Trojan Horses, and any other disabling agents. Users shall not disable the anti-virus software.
 - ii. The anti-virus protection software shall be installed so that all attachments are scanned before downloading to a workstation and prevent the download of attachments containing viruses, worms, Trojan Horses or other disabling agents.
 - iii. Users shall scan for viruses or other disabling agents whenever external files are placed on any workstation that accesses UTD's internal network and computer system.

- 5. Servers. Director-on-call shall configure servers to perform a single function, if possible. For example:
 - a. System Administrator shall configure network servers' host machines to offer only essential network services and operating system services.
 - b. System Administrators shall configure the web server with appropriate object, device, and file access controls and to enable only web server specific logging mechanisms.
 - c. System Administrator shall configure authentication servers to store information relating to user accounts, user IDs and passwords.

Date Approved: _____	Date Revised/Reviewed: _____
Approved By: _____	_____
Title: _____	_____
Signature: _____	_____