



THE UNIVERSITY OF TEXAS AT DALLAS

SECURITY OF ELECTRONIC HEALTH CARE INFORMATION

Section 3.4: Workforce Security	Page: 1 of 3
Effective Date: March 21, 2005	

POLICY

UTD shall protect the confidentiality and integrity of electronic protected health information and permit only authorized individuals access to such information. This policy shall apply to all members of UTD's workforce in each location where UTD conducts business.

PERSONNEL

Security Officer

Privacy Officer

Director-on-call

Callier Center Management

Human Resources

Internal Audit

PROCEDURES

1. Authorization and Supervision. UTD has implemented the following procedures to ensure appropriate authorization and supervision over its workforce members who either work with electronic protected health information or work in locations where electronic protected health information might be accessed:
 - a. *Authorization.* Security Officer shall assign unique user IDs to all workforce personnel. Access rights shall be granted by Director-on-call or designated System Administrators in accordance with the Access Control Policy (Section 5.1 of this Manual). Also in accordance with this policy, they shall modify or terminate access rights as required by a change in the

applicable UTD workforce personnel's job position or as required by an emergency or temporary circumstance. In addition, they shall protect UTD's systems by requiring screen savers with password controls in accordance with the Workstation Security Policy (Section 4.3 of this Manual).

- b. *Supervision.* Director-on-call shall authorize maintenance personnel and other employees access to areas where protected health information may be stored only under certain conditions and with adequate supervision. Director-on-call shall restrict access to its facilities by contractors and visitors in accordance with the Facility Access Controls Policy (Section 4.1 of this Manual). In accordance with the Security Training Section of the Information Resources Use and Security Policy, Human Resources shall provide training to promote effective supervision of employees who work with and/or in proximity to protected health information. In accordance with the Security Management Process Policy (Section 3.1 of this Manual), Management shall review reports prepared by the Security Officer and Director-on-call on a semi-annual basis to determine if any problem reported could have been prevented by increased supervision.

2. Workforce Clearance Procedure. The Security Officer and UTD Callier Center Management shall work together to ensure that each workforce member's access to electronic health information is appropriate and consistent with the minimum necessary rule set forth in Section 6.1 of the Privacy Manual. In accordance with the Access Control Policy (Section 5.1 of this Manual), access rights shall be granted based on a workforce member's role within UTD. In accordance with the Evaluation of Safeguards Policy (Section 12.1 of the Privacy Manual) and the information systems activity review portion of the Security Management Process Policy (Section 3.1 of this Manual), Internal Audit shall conduct evaluations on a yearly basis during which Internal Audit shall take a sample of current system users of various positions within UTD to ensure that their passwords do not allow them access to more information than intended by management. Internal Audit shall also take multiple samples of current system users in the same job position to ensure that their passwords do not allow them access to more information than other users in the same job position, unless otherwise intended by documented requests of management. In addition to the authentication and testing of passwords, Internal Audit shall conduct annual reviews of the adequacy of its administrative, technical, and physical safeguards in accordance with the Evaluation of Safeguards Policy (Section 12.1 of the Privacy Manual) and the Security Management Process Policy (Section 3.1 of this Manual).

3. Termination Procedures. Security Officer, Human Resources and Director-on-call shall perform the following procedures for terminating access to electronic protected health information when the employment of a workforce member ends:

- Upon the termination of a workforce member, Director-on-call and Security Officer ensure that such person no longer has access to sensitive areas containing PHI, such as computer equipment storage facilities, data centers, communication closets and medical records storage facilities.
- Human Resources shall remove such person’s name from its list of authorized employees, contractors, and volunteers and shall file any information regarding such person with the records of other terminated workforce members.
- Callier Center Management shall recover all keys, identification cards, physical tokens, and any other objects that facilitate physical access to property, buildings, and equipment. Security Officer and Director-on-call shall change the locks and/or combinations that control physical access to areas and equipment on a semi-annual or as-needed basis.
- Callier Center Management shall recover any information regarding UTD and any property of UTD that may be in the terminated workforce member’s possession. Callier Center Management or Human Resources may require that terminated workforce members are escorted while they pack their belongings and as they leave the premises.
- Security Officer and Director-on-call shall deactivate user identification numbers, passwords, tokens, and other electronic access codes upon the termination of employment of a workforce member.

Date Approved: _____

Date Revised/Reviewed: _____

Approved By: _____

Title: _____

Signature: _____
