Policies of the University of North Texas Health Science Center	Chapter 14 UNT Health
I. **14.250 Electronic Protected Health Information HIPAA Compliance Policy**	

II.

Policy Statement. This policy sets forth the framework for the Institution's compliance with the Security Rule of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). It is applicable only to those units of the Institution that have been designated as "covered components" under HIPAA. This policy is limited to the final HIPAA Security Rule. Other aspects of law, including rules governing privacy and human subject research, are addressed in other Institutional policies. The Institution recognizes that adequate and appropriate security is necessary for HIPAA's privacy rules to work as intended.

Application of Policy. The HIPAA Security Policy applies to the HIPAA-covered entities at the University of North Texas Health Science Center and UNT Health.

Definitions.

1. HIPAA Security Officer. The HIPAA Security Officer is the Institutions' senior electronic Security Officer. This position is defined in the Information Security Policy.
2. HIPAA Security Rule. This rule covers security standards for certain health information specifically for safeguarding Electronic Protected Health Information (ePHI).
3. HIPAA Privacy Rule. This rule defined the standards for how protected health information should be controlled. See HIPAA Privacy Policies, including definitions.
4. Electronic Protected Health Information. ePHI includes any computer data relating to the past, present or future physical or mental health, health care treatment, or payment for health care. EPHI includes information that can identify an individual, such as name, social security number, address, date of birth, medical history or medical record number, and includes such information transmitted or maintained in electronic format, but excluding certain education and student treatment records. Not included within EPHI are student education records, including medical records (which are protected under FERPA), medical records of employees received by UNTHSC in its capacity as an employer, and workers' compensation records. Although these records are not covered under the HIPAA Privacy or Security Rules, other Institutional Policies cover the confidentiality and security of these materials. There are special provisions in the law governing the release of psychotherapy records.

III. **Procedures and Responsibilities.** HIPAA security and confidentially rule compliance.

1. Administrative Safeguards

1.1 **Risk analysis** will be performed for assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI at UNTHSC on a biannual basis or as significant changes are made to ePHI systems. This risk analysis will be presented to management and will include a documented response with remediation steps, for any identified risks.

1.2 **Information System Activity Review**. Annual reviews of information system security controls including activity records, audit logs, access reports, and security incident tracking reports will be conducted to ensure that implemented security controls are effective and that ePHI has not been compromised. Measures include user access controls, exception reports/logs, and compliance to security policies and procedures. Log information will be maintained according to the retention schedule. A periodic review of information system activity records including audit logs, access reports, and security incident tracking reports will be conducted to ensure that implemented security controls are effective.

1.3 **Information Access Management**, **Authorized Personnel and Workforce Security**. Systems that manage ePHI will have authorization controls that allow only authorized personnel access and ensure appropriate access based on authorized personnel's job role. Access to ePHI systems will require managerial approval before any person is granted access. Authorized persons' access to ePHI will be limited to the extent that access to this information achieves the requirements of the person's job responsibilities. Procedures for terminating access to ePHI from logical and physical access will be maintained. Periodical reviews of the accounts on systems managing ePHI will be conducted to ensure that only currently authorized persons have access to these systems.

1.4 **Password Management**. Passwords with no fewer than 10 characters will be required for access to ePHI. Passwords will not be shared, should not be written down and not stored in locations where they can be found, will be changed every three months, and will be changed immediately if compromised. In addition, pin numbers will also be used for logging in that are no less than six numeric characters.

1.5 **Security Awareness and Training.** Awareness and training will include periodic security updates, the University's HIPAA security training, and the campus annual information security training. Procedures and logging mechanisms will be in place for the security officer (or his/her information security delegate) to receive alerts notifying of failed log-in attempts from unauthorized users.

1.6 **Security Incident Procedures.** Procedures will be implemented to insure notification of the HIPAA Security Officer when a system managing ePHI is involved in a security incident. Incidents will be reported to the UNTHSC Compliance Officer and the Compliance Council.

1.7 **Contingency Plan.** The UNTHSC Disaster Recovery plan is in place to respond to an emergency or other occurrence

(such as fire, flood, vandalism, and unrecoverable hardware failures) that damage systems managing ePHI. Measures

that are addressed include procedures for creating and maintaining backups of ePHI to both restore data and the

systems maintaining this data, provide for adequate protection of the security of ePHI while operating in emergency

mode, and an annual campus-wide DR drill led by the campus Safety Officer.

1.8 **Evaluation.** A review to demonstrate compliance with the University's HIPAA Security Rule Policy will

be conducted periodically. Results of the review will be presented to UNT Health management which will provide a documented response, including remediation steps, for any identified gaps in compliance with the policy.

