Uses and Disclosures of PHI

Policy # 2.8

Safeguarding PHI: Use and Storage

Original Effective Date: 6/21/2016

Revised Date: 3/22/20022

Purpose: To provide a policy and standards for the safeguarding of PHI by workforce members.

Policy: Travis County**, to the extent possible**, implements measures to safeguard against the inappropriate disclosure of PHI.

Process:

Administrative Safeguards

1. The HIPAA Compliance and Privacy Officer will implement policies and procedures to prevent, detect, contain, and correct violations of the HIPAA Privacy Rule.

2. The HIPAA Compliance and Privacy Officer will periodically review these policies and procedures and will conduct evaluations of each Covered Component's compliance with these policies and procedures.

Physical Safeguards

Covered components ensure that reasonable physical safeguards are in place to ensure the privacy of PHI. For example, in County facilities where conversations involving PHI regularly occur, office spaces and cubicles should be located in areas that limit the ability of unauthorized persons to access PHI. Whenever possible, unauthorized persons are not allowed into areas where PHI is used or stored.

Physical Safeguards for Conversations

1. In County departments in which conservations, whether face-to-face, by telephone, or Remote Home Environments involve PHI, conversations are conducted:
    - In a private office; or
    - if no private office is available, in a non-public area where no other workforce members are present; or
    - if a public area cannot be avoided, only after unauthorized workforce members are asked to vacate the area and noise cancelling devices, fans, or other noise distorting equipment have been previously installed; or
    - using lowered voices to minimize the possibility that unauthorized persons may overhear a conversation; and
    - without excessive use of the Individual's name.
2. Workforce members should not leave a detailed message on an individual's answering machine or an individual's voice mail without an individual's consent. Only a generic message, **containing as little PHI as possible**, should be left.

Physical Safeguards for Printers, Copiers, and Fax Machines

1. In County departments or Remote Home Environments in which PHI is printed, copied, or faxed, the machines that perform these functions will be:
    - located in areas that are not easily accessible to unauthorized persons;
    - placed behind locked doors; and
    - if placement behind locked doors is not possible, have PIN controlled access capabilities.

2. Moreover, workforce members will:
    - promptly remove documents containing PHI from the printer, copier or fax machine;
    - mark all pages of an outgoing fax containing PHI as **"CONFIDENTIAL"**;
    - attach a facsimile cover sheet to an outgoing fax that:
        - informs the recipient of the fax that the information in the fax is confidential,
        - identifies the proper recipient, and
        - directs any other person who receives the fax to notify the sender of the error;
    - program frequently used numbers into the fax machine;
    - periodically check numbers programmed into the fax machine for accuracy;
    - verify the accuracy of new fax numbers before faxing PHI;
    - review fax confirmation sheets to determine whether the intended destination matches the number on the confirmation; and
    - promptly inform the HIPAA Compliance and Privacy Officer of any misdirected faxes. Workforce members may contact any unintended recipient of a fax to instruct the recipient to destroy the misdirected fax.

Physical Safeguards for PHI Maintained in Hard Copy Format

1. In County departments in which PHI is maintained in hard copy form, workforce members will:
    - clean desks and working areas such that all PHI is properly secured;
    - place documents containing PHI in a
        - locked file,
        - locked drawer,
        - locked room, or
        - safe;
    - Shred documents containing PHI or place the documents in secured shred bins for Travis County contractors to shred.
    - **Keep documents containing PHI at the office** (i.e., will not transport hard copies of PHI offsite.) Should the workforce member need to transport documents offsite, paper copies of PHI are not to be left unattended in vehicles or in alternate worksites.

Technical Safeguards

1. Workforce members under the authority of the Commissioners Court abide by the policies and procedures set forth in the Travis County Security Policies, which can be accessed on Travis Central under the ITS Security link, or by contacting the Security Officer. Workforce members pay particular attention to policies related to the use of county computers and the transmission of sensitive data.

2. Workforce members under the authority of a non-Commissioners Court Elected or Appointed officials abide by the Information Security Policies and Procedures adopted by the particular Elected or Appointed Official, where that Elected or Appointed Official has not adopted the policies and procedures set forth by the Chief Information Officer.

3. When transmitting PHI (such as when responding to an individual's request for PHI by mailing a requested flash drive), workforce members use reasonable and appropriate safeguards based on the method of transmission to ensure that unauthorized individuals will not be able to access such PHI. If an Individual emails a Workforce Member about an issue involving PHI, such Workforce Member should ask whether to **encrypt** the reply email and describe the risks of not encrypting an emailed communication.

In addition, workforce members acting on behalf of Travis County or any of its Covered Components take all reasonable precautions to safeguard PHI from all intentional and unintentional uses or disclosures in violation of the privacy rule, including storing electronic files (ePHI) securely. Workforce members ***DO NOT*** store files on local drives. Workforce Members will **NOT** use personal emails, texts, phones, software, hardware, computers, or any other device or mechanism ***NOT AUTHORIZED*** by Travis County to receive, send, transmit, store, or disclose PHI. Files containing PHI (ePHI) are stored on ***AUTHORIZED*** Servers and Travis County devices.