



THE UNIVERSITY OF TEXAS AT DALLAS

SECURITY OF ELECTRONIC HEALTH CARE INFORMATION

Section 3.5: Information Access Management	Page: 1 of 3
Effective Date: March 21, 2005	

POLICY

UTD shall establish procedures that (i) assign and manage access to electronic protected health information (“PHI”) in a manner commensurate with the role of each workforce member, and (ii) are consistent with the Security Rule. This policy shall apply to all UTD personnel.

SYSTEMS AFFECTED

This policy shall apply to UTD’s computer systems that contain or access electronic PHI, including, but not limited to, network servers, application servers, desktop computer systems, laptops, handheld devices, data management systems, and infrastructure devices.

PERSONNEL

Security Officer or designee

Director-on-call

System Administrator

Human Resources

Privacy Officer

PROCEDURES

1. Access Authorization.
 - a. The Security Officer shall establish role-based access as set forth in the Access Control Policy and Workforce Security Policy.
 - b. The authorization criteria shall include required levels of training and training certification requirements commensurate with the level of access in accordance with the Security Awareness and Training Policy. The access level shall be established by either the Security Officer or his or her

designee, and approval may be for a limited period. Renewal or a change of access level may require full re-evaluation of access needed and may require additional training.

- c. A member of the workforce shall not be authorized to access another workforce member's client record unless it is for the purpose of treatment, payment, or health care operations associated for the member of the workforce whose record is accessed.

2. Access Establishment.

- a. Information Security shall implement the following procedures to ensure appropriate access and access authorization:
 - i Upon hire, each workforce member shall be identified by the security class applicable to their job functions.
 - ii User department shall ensure that new workforce members complete the appropriate access request form in order to establish the appropriate level of access and to request a unique user identification number. The department head of the new workforce member shall sign the access request form to verify accuracy.
 - iii Once approval is obtained and the appropriate access request form has been signed by all necessary parties, as set forth above, Information Security or Director on Call will assign appropriate access.

3. Access Modification.

- a. If a workforce member's employment is terminated or if a workforce member leaves UTD or if a workforce member's position is changed so that the workforce member is performing a different role:
 - i User department shall notify Security Officer.
 - ii Security Officer and Director-on-call shall implement the procedures set forth in the Workforce Security of this Manual if the workforce member is being terminated.
 - iii System Administrator shall modify or terminate access upon instruction from Security Officer or Director-on-call, as set forth in the Access Control Policy of this Manual.

Date Approved: _____

Date Revised/Reviewed: _____

Approved By: _____

Title: _____

Signature: _____
