



THE UNIVERSITY OF TEXAS AT DALLAS

CONFIDENTIALITY OF HEALTH CARE INFORMATION

Section 3.6: Security Awareness and Training	Page: 1 of 4
Effective Date: March 21, 2005	

POLICY

UTD health care operations and designated Information Resources department workforce members shall receive training on UTD's HIPAA security policies and procedures with respect to safeguarding electronic PHI as reasonable and appropriate to carry out their functions within or on behalf of UTD.

PERSONNEL

Security Officer

Privacy Officer

Director-on-call

Workforce Members

System Administrator

Human Resources

Callier Center Management

PROCEDURES

1. Responsibility for Training. Callier Center Management shall oversee the training of UTD workforce members regarding UTD's HIPAA security policies and procedures. Callier Center Management shall work with the Security Officer

to develop a security program to cover the policies and procedures in this Manual and the Security Rule.

2. Duties of Security Officer. The Security Officer shall have the following duties with respect to developing and administering a training and security awareness program:
 - a. working with Callier Center Management to modify UTD's existing training program to include the policies and procedures in this Manual and any additional requirements under the Security Rule;
 - b. developing a security awareness program on the policies and procedures in this Manual and the Security Rule (e.g., posters in hallways, monthly presentations);
 - c. obtaining any necessary additional training regarding HIPAA security requirements;
 - d. developing standardized methods and materials to provide security training;
 - e. ensuring that current policies and procedures are addressed periodically at departmental staff meetings;
 - f. ensuring that the form of training is tailored to UTD's policies and procedures and workforce members' job functions and activities in their working environment;
 - g. maintaining all documentation of training; and
 - h. developing competency tests to evaluate training effectiveness.
3. Initial Training.
 - a. Callier Center Management shall ensure that initial training for all existing workforce members must take place before April 20, 2005, the deadline for compliance with the Security Rule.
 - b. Callier Center Management shall ensure that training of new workforce members must occur as stated in Section 11 of the Privacy Manual. Callier Center Management shall provide security policies and procedures to be included in any orientation information packet provided to new employees, trainees, volunteers, vendors, and clinical staff.
4. Additional Security Training. After initial training, workforce members shall complete additional training periodically in response to environmental and operational changes affecting the security of electronic PHI and, at a minimum, on an annual basis. In addition, in the event of a material change in UTD's HIPAA security policies and procedures, workforce members whose functions are affected by the material change shall complete additional training within a reasonable period of time, generally 30 days after the material change becomes effective.
5. Addressable Implementation Specifications.

- a. *Periodic Security Updates.* The Security Officer shall ensure that security updates are provided to workforce members periodically.
 - i. The Security Officer shall meet periodically with the Director-on-call to become aware of the latest information technological advances and potential security threats.
 - ii. The Security Officer and Director-on-call shall develop methods for delivering security updates that address environmental and operational changes that affect the security of electronic PHI. Such methods could include:
 - (1) Distributing pamphlets;
 - (2) E-mailing security updates; or
 - (3) Conducting security presentations.
- b. *Malicious Software.* The Security Officer shall provide as part of the security training program user education on guarding against, protecting from and reporting of malicious software, including educating workforce members regarding:
 - i. the danger of malicious software, such as viruses, worms, Trojan Horses or any other agents that can alter or destroy data;
 - ii. preventing the spread of computer viruses, worms, Trojan Horses or any other agents designed to alter or destroy data;
 - iii. use of anti-virus protection software;
 - iv. not downloading files or applications from the Internet;
 - v. not opening files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source;
 - vi. ensuring that any external files to be placed on any computer accessing UTD's internal network and computer system are scanned for viruses or other disabling agents; and
 - vii. alerting the Technical Services Department upon discovery of an infected computer or other electronic media.
- c. *Monitoring Log-in Attempts.* The Security Officer or Director-on-call shall provide as part of the security training program user education on monitoring log-in attempts and reporting discrepancies if the User becomes aware of such discrepancy.

- d. *Password Management.* The Security Officer or Director-on-call shall provide as part of the security training program user education on creating, changing and safeguarding passwords, including educating End Users regarding UTD’s Password Standards in Section 5.1 of this Manual.

Date Approved: _____

Date Revised/Reviewed: _____

Approved By: _____

Title: _____

Signature: _____

