Privacy Administration

Policy # 1.3

Reporting, Investigating, & Documenting Suspected Breaches of PHI

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To provide a process by which to conduct a thorough investigation of any reported acquisition, access, use or disclosure of PHI that is not authorized by HIPAA (a breach or a potential breach).

Policy: Suspected breaches are treated as a priority by workforce members and other involved parties. Workforce members who suspect a breach of PHI must report this information immediately. Travis County investigates any suspected breaches of PHI of which it becomes aware.

Breaches are treated as "discovered" on the first "Date of Discovery" any workforce member in the covered component becomes aware of the breach OR the first "Date of Discovery" a workforce member would have been aware of a breach by exercising reasonable diligence, whichever is earlier.

Process:

Reports of Suspected Breaches of PHI:

1. Workforce members who suspect a breach must ***immediately*** report this information to the appropriate management personnel, as described in the table below. Workforce members should provide as much information as possible about suspected breach including, but not limited to:

    a) **Date of Discovery**
    b) **Discovered by who**
    c) **How it was discovered**
    d) **Employee(s) Involved – Any contact information**
    e) **Devices used and any associated numbers attached to devices**
    f) **Description of Incident – Detailed as possible**
    g) **Has employee been questioned by the appropriate staff (Security/HIPAA Compliance and Privacy)**

POTENTIAL BREACH	REPORT TO
Suspected virus, spyware, and other intrusions	➢ **ITS Service Desk at Extension = Internally: 4-9175** **1. (Externally: 512-854-9175)** • ***For after-hours calls, follow the