



THE UNIVERSITY OF TEXAS AT DALLAS

SECURITY OF ELECTRONIC HEALTH CARE INFORMATION

Section 4.4: Device and Media Controls	Page: 1 of 9
Effective Date: March 21, 2005	

POLICY

UTD shall implement reasonable and appropriate controls to govern the receipt and removal of hardware, to govern electronic media that contain electronic protected health information (“PHI”) into and out of UTD’s facilities and within UTD’s facilities, and to implement methods to dispose of electronic PHI.

PERSONNEL

Security Officer

Privacy Officer

Facilities Manager

System Administrator

Director-on-call

Workforce Members

Callier Center Management

Security Personnel

IMPACTED EQUIPMENT

This policy shall apply to UTD-owned hardware containing electronic PHI, including servers, PCs, laptops, personal digital assistants (PDAs), etc. and electronic media containing PHI, including hard disk drives, DVDs, CDs, flash drives, pen drives, USB drives, diskette tapes, floppy disks and other portable storage devices.

PROCEDURES

1. Receipt of Hardware or Electronic Media Containing PHI. The following procedures shall govern the receipt of hardware or electronic media containing PHI from outside entities or persons:
 - a. The Supervisor of Medical Records shall receive any hardware or electronic media containing PHI on UTD's behalf. If any UTD workforce member receives hardware or electronic media containing PHI, the workforce member shall notify the Supervisor of Medical Records to coordinate the receipt in accordance with the procedures in this Device and Media Controls Policy.
 - b. Upon receipt of hardware or electronic media containing PHI, the Supervisor of Medical Records shall log who received the hardware or electronic media, a description of the hardware (including the serial number) or type of media, from whom received, the person(s) to whom the PHI pertains, the reason for receiving, and the date of receipt. (See Appendix 4.4.1 for a sample of the *Receipt of Hardware or Electronic Media Containing PHI Log* form)
 - c. If the hardware or electronic media containing PHI is subsequently returned to the person or entity who initially gave it to UTD, the date of return, to whom returned and the person returning it shall be recorded in the log described in paragraph 1(b) above. (See Appendix 4.4.1 for a sample of the *Receipt of Hardware or Electronic Media Containing PHI Log* form)
2. Movement of Hardware and Electronic Media from UTD's Facilities.
 - a. UTD workforce members shall not remove from UTD's facilities any hardware or electronic media containing electronic PHI nor download PHI to any computer, device, or network that is not located in UTD's facilities without the approval of the Data Owner(s) or Callier Center Management. Such approval shall only be granted if the hardware, electronic media or downloaded PHI is necessary for the performance of a job-related function on UTD's behalf.
 - b[jd11]. If a workforce member needs to remove from UTD's facilities hardware or electronic media containing PHI or download PHI to any computer, device, or network that is not located in UTD's facilities, the workforce member shall make a written request to the head of the workforce member's department or Callier Center Management on a form specified by the Security Officer or Callier Center Management. (See Appendix

4.4.2 for a sample of the *Request to Remove PHI from UTD Callier Center* form. Instructions for completing and processing the form are included on the form.)

- i. The request form shall include at a minimum the following:
 - (A) the name of the workforce member;
 - (B) the date range for which the request is made;
 - (C) if the request involves UTD hardware, the property tag number, brief description and serial number of the device, and an acknowledgement and acceptance of the workforce member's obligations under UTD Property Administration policies and procedures to safeguard such hardware;
 - (D) if the request involves only electronic media, a description of the media including type and date of creation;
 - (E) the basis for the request, including the name and account identifying number (CCCD#) of the patient(s) whose PHI is either stored on the hardware or electronic media or whose PHI will be downloaded by the workforce member; and,
 - (F) an acceptance of responsibility for safeguarding and protecting the confidentiality of any PHI contained on the hardware or electronic media or downloaded PHI in accordance with this Manual and UTD's Employee Handbook.
 - ii. The head of the workforce member's department or Callier Center Management shall not grant any request to remove hardware or electronic media containing PHI or download PHI unless it is necessary to perform a job function for UTD and the request has the approval of the Data Owner(s), if different from the head of the workforce member's department or Callier Center Management.
 - iii. If the workforce member's duties involve continued need and use of the same patient(s) PHI over an extended period of time, e.g. a semester, an academic year, etc., a single check-out form may be used with the proviso that approval is only granted for such time period, the equipment or electronic media must be presented to the approver for inspection at least once every six months or semester end, whichever shall occur first, and that a new check-out form must be prepared at least annually or whenever the patient(s) whose PHI is stored on the equipment or electronic media change.
- c. UTD workforce members shall return the hardware or electronic media or erase the downloaded PHI when the job function is completed. If not

erased, the workforce member shall safeguard the information in accordance with paragraph 2(b)(i)((F)) of this Policy.

