Policies of the University of North Texas Health Science Center	Chapter 14 UNT Health
I. **14.221 Mitigating Violations of HIPAA Security and Privacy-Related Policy and Procedures**	

II.

Policy Statement

UNTHSC will mitigate, to the extent practicable, any harmful effects that are known to it, which arise out of inappropriate or unauthorized access, use and/or disclosure of Protected Health Information (PHI) in violation of UNTHSC security or privacy-related policies or in violation of HIPAA, by either members of its workforce or its business associates.

Application of Policy

All UNTHSC providers, employees, and business associates.

Definitions

1. Business Associates: "Business Associates" means a vendor or individual under contract with UNTHSC who either creates or receives PHI on behalf of UNTHSC.

2. Protected Health Information (PHI): is individually identifiable health information that is transmitted or maintained in any form or medium, including oral, written, and electronic.

3. Workforce member: means employees, volunteers, trainees and other persons whose conduct, in the performance of work for UNTHSC, is under the direct control of UNTHSC, whether or not they are paid for by UNTHSC.

4. Electronic Communication Resources: includes telecommunications equipment, electronic audio/video devices, encoding/decoding devices, computers, servers, data processing or storage systems, mobile communication devices, networks, input/output and connecting devices and related programs, software and documentation that support electronic communications. UNTHSC electronic communication resources include institutional and departmental information systems, faculty research systems, desktop computers, UNTHSC campus networks and general access computer systems.

Procedures and Responsibilities

5. All suspected violations of UNTHSC security or privacy-related policies or of HIPAA requirements by a workforce member or by a business associate should be reported by calling the UNTHSC Ethics Hotline (1-877-606-9187), or reporting to the UNTHSC Privacy Officer (example: complaints about patient privacy), the UNTHSC Security Officer (example: complaints regarding inappropriate access to network) and/or the UNTHSC Institutional Compliance Officer.

Responsible Party: UNTHSC providers, employees and business associates

1. In situations where an electronic communication resource was inappropriately or without proper authorization accessed, used or disclosed, the UNTHSC Security Officer must be immediately notified. An example may be a lost/stolen computer, USB drive, etc.

I. Responsible Party: UNTHSC providers, employees and business associates

1. Upon receiving a report of suspected violations of UNTHSC security or privacy-related policies or of HIPAA requirements by a workforce member or by a business associate, the Privacy Officer and/or the Security Officer:

a. Will conduct an investigation of the reported violation and, as part of that investigation:

i. Will consult with legal counsel as necessary;

ii. Will review all related Security and Privacy Policies and HIPAA regulations; and

iii. Will thoroughly document all actions taken and any resulting harmful effects of which he or she knows;

b. Will develop a corrective action plan to mitigate any resulting harmful effects. Such plan will be promptly communicated to all affected employees as appropriate; and

c. Will maintain the documentation for six years.

Responsible Party: UNTHSC Privacy Officer and/or UNTHSC Security Officer as appropriate; UNTHSC Institutional Compliance Officer

1. After completion of investigation into the reported violation, a determination of the appropriate corrective, remedial or disciplinary action will be made based on the specific facts and circumstances of each case. Performance management, training and/or disciplinary action up to and including termination will be taken on a fair and equitable basis.

I. Responsible Party: UNTHSC Privacy Officer and/or UNTHSC Security Officer as appropriate, Directors of Clinical Operations

1. In the event UNTHSC determines a fax has been inappropriately sent, the following mitigation efforts must be taken:

a. A phone call, (supplemented by a note referencing the conversation) should be made to the recipient of the misdirected fax requesting that the entire content of the misdirected fax be destroyed or returned to UNTHSC and obtain a written confirmation of the destruction of the fax. If the recipient cannot be reached by phone, a fax should be sent to the recipient requesting that the entire content of the misdirected fax be destroyed;

b. Correct fax directories or pre-programmed numbers that contain incorrect fax

numbers.

c. If a fax transmission is not received by the intended recipient because of a misdial, the internal logging system of the fax machine must be checked to obtain the misdialed number;

d. It is the responsibility of the clinic/department sending the misdirected fax to forward the following information to the HIM manager:

i. Fax confirmation sheet; and

ii. Supplemental documentation outlining the course of action.

II. Responsible Party: UNTHSC employees

1. For paper documents and electronic medical records containing PHI which are accessed, used, and/or disclosed inappropriately without authorization, the following actions must be taken:

a. If the incorrect PHI is given to a patient, UNTHSC must make attempts to retrieve the PHI or request that the PHI be destroyed. Documentation supporting the attempts to retrieve the PHI and the action steps taken must be included as part of the documentation.

b. Efforts must be made to account for documents containing PHI left unattended or visible after hours and steps must be taken to ensure a process is in place to prevent any occurrence in the future.

c. UNTHSC must make every effort to locate documents containing PHI that are lost or stolen.

III. Responsible Party: UNTHSC Privacy Officer and UNTHSC employees

1. In situations involving individuals displaying inappropriate behavior which may jeopardize a patient's privacy, workforce members must inform the individual(s) that their behavior is not permitted and the workforce member must notify their supervisor immediately. If warranted, the UNTHSC Privacy Officer should be notified.

IV. Responsible Party: UNTHSC employees

1. In the event the situation meets the definition of a HITECH breach, notification to the patient(s), the Department of Health and Human Services, and if applicable, the media, will be made in accordance with HHS Breach Notification Protocol.

V. Responsible Party: UNTHSC Privacy Officer, UNTHSC Security Officer and UNTHSC Institutional Compliance Officer

References and Cross-references

45 CFR Parts 160 and 164: Breach Notification for Unsecured Protected Health Information

Forms and Tools

Approved: January 26, 2012

Effective: January 26, 2012

Revised: October 11, 2012