



# THE UNIVERSITY OF TEXAS AT DALLAS

## SECURITY OF ELECTRONIC HEALTH CARE INFORMATION

<b>Section 5.1: Access Control</b>	<b>Page:</b> 1 of 5
<b>Effective Date:</b> March 21, 2005	

### **POLICY**

UTD shall limit access to its electronic information systems that maintain protected health information (“PHI”) only to those persons or software programs that have been granted access rights. This policy applies to all computer systems, desktop systems, laptops, handheld devices, database servers, application servers, data management systems, and infrastructure devices from which electronic PHI can be accessed or upon which it is maintained. All UTD health care operations workforce personnel shall be familiar with the access control procedures of this policy.

### **PERSONNEL**

Security Officer

Privacy Officer

System Administrator

End User

Callier Center Management

Data Owner

Director-on-call

## **PROCEDURES**

### 1. Unique User Identification.

- a. *Creation.* System Administrator shall assign to each UTD workforce personnel and any other users of UTD's health care operations-related electronic information system a unique user ID to access UTD's electronic information system upon request and approval by Callier Center Management.
- b. *Temporary Access Rights.* If non-UTD employees need access to UTD's information systems to perform job functions for UTD, such as independent contractors, System Administrator shall assign temporary user ID's and passwords and their access shall be limited to only the information necessary to perform the specific function for which they have been retained.
- c. *Modifying or Terminating Access Rights.*
  - i. A user's access rights may be modified based upon a change in job function or location within the facility or employment status.
  - ii. Students may be provided temporary access (generally semester-limited) to UTD's information systems either for educational or part-time employment purposes.
  - iii. Callier Center Management shall notify System Administrator and Security Officer promptly after a change in a User's job function, location, employment or student status. System Administrator and Security Officer shall promptly modify or disable access, as applicable.
- d. *New Application or System.* Before permitting access to any newly installed application or system, System Administrator shall configure such application or system to comply with password standards, if practicable, and to require Users to input a unique user ID and password.

### 2. Password Standards.

- a. Users are responsible for keeping their user IDs and passwords confidential and are prohibited from sharing their user IDs and passwords with anyone. Users should not write down their passwords and should never transmit them in emails or other forms of electronic communication.

- b. Passwords shall contain at least seven characters and should contain a mixture of small letters, capital letters, as well as numbers and special characters.
  - c. Users shall change their passwords on a regular basis (no less than annually), and users shall not be allowed to re-use previous passwords.
  - d. Users should not use passwords that are easily guessable, such as family names, pet names, or birth dates.
3. Role-based Access. Access to UTD's electronic information systems shall be further controlled by a workforce member's role within UTD, where practicable. For members who are only allowed to access certain categories of information, UTD shall assign the access rights to these members. General Principles of Role-based Access are set out below (*see also* Section 6.2 of the Privacy Manual):
- a. *Identify Roles.* Callier Center Management and/or Data Owner(s) shall identify the members of UTD's workforce that need access to PHI, which may include individuals (e.g., a certain clinician or administrator) or groups of individuals (e.g., business office staff) that are employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UTD, subject to UTD's security policies, is under the direct control of UTD, whether or not paid by UTD. Based upon such identifications, System Administrator shall assign roles defined by Callier Center Management, Data Owner(s), and/or Security Officer. Callier Center Management, Security Officer, Director-on-call, or his or her designee shall review the roles on an annual basis and update as necessary. Callier Center Management and Data Owner(s) shall permit access to PHI only for treatment, payment or healthcare operations as defined by the Privacy Rule (Standards for Privacy of Individually Identifiable Health Information. 67 Fed. Reg. 53182-53273 (Aug. 14, 2002)).
  - b. *Identify Categories of PHI That Roles Must Access.* Callier Center Management and Data Owner(s), with the support of Security Officer and Director-on-call, shall identify and document the electronic, paper, or other forms of PHI to which each individual or group of individuals needs access consistent with their job responsibilities (roles) (collectively "Access Rights"). Callier Center Management, Data Owner(s) and Security Officer (or designees) shall review these access rights on an annual basis and update as necessary.
  - c. *Implement Role-based Access.* Based upon the assigned role of each user and that user's unique login, System Administrator shall limit the ability of the user to access only the PHI in files, database, and applications, as described in the Access Rights document issued by Callier Center Management and Data Owner(s) insofar as such capability is provided by

the computer software which provides the medical record and business functionality used by UTD's health care operations.

4. Access Configuration and Firewalls. To limit only authorized external access, System Administrator shall create and document a standard configuration for all servers that include a modem, router, or other external access device and shall not modify any server so that it no longer conforms to the standard configuration. In addition, UTD's System Administrator shall install and operate a firewall on every system with an Internet or other open network connection. Such firewalls shall block the following from accessing UTD's internal network and health care operations-related electronic information systems:
  - a. Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself (except for inbound email).
  - b. Inbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks.
  - c. Inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic.
  - d. Inbound traffic containing IP Source Routing information.
  - e. Inbound or outbound network traffic containing a source or destination address of 127.0.0.1 (localhost).
  - f. Inbound or outbound network traffic containing a source or destination address of 0.0.0.0.
  - g. Inbound or outbound traffic containing directed broadcast addresses.
  - h. Inbound traffic with a source address indicating that the packet originated on a network behind the firewall.
5. Unauthorized Devices. System Administrator shall audit by scanning the UTD network to which the workstations and servers are connected on a semi-monthly basis to verify that no unauthorized modems or other communications devices have been attached. System Administrator shall report to Callier Center Management and the Security Officer any unauthorized communications devices that System Administrator discovers, and Callier Center Management shall impose appropriate sanctions on the person(s) responsible for such unauthorized devices.
6. Remote Access Procedures. UTD shall allow users to connect remotely to the information systems in accordance with the procedures below:

- a. Dial-in access to the UTD network is not allowed.
- b. System Administrator, on request and approval of Callier Center Management, may grant remote network access, either by virtual private network, remote desktop access or other UTD-approved remote network access methodology, to Users, who shall be responsible for giving their remote access connection the same consideration and protection as users give their onsite connection. Users are responsible for any unauthorized use or for any breaches of security resulting from users' remote access capability.

7. Addressable Implementation Specifications.

- a. *Automatic<sup>[jdl1]</sup> Logoff.* System Administrator shall configure all workstations, all applications with an automatic log off capability, all remote access sessions, and any other configurable applications to terminate a session after 15 minutes without any user activity.
- b. *Encryption and Decryption.* UTD has determined that it is appropriate to implement encryption on PHI received via UTD's website. UTD shall use secure socket layer (SSL) encryption on any web page that gathers PHI.

However, UTD has determined that it is not appropriate to encrypt all PHI transmitted via open networks due to the absence of any standard in this area and the difficulty in communicating with clients, providers, payors and business associates. Security Officer shall review this determination on an annual basis to determine whether it is reasonable and appropriate to implement encryption on all transmissions containing PHI over an open network.

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