



THE UNIVERSITY OF TEXAS AT DALLAS

SECURITY OF ELECTRONIC HEALTH CARE INFORMATION

Section 3.10: Evaluation	Page: 1 of 3
Effective Date: March 21, 2005	

POLICY

UTD shall perform periodic technical and non-technical evaluations to establish the extent that UTD's HIPAA Security Policies and Procedures meet the requirements of the Security Rule based upon (a) the standards and specifications of the Security Rule and (b) environmental and operational changes affecting the security of electronic protected health information ("PHI").

PERSONNEL

Security Officer

Privacy Officer

Director-on-call

Internal Audit Office

System Administrator

Facilities Manager

Senior Management

PROCEDURES

1. Initial Evaluation.
 - a. Before implementing the policies and procedures of this Manual, Internal Audit shall initiate and oversee the evaluation of each policy and procedure in this Manual to demonstrate and document compliance with the Security Rule.

- b. Internal Audit shall initiate and oversee the evaluation of UTD's technical and physical safeguards put in place to safeguard electronic PHI to demonstrate and document compliance with the policies and procedures of this Manual (once the Manual has been certified as being in compliance with the Security Rule) and the requirements of the Security Rule.
- c. This initial evaluation shall be completed no later than one (1) month before the implementation date of the policies and procedures in the Manual.
- d. Internal Audit shall prepare a detailed report regarding each area of noncompliance. Internal Audit shall submit the report to the Security Officer, Privacy Officer, and Callier Center Management.
- e. To the extent that any policy or procedure is not in compliance with the Security Rule, the Security Officer shall review and remedy the area of noncompliance and present the revision to Callier Center Management for approval.
- f. To the extent that a technical or physical safeguard is not in compliance with the policies and the Security Rule, the Security Officer shall meet with the Director-on-call or Facilities Manager to resolve and remedy any areas of noncompliance in UTD's technical or physical safeguards. The Security Officer shall review any revision to a technical or physical safeguard to determine compliance with the Security Rule.
- g. Any approved changes to a policy or procedure in this Manual shall be presented to the Security Officer for re-evaluation to determine compliance with the Security Rule.

2. Implementation Evaluation.

- a. Within the first six months of the implementation of this Manual, Internal Audit shall re-evaluate the policies and procedures to determine compliance by UTD personnel with the policies and procedures in this Manual and the continued compliance of the policies and procedures with the Security Rule.
- b. Areas of noncompliance shall be presented to the Security Officer, the Privacy Officer, and Callier Center Management in a written report that fully describes the noncompliant practices. The Security Officer and Callier Center Management shall be responsible for addressing the areas of noncompliance and bringing UTD into compliance with the security policies and procedures in this Manual and with the Security Rule.

3. Periodic Evaluations

- a. Internal Audit shall review no less than once a year:
 - (i) Each policy and procedure in this Manual to assure continued compliance with the Security Rule.
 - (ii) Each technological and physical safeguard to assure continued compliance with this Manual and the Security Rule.
 - (iii) UTD's compliance with the policies and procedures in this Manual.

The Security Officer shall assist in such review.

- b. The Security Officer and Callier Center Management shall address and remedy any policy, procedure, or safeguard determined not to be compliant.
- c. The Security Officer and Callier Center Management shall be responsible for determining the need to modify a security policy or procedure in light of current threats, available solutions, costs, operation changes, or environmental changes. The Security Officer and Callier Center Management shall evaluate security policies or procedures affected by an operational change (such as an adoption of new technology) or an environmental change (such as a newly recognized risk or change in the Security Rule) to determine whether the policy or procedure should be revised to assure continued compliance with the Security Rule.
- d. If the Security Officer and Callier Center Management determine that a policy or procedure should be modified, the Security Officer shall submit proposed modifications to Facilities Manager for approval. If approved by Facilities Manager the revised policy or procedure shall be submitted to Internal Audit to determine whether the change complies with the Security Rule.

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