



TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

Operating Policy and Procedure

HSC OP: 52.05, **HIPAA; Electronic Transmission of Protected Health Information (PHI)**

PURPOSE: The purpose of this Health Sciences Center Operating Policy and Procedure (HSC OP) is to provide a framework to allow electronic Protected Health Information (EPHI) to be securely transmitted over electronic communication networks such as e-mail and the internet.

REVIEW: This HSC OP will be reviewed on May 1 of each even-numbered year (ENY) by the HIPAA Privacy and Security Committee, with recommendations for revisions forwarded to the Institutional Compliance Officer, the Institutional Chief Information Officer, and the Executive Vice President for Finance and Administration by June 15.

POLICY/PROCEDURE:

1. Definitions.

- a. Electronic PHI (EPHI)** is defined in HSC OP 52.02, as individually identifiable health information that is transmitted by electronic media (internet, extranet, leased lines, dial-up lines, private networks, flash drives, CD, etc.) or maintained in electronic media (hard drives, magnetic tape/disk, CD, digital memory card, etc.)
- b. TTUHSC Exchange e-mail** is the Microsoft based e-mail system supported by Texas Tech University Health Sciences Center. The primary client software for Exchange email is Outlook and Outlook Web Access. All e-mails ending in "ttuhsc.edu" are routed through TTUHSC Exchange email services.

2. Secure Transmission of PHI through Electronic Means

The Health Insurance Portability and Accountability Act (HIPAA) Security Standard (45 CFR 164.312(e)(1)) requires TTUHSC to "implement security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network". As such, TTUHSC is required to "implement a mechanism to encrypt electronic protected health information whenever deemed appropriate¹."

Where other secure means of transmission are available (fax, electronic shared secure files) transmission of EPHI through e-mail or the internet shall be limited. EPHI shall only be transmitted or received over electronic communication networks as outlined in the procedures below.

3. Transmission of EPHI through TTUHSC Internal E-Mails.

TTUHSC has multiple security strategies in place to protect e-mails transmitted through the TTUHSC Exchange email system from unauthorized access from outside the TTUHSC system. PHI transmitted through the TTUHSC Exchange email service, where the sender and recipients' e-mail addresses (including "cc" and blind copies) all end in "ttuhsc.edu", does not need to be encrypted. If any sender or recipient's e-mail address does not end in "ttuhsc.edu", then the EPHI must be encrypted as outlined in paragraph 4 below.

4. Transmission of EPHI through External E-Mails.

Any e-mail containing EPHI (either within the body of the message or as an attachment) that is sent from and/or to a **non-TTUHSC** email address (i.e., IT DOES NOT END IN "ttuhsc.edu") **must**

¹ 42 CFR 164.312(e)(2)(ii)

be encrypted.

- a. **Manual Encryption.** TTUHSC currently has a manual encryption system in place to secure EPHI that is e-mailed outside the TTUHSC Outlook Webmail system. EPHI e-mailed outside the TTUHSC Outlook Webmail system (one or more e-mail addresses do not end in "ttuhsc.edu") **must** be manually encrypted. To manually encrypt e-mail, one of the following designations **MUST BE TYPED INTO THE SUBJECT LINE** of the e-mail to be encrypted:

- [ss]; or
- [send secure]

E-mail will not be encrypted if one of these bracketed designations is not manually typed into the subject line of the e-mail. A subject title can be added after either of these designations.

Example: [ss] Medical Records

- b. **Automatic Encryption.** TTUHSC is currently developing an automatic encryption process. This policy will be updated once the automatic encryption process is available.

5. **Transmission of EPHI through the Internet**

EPHI transmitted through the Internet **must** be encrypted or otherwise secure. Any Department and/or School that desires to use the internet to transmit and/or receive EPHI is responsible for obtaining written approval from the TTUHSC Privacy Officer and TTUHSC Security Officer confirming that the information is adequately encrypted or otherwise secure.

6. **Education & Training**

Information and education regarding electronic transmission of PHI shall be provided through various sources, including, but not limited to the TTUHSC website, live training and published notices. TTUHSC Information Technology Division shall have information regarding e-mailing of PHI posted at: <http://www.ttuhsc.edu/it/helpdesk/emailencryption.aspx>

7. **Response to Non-Compliance**

Violations of this policy shall be investigated and addressed by the TTUHSC Privacy Officer and/or Security Officer and reported to the HIPAA Committee, which may recommend additional corrective action.

8. **Right to Change Policy**

TTUHSC reserves the right to interpret, change, modify, amend or rescind this policy in whole or in part at any time without consent of employees.