Responsible Party: HIPAA Security Officer; Privacy Officer; all clinic managers and users with access to ePHI systems

2. Physical Safeguards. Systems which manage ePHI will be kept in areas with physical security controls that restrict access.

2.1 **Facilities Access.** Servers and network equipment which manage ePHI will be kept in an isolated room with controls that prevent unauthorized access to these systems. Unauthorized persons (such as vendors, contractors, and visitors) will be escorted and monitored by an authorized person when entering and remaining in the isolated room. Access logs details of the maintenance activities, including dates and times, will be maintained.

2.2 **Workstation Use.** Only designated workstations possessing appropriate security controls will be used to access and manage ePHI, and these workstations will not be used in publicly-accessible areas nor used by multiple users not authorized to access ePHI. This security measure extends to the use of laptops and home machines. These workstations will have the following security tools installed: anti-virus software with updated virus definitions, spyware detection software with updated spyware definitions, and an automated patch management system for operating system updates.

2.3 **Workstation Security.** Physical safeguards are in place to protect workstations that access and manage ePHI, including restricted physical access, screens that are turned away from unauthorized users, and authentication with a unique user ID and password to access the workstation. The workstation will be configured with a password-protected screensaver that is evoked after five minutes of inactivity.

2.4 **Device and Media Controls.** Procedures to govern the installation, moves, and removal of hardware and electronic media that contains ePHI will be followed. Disposing of media with ePHI will use means that prevent its recovery, including erasing and overwriting media before disposal, physically destroying the media, and preventing systems that managed ePHI. Backups of ePHI will be made and retained according to the retention schedule.

2.5 **Mobile Devices**. Transferring ePHI data or information to mobile devices is strictly prohibited. This includes memory sticks, external hard drives, smartphones, or any other mobile device. Use of mobile devices with ePHI may only occur given prior, written permission from the HIPAA Security Officer and must be encrypted. Moving ePHI to a mobile device without permission or secure encryption will result in Sanctions as described in section 4 of this policy.

Responsible Party: HIPAA Security Officer; Information Technology Managers, Clinic Managers, all ePHI users

3. Technical Safeguards

3.1 **Access Control.** Security controls will be maintained to protect the integrity and confidentiality of ePHI residing on computer systems. The information security policies of the UNTHSC apply to all ePHI systems. In addition, the security features of the NextGen Electronic Medical Record (EMR) program will be fully utilized to securely manage information.

3.2 **Audit Controls.** The audit controls that are a part of the NextGen EMR will be fully implemented to allow an independent reviewer to review system activity. Audit logs will be captured on systems managing ePHI and will be securely retained for a minimum of one year using an archiving solution that allows for recovery within 24 hours upon request.

3.3 **Data Integrity**. The EMR systems and applications managing ePHI will have the capacity to maintain data integrity at all times. These capabilities include error correcting memory, disk storage with build-in error detection and correction, checksums, and encryption

3.4 **Person or Entity Authentication.** Controls will be in place that verify that a person seeking access to ePHI is the one claimed. Access to data will be controlled using username, password, and challenge and response mechanisms.

3.5 **Transmission Security.** Secure transmission mechanisms that encrypt ePHI as well as confirm that data integrity has been maintained will be used. The use of e-mail for transmitting EPHI should be avoided; if required, e-mails with ePHI should be encrypted.

Responsible Party: HIPAA Security Officer; Information Technology Managers; Managers and all users with access to ePHI

4. Sanctions

It shall be the responsibility of each covered component to implement procedures to meet the requirements of HIPAA set forth in this policy. Every employee in a covered component with access to ePHI is required to adhere to all HIPAA mandates. Violation of this policy may result in disciplinary action up to and including termination of employment. Under federal law, violation of the HIPAA privacy rule may result in civil monetary penalties of up to $250,000 per year and criminal sanctions including fines and imprisonment.

References and Cross-references.

HIPAA Privacy and Security Regulation & DHHS Regulations

HITECH Act

UNTHSC Acceptable Electronic Communications Use Policy

UNT Health HIPAA Privacy and Security Policy

UNT Health Use of Electronic Communications to Transmit Protected Health Information Policy and Procedures

UNT Health HIPAA Risk Analysis and Risk Management Policy 4.029

UNTHSC Disaster Recovery Plan

UNTHSC Records Retention Schedule

UNT Health HIPAA Risk Analysis and Risk Management

Gram-Leach Bliley Act

Senate Bill 11, Chapter 181

FERPA

Forms and Tools. (optional) Include information on any forms and/or tools required for compliance with the policy, as well as how to obtain such forms and/or tools.

Approved: January 26, 2012

Effective: January 26, 2012

Revised: June 23, 2009