



THE UNIVERSITY OF TEXAS AT DALLAS

SECURITY OF ELECTRONIC HEALTH CARE INFORMATION

Section 5.4: Person or Entity Authentication	Page: 1 of 4
Effective Date: March 21, 2005	

POLICY

UTD shall employ technical safeguards to verify that a person or entity seeking access to electronic protected health information (“PHI”) is the one claimed. This policy shall apply to all UTD locations. End Users (*see* definition of End User in Section 2 of this Manual) shall be familiar with this policy.

PERSONNEL

Security Officer

Privacy Officer

System Administrator

End Users

Callier Center Management

PROCEDURE

1. Personnel Responsibility.
 - a. *Implementation of Procedures.* System Administrator shall initiate and oversee the implementation of the following procedures for person and entity authentication, either singly or in combination, to authenticate that the person or entity seeking access to electronic protected health information is the one claimed.
 - b. *Monitoring Access Attempts.* System Administrator shall review access logs to monitor and detect unauthorized access attempts.
2. Person Authentication.
 - a. *Person Password Authentication.*

- i. System Administrator shall assign to each UTD workforce personnel and any other person that must access electronic PHI stored on UTD's computer systems each User's unique User ID pursuant to the Access Control Policy (*see* Section 5.1 of this Manual).
- ii. Users shall select passwords in accordance with the procedures described in the Access Control Policy (*see* Section 5.1 of this Manual).
- iii. Each User shall enter a password along with his or her unique User ID to authenticate his or her identity. A User shall be denied access if the password entered does not match the password assigned to the User ID entered by the User.

b. *End User Responsibility.*

- i. Users shall be responsible for keeping their User IDs and passwords confidential and shall be forbidden from sharing their User IDs and passwords with anyone, unless authorized by System Administrator.
- ii. If User becomes aware that someone has improperly obtained his or her User ID and password or has improperly accessed UTD's health care operations-related electronic system through the use of the User ID and password, the User shall immediately notify the Security Officer or System Administrator. System Administrator shall promptly disable access rights to that User ID.
- iii. If User's unique User ID and password are improperly used to gain access to electronic PHI, the User may be subject to discipline in accordance with UTD's Sanctions Policy (*see* Section 3.2 of this Manual), which may include the loss of his or her access rights.

3. Entity Authentication.

a. Entity Password Authentication.

- i. System Administrator shall assign to each entity needing access to UTD's electronic information system containing PHI a unique ID pursuant to the Access Control Policy (*see* Section 5.1 of this Manual).
- ii. Entities shall select passwords in accordance with the procedures described in the Access Control Policy (*see* Section 5.1 of this Manual).

iii. Each entity shall enter a password along with the unique User ID assigned to it to authenticate its identity. An entity shall be denied access if the password entered does not match the password assigned to the User ID entered by the entity.

b. *Entity Responsibility.*

i. Entities shall be responsible for maintaining the confidentiality of their unique User IDs and the passwords. Entities shall not make UTD's assigned User IDs and their passwords available company-wide. The unique User ID and password shall only be provided to those entity personnel with a need to know to perform a service on UTD's behalf. An entity may lose its access rights for failing to protect the confidentiality of the unique User ID and password.

ii. If an entity determines that any of its personnel or any other person or entity has improperly obtained its User ID and password or has improperly accessed UTD's health care operations-related electronic system through the use of the User ID and password, the entity shall immediately notify Callier Center Management or Security Officer. System Administrator shall promptly disable access rights to that entity's User ID.

iii. Callier Center Management or the Security Officer shall determine the proper response to an entity's failure to properly safeguard its User ID and password. Such response may include a recommendation to the Chief Operating Officer to deny access rights to the entity or termination of the business relationship.

4. Two-factor Authentication.

UTD has determined at this time not to require two-factor authentication based upon its risks analysis and cost/benefits analysis. The Security Officer shall review this determination on an annual basis to determine whether it is reasonable and appropriate to implement two-factor authentication.

5. Digital Signature Authentication.

UTD has determined at this time not to require digital signature authentication based on public key encryption due to a lack of infrastructure support. Security Officer shall review this determination on an annual basis to determine whether it is reasonable and appropriate to implement such digital signature authentication.

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