Health Information Privacy Laws Compliance Procedures

Purpose

The federal Health Insurance Portability and Accountability Act and the Texas Medical Records Privacy Act, as well as the Family Educational Rights and Privacy Act (FERPA), govern how the University of North Texas institutions protect health information. This document gives an overview of HIPAA and the Texas Medical Records Privacy Act along with the procedures required to protect individual's health information.

Scope

These procedures apply to all personnel of UNT institutions within a health care component or organizations that collect, evaluate, use, store or transmit protected health information, that is not considered to be protected under FERPA.

Procedure

Overview

The Health Insurance Portability and Accountability Act, known as HIPAA, provides a basic level of privacy of an individual's health care information. Protected Health Information, or PHI, includes individually identifiable health information that a UNT institution may receive electronically, on paper or verbally. It applies to health care providers, health plans, and processors of health insurance claims. In 2009, the Federal Government expanded these protections with the Health Information Technology for Economic and Clinical Health Act (HITECH) to apply to business associates and increased the notification requirements and penalties for violations.

HIPAA Privacy Standards pertain to the protection of an individual's health information and apply to electronic, paper or verbal information. HIPAA Security Standards are rules for covered entities to protect electronic-PHI and fall into three categories: administrative safeguards, physical safeguards, and technical sageguards.

In 2011, the state of Texas added further protections with the Texas Medical Records Privacy Act. This act broadens privacy responsibilities beyond health care providers, health plan providers and insurance processors to business, individuals and organizations that collect, evaluate, use, store or transmit PHI. The Texas Privacy Act requires verified training for employees of covered entities no later than the 60th day of employment and to be completed again at least once every 2 years. Because it is more stringent than the federal HIPAA law, the requirements of the state law prevail.

The HIPAA privacy rule excludes educational records that are protected under FERPA. Therefore healthcare records of a student who receives medical care from a health clinic run by a postsecondary institution are considered educational or treatment records under FERPA, and are not subject to HIPAA or the Texas Medical Records Privacy Act. More information about the relationship between HIPAA and FERPA can be found in the UNT Protected Health Information Privacy Policy (10.7) at http://policy.unt.edu/policy/10-7.

Created: 9/5/2013
Updated: 10/21/2013

Violations of HIPAA can range from $100 per violation to $1.5 million depending on the nature and extent of the breach, harm done by exposure and other factors. Penalties cannot be imposed if the violation is corrected within 30 days and was not due to willful negligence.

The penalties for violations of the Texas Privacy Act range from $5000 each violation per year if they are due to negligence; $25,000 if they were knowingly committed; and up to $250,000 if done for financial gain.

Obligations

Anyone handling PHI protected under HIPAA must adhere to the following rules:

- Share PHI only on a need-to-know basis
- Get written authorization for use or disclosure of PHI for anything other than direct care or treatment
- Use and disclose only what is minimally necessary
- Use only authorized systems for processing, storing or entering PHI
- Securely transmit all PHI by following the UNT System Information Security Standards and Practices Guide
- Dispose of PHI securely by shredding, or rendering it unreadable
- Report lost or stolen PHI immediately to your helpdesk or Information Security group.

Under the UNT System Information Security Standards and Practices Guide, medical records, whether protected under FERPA or HIPAA, are classified as Category I information requiring a high level of security controls. Custodians and owners of medical records must follow these security controls concerning backups, change management, malware protection, physical security, system hardening, security monitoring and audit as a part of their overall information security plan. More information about these controls can be found in the UNT System Information Security Standards and Practices Guide at https://itss.untsystem.edu/sites/default/files/2012/12/Information%20Security%20Standards%20and%20Practices.pdf.

References

UNT Protected Health Information Privacy Policy: http://policy.unt.edu/policy/10-7
HSC Protected Health Information Electronic Communications Policy:
http://www.hsc.unt.edu/policies/PolicyStorePDF/PHI%20Electronic%20Communications.pdf

UNT System Information Security Standards and Practices Guide:
https://itss.untsystem.edu/sites/default/files/2012/12/Information%20Security%20Standards%20and%20Practices.pdf.

Public Law 104-191: http://aspe.hhs.gov/admnsimp/pl104191.htm

Overview of the HIPAA Final Privacy Regulations: http://healthcare.partners.org/phsirb/hipaaov.htm

Created: 9/5/2013
Updated: 10/21/2013

Texas Medical Records Privacy Act:

https://www.oag.state.tx.us/consumer/hipaa.shtml

http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.181.htm

Contact Information

For more information, refer to the above websites or contact security@untsystem.edu.

Created: 9/5/2013
Updated: 10/21/2013