Secure Text Message Policy

Policy #: TC-ITS-230 **Approved By**: Paul Hopingardner, County Executive, Technology & Operations
Version #: 1.4 **Effective Date**: May 30, 2015

Accountability & Responsibility

This policy is governed by the accountability and responsibility section found here.

Purpose

The purpose is to ensure that the risk associated with text messaging sensitive information is managed appropriately to safeguard both the privacy and security of the information exchanged. Under the HIPAA Security Rule (164.308 (a) (1) (ii) (A) and (B)), text messaging is addressed as part of Travis County's comprehensive risk analysis and management strategy. Based on the risk analysis, Travis County must determine the appropriate administrative, physical, and technical controls to mitigate the risk of text messaging electronic protected health information (ePHI, PII, CJI).

The policy applies to company-owned and personal mobile computing devices capable of transmitting text messages. Further, the policy applies to the network, systems, and applications that process, store, maintain, or transmit corporate data.

Policy

It is the policy of Travis County to implement reasonable safeguards while sending text messages containing ePHI, PII, or CJI using cell phones, smartphones, and other computing equipment.

1. Text messages are electronic communications sent with a mobile device or computer system. Text messages can transmit both photos and written word formats of communication. If the content of such a message contains electronic protected health information (ePHI), then the text message must comply with HIPAA requirements.
2. All text messages that contain ePHI, PII, or CJI must be limited to the minimum information necessary for the permitted purpose.
3. Travis County recommends that all text messages containing patient information be transmitted in a secure and encrypted format.
4. The following requirements must be met when protected health information is transmitted, stored, or processed through a text messaging platform:
    a. Do NOT send text messages containing protected health information unless the text message is encrypted both in transit and at rest using an encryption application.
    b. The text message must be communicated from the sending device through the mobile provider or a software application to the recipient's device in an encrypted manner.
    c. The encrypted text message should not be decrypted and stored on the cellular provider's systems in ways that can be accessed by unauthorized personnel. An example of this would be taking screen shots of the messages and saving images to your device.
5. If any individual defined in the Scope wishes to send protected health information through text message to another individual as defined in the Scope, both the Sender(s) AND the Receiver(s) must fulfill both the encryption requirements listed above (encryption of the message in transit and at rest).
6. All individuals defined in the Scope who wish to send OR receive text messages containing ePHI must register any device capable of sending text messages with the ITS Security Team for approval per the following requirements:
    a. The individual defined in the Scope MUST submit their mobile device number to the ITS Service Desk or to the ITS Security Team. This step ensures that Travis County takes proper inventories of all mobile devices sending or receiving protected health information. The IT Security Team can be reached at ITS-Security-Group@traviscountytx.gov.
    b. Mobile devices used to text electronic protected health information MUST be properly sanitized upon retirement of the device. The Travis County IT department securely wipes all mobile devices upon return to the ITS Department. If a workforce member is using a personal device, they MUST contact the ITS Department to securely wipe the device prior to returning the device to their cellular provider.
7. The following safeguards must be implemented by both the Sender(s) AND the Receiver(s):
    a. The mobile device MUST be password protected; this feature must never be disabled.

   b. The mobile device MUST be configured to lock automatically after a period of inactivity (not to exceed 10 minutes).
   c. All text messages containing protected health information should be limited to the minimum information necessary for the permitted purpose. Multiple identifying factors (such as full name, date of birth, medical record number, social security number, or condition-specific information) should not be used.
8. The following guidelines MUST be followed when texting protected health information. Ensure the accuracy of the information being texted by administering the following precautions:
   a. Obtain written authorization from client or designee for electronic text communication.
   b. Do not use shorthand or abbreviations.
   c. Review texts prior to sending to ensure accuracy. Beware of autocorrect functions.
   d. Do NOT text patient orders.
   e. ALL text messages (or annotations of text messages) that are used for clinical decision making must be documented in the medical record.
   f. Delete all text messages containing protected health information on a frequent basis.
9. Report all lost or stolen mobile devices to the ITS Service Desk.
10. Report all unencrypted text messages that are received or sent out that contain any patient information to the ITS Service Desk or the ITS Security Team (ITS-Security-Group@traviscountytx.gov). Report all text messages that are sent to the wrong individual to the Services Desk or the ITS Security Team (ITS-Security-Group@traviscountytx.gov).

Policy Revision

Version	Purpose/Changes	Editor	Date
1.0	Travis County Information Technology Services Information Security Policies Creation	Randy Lott	05/30/2015
1.1	Removed HIPAA from title. Added 8a. for written authorization. Changed wording in Item #3 from requires to recommends.	ITS Policy Committee	11/13/2015
1.2	Deleted #8b & 8c from policy. (Confirm the recipient of your text. Confirm delivery and receipt of the text. A confirmation receipt that the information was received is ideal.)	ITS Policy Committee	09/28/2016
1.3	Updated name of CIO	Randy Lott	12/18/2017
1.4	Updated policy number from 123 to 230 and updated approver's title.	Joyce Miller	11/20/2019