Texas Tech University Health Sciences Center
HIPAA Privacy Policies

Use, Disclosure and Disposal of PHI	**Policy 4.2**
Texting of Protected Health Information	**Effective Date: June 25, 2016**
References: http://www.hhs.gov/ocr/hipaa HSC HIPAA website http://www.ttuhsc.edu/hipaa/policies_procedures.aspx	

Policy Statement The purpose of this Health Sciences Center HIPAA Policy and Procedure (HSC OP) is to define accepted practices, responsibilities and procedures for the transmission of PHI via secure text messaging between clinic providers and staff. Text messaging is a form of informal communication that can be beneficial if used appropriately.

Scope and Distribution

This policy applies to all health care clinical service areas owned and/or operated by TTUHSC.

Definitions

Refer to HPP 1.1 for Glossary of HIPAA Terms

See *Old/New HIPAA Policy Number Cross Reference Chart*

Procedure

1. Eligibility

   A. Cortext (Imprivata) is the only secure text messaging platform approved for use by TTUHSC health care professionals. Other text messaging platforms, e.g., TigerText will not be used.

   B. Cortext is available by contacting the Information Technology (IT) Department at each respective campus or calling the Lubbock IT Help Desk at 806-743-1234.

   C. TTUHSC faculty, staff, and students can use a smart phone, TTUHSC managed computer workstation or device, or a personal mobile device to access the secure messaging solution.

2. Scope of Use

   A. All messages that reference a patient should include two patient identifiers in order to confirm patient identity.

   B. It is HSC's policy **not** to allow secure texting as a method to communicate patient orders.

C. Text messages are not stored as part of the medical record. Text messages are automatically deleted after 7 days and archived for 30 days.

3. Ownership

A. All data transmitted via Cortext is the sole property of TTUHSC. TTUHSC has absolute right of access to all of the data sent via secure texting and may exercise its right whenever it is deemed appropriate.

B. Audits by the Office of Institutional Compliance or Information Technology-Security Division may be conducted as needed to determine compliance with TTUHSC policy guidelines.

4. Security

A. Refer to TTUHSC IT Policy 56.01, Use of Information Technology Resources for additional guidelines on mobile device security.

B. Users of mobile devices are responsible for physical security of these devices both onsite and offsite. In the event a mobile device becomes lost or stolen, either personal or TTUHSC owned, the responsible TTUHSC faculty, staff or student shall report the incident immediately to his/her supervisor, the TTUHSC Privacy Officer (IPO), and the TTUHSC Information Security Officer (ISO).

C. Refer to TTUHSC IT Policy 1.4.1 that users should never share logins, passwords, or other security measures and should not disable or alter any security measures configured on a mobile device.

5. Right to Change Policy

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

This policy and procedure will be documented and retained for a period of 6 years from the date of its creation or the date when it last was in effect, whichever is later.

Knowledge of a violation or potential violation of this policy must be reported directly to a Regional Privacy Officer, the Institutional Privacy Officer or to the employee Compliance Hotline at (866) 294-9352 or Ethics Point - Texas Tech University under HSC.

Approval Authority

The TTUHSC Privacy and Security Committee has authority for HIPAA policy approval.

Responsibility and Revisions

Questions regarding this policy may be addressed to the Regional Privacy Officer (Amarillo, Permian Basin Lubbock), the Institutional Privacy Officer, or the Institutional Compliance Officer.