Privacy Administration

Policy # 1.4

Mitigation of Harm Resulting from Impermissible Use or Disclosure of PHI

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To establish a process to appropriately mitigate any potential harm to individuals due to possible exposure and/or disclosure of PHI.

Policy: Travis County mitigates, **to the extent possible**, any harmful effects of a violation of these HIPAA Policies/PHI Regulations or the ITS Security Policies or State or Federal Laws concerning the unauthorized access, acquisition, use or disclosure of PHI by workforce members or business associates.

Process:

1. The policy entitled Reporting, Investigating, and Documenting Suspected PHI Breach outlines the policy and process for determining whether-or-not a breach of PHI has occurred.

2. If the HIPAA Compliance and Privacy Office has determined that a breach of PHI has occurred, the HIPAA Compliance and Privacy Officer, in consultation with Legal Counsel, evaluates whether any damage has occurred, the extent of any damage that has occurred, and what actions should be taken to mitigate any damage. This includes an evaluation of applicable State and Federal statutes and regulations. The recommendations related to the actions that should be taken to mitigate any damage will be based on at least the following factors:
    - knowledge of where the information has been disclosed; and
    - how the information might be used to cause harm to the patient or another individual; and
    - what steps can actually have a mitigating effect under the facts and circumstances of any specific situation

3. The HIPAA Compliance and Privacy Officer and/or the Security Officer will review policies applicable to the suspected breach and evaluate whether there are ways to improve policies where necessary.

4. The HIPAA Compliance and Privacy Officer reports to the County Executive, Department Head, Elected/Appointed Official or their designee responsible for programs in which a breach is reported, the nature and any consequences of actual breaches of PHI. The HIPAA Compliance and Privacy and/or Security Officer may recommend possible operational improvements to prevent recurrence of any breach. The HIPAA Compliance and Privacy Officer reports, **in aggregate**, small and low-risk breaches to the County Risk Manager on a periodic basis. The HIPAA Compliance and Privacy Officer reports breaches of over **500** records to the County Risk Manager.

5. The HIPAA Compliance and Privacy Officer uses their **professional judgement** to determine whether circumstances warrant informing the Commissioners Court, or the HIPAA Compliance and Privacy Officer's Court subcommittee of a breach or violation. The HIPAA Compliance and Privacy Officer always informs the Court of suspected breaches involving more than **500** records. To inform the Court, the HIPAA Compliance and Privacy Officer issues a memo with information pertaining to the breach or violation and any actions the Officer believes are necessary to mitigate the breach. The Court may direct that certain action be taken to mitigate the risk.

6. If any circumstance prevents the Commissioners Court from taking action before the end of the time in which the County must provide individuals with notice, or if an immediate action is required to mitigate risk, the County Executive to whom the HIPAA Compliance and Privacy Officer reports has the authority to act on behalf of the County to mitigate risks associated with the breach.

The HIPAA Compliance and Privacy Officer and/or the Security Officer review policies applicable to the suspected breach and evaluate whether there are ways to improve policies.