- d. UTD workforce members may remove from UTD's facilities personal portable computing devices (notebook or laptop computers, pocket computers, personal digital assistant devices (PDAs) or other similar computing devices) that contain or are capable of accessing PHI provided that the provisions of paragraphs 2(a) through 2(c) of this Policy are adhered to. In addition to those provisions, the following additional requirements shall be in force:
 - i. The portable computing device shall be password-protected, requiring that the workforce member enter a password before accessing any PHI.
 - ii. The PHI on portable computing devices shall be encrypted.
 - iii. If PHI is uploaded from the portable computing device to a computer, the workforce member shall be responsible for safeguarding such PHI on that computer in accordance with all applicable policies and procedures of this Manual. For example, the workforce member shall have in place role-based access so that only those allowed to access the PHI under this Manual may do so; there must be adequate firewall protections to prevent unauthorized external access. Moreover, the PHI shall be permanently deleted in its entirety from the computer after use in accordance with the procedures for removal of PHI contained in this Manual.
 - iv. The workforce member shall be responsible for the security of the device and protecting the confidentiality of any PHI in accordance with paragraph 2(b)(i)((F)) of this Policy.
- e. UTD workforce members shall promptly report the loss or theft of any hardware, electronic media, or any PHI data stored on the hardware or electronic media to Callier Center Management, the head of the workforce member's department, the Data Owner(s) and the Security Officer.

3. Final Disposal of Electronic PHI.

- a. *Removal Standard.* System Administrator shall ensure that PHI subject to final disposition by UTD is disposed of by using a method that ensures the PHI cannot be recovered or reconstructed.
- b. *Retrievable Copy.* Callier Center Management shall ensure that a retrievable back-up copy is made before submitting hardware or electronic

media for disposal of electronic PHI if it contains the only copy of the electronic PHI that is required or needed by UTD.

- c. *Hardware.* System Administrator shall be responsible for the final disposal of hardware that contains PHI or the final disposal of electronic PHI on hardware using the following methods:
 - i. Electronic PHI on Retained Hardware.
 - (1) If UTD is deleting PHI but not the hardware, System Administrator shall remove PHI from hardware using initialization utilities installed on such hardware that are designed to permanently remove data from memory locations.
 - (2) If all data is being removed from the hardware, System Administrator shall reformat and overwrite memory locations using an appropriate overwriting program or degauss the hardware if practical and appropriate.
 - (3) System Administrator shall maintain a log of such data destruction that lists the device, the date of destruction, the workforce personnel authorizing the destruction, general description of the PHI (if available), and the identity of the workforce personnel performing the destruction.
 - ii. Electronic PHI on Hardware Being Disposed of by UTD. System Administrator shall remove all PHI from hardware being sold, replaced, or destroyed so that it cannot be recovered or reconstructed using appropriate disposal techniques. System Administrator shall employ one of the techniques listed below:
 - (1) Using appropriate initialization utilities installed on the hardware that are designed to permanently remove data from memory locations;
 - (2) Running an overwriting program on such hardware that overwrites all memory locations.
 - (3) Degaussing any hardware to the extent practical and appropriate.
 - (4) System Administrator shall maintain a log of such data destruction that lists the device, the date of destruction, the workforce personnel authorizing the destruction, general

description of the PHI (if available), the identity of the workforce personnel performing the destruction and the disposition of the device. (See Appendix 4.4.3 for a sample of the *PHI Destruction Log*.)

- d. *Electronic Media*. System Administrator shall be responsible for the final disposal of PHI on electronic media and/or the final disposal of the electronic media on which it is stored. Although Users may erase any PHI contained on electronic media, any media containing PHI to be disposed of on a final basis by UTD shall be submitted to System Administrator for deletion.
 - i. *Specific PHI on Electronic Media*. System Administrator shall delete PHI stored on electronic media using utilities that are designed to permanently remove data from memory locations.
 - ii. *Destroying All Data on Electronic Media*. System Administrator shall destroy all data on electronic media intended to be re-used, sold, replaced or destroyed using appropriate disposal techniques. System Administrator shall employ one of the techniques listed below:
 - (1) Degaussing computer tapes and diskettes to prevent recovery of electronic PHI;
 - (2) Reformatting the electronic media and overwriting the memory locations;
 - (3) Overwriting data with a series of characters;
 - (4) If the electronic media is not to be re-used, physically damaging the media to the level that the media is no longer usable and data cannot be retrieved from the media.
 - iii. System Administrator shall maintain a log of such data destruction that lists the device, the date of destruction, the workforce personnel authorizing the destruction, general description of the PHI (if available), and the identity of the workforce personnel performing the destruction. (See Appendix 4.4.3 for a sample of the *PHI Destruction Log*.)
4. Media Re-use.
- a. *Media Re-use Standard*. Media shall not be re-used for any purpose other than storing other PHI unless all PHI has been removed from the media

before such re-use. However, if the media is re-used as part of UTD's data back-up procedures or disaster recovery, such media shall not be subjected to these procedures before each re-use.

- b. *Personnel Responsibility.* Users shall not re-use CDs, diskettes or other electronic media on which PHI has been stored for any purpose other than storing other PHI before the PHI is removed by Systems Administrator using one of the following methods:
 - i. Degaussing computer tapes and diskettes to prevent recovery of electronic PHI;
 - ii. Reformatting the electronic media and overwriting the memory locations; or,
 - iii. Overwriting data with a series of characters;

5. Addressable Implementation Specifications.

- a. *Accountability.* UTD shall implement the following procedures to maintain a record of the movements of hardware and electronic media and any person responsible for such movement:
 - i. Hardware.
 - (1) UTD shall employ inventory controls by affixing bar codes to each piece of hardware and take inventory on an annual basis throughout the enterprise to track hardware and its location within the facility. Callier Center Management will use the results of such inventory to accomplish the following:
 - (a) When equipment containing electronic PHI is moved within the facility, the location of the equipment shall be recorded by the head of the department where the equipment is located and who moved the equipment and the information shall be reported to the Director-on-call to track the equipment.
 - (2) The head of the department shall maintain a log of any hardware containing electronic PHI that has been removed from UTD's facilities, that notes the workforce member removing the equipment, the date of removal, the person approving the removal, and the date the hardware was

returned. Workforce members shall fill out forms in accordance with paragraph 2(b) of this Policy. (See Appendix 4.4.2 for a sample of this form, including the instructions for completing and processing it.)

- (3) UTD workforce members shall not otherwise remove hardware containing PHI from UTD's facilities without prior written approval from the head of the workforce member's department or Callier Center Management.

ii. *Electronic Media.*

- (1) The head of the workforce member's department or Callier Center Management shall maintain a log of any media^[jd12] containing electronic PHI that has been removed from UTD's facilities showing the type of media, workforce member removing the media, the date of removal, the person approving the removal, and the date the media was returned. Workforce members shall fill out forms in accordance with paragraph 2(b) of this Policy.

- (2) UTD workforce members shall not otherwise remove electronic media containing PHI from UTD's facilities without approval from the head of the workforce member's department or Callier Center Management.

b. *Data Back-up and Storage.*

The Systems Administrator shall implement the following procedures to create a retrievable, exact copy of PHI, when needed, before equipment is moved:

- i. *Back-up Data.* The Systems Administrator shall back up all files containing PHI to a computer, tape, CD Rom, disk, or other storage media before equipment is moved within UTD.
- ii. *Validate Accuracy.* The IT Department shall use a UTD-approved backup software application's reporting utilities to validate the accuracy, completeness and integrity of the back-up.
- iii. *Secure Back-up.* The backed-up data shall be stored in a secure area until it is placed on different equipment or restored to the original equipment from which it was removed.

Date Approved: _____

Date Revised/Reviewed: _____

Approved By: _____

Title: _____

Signature: _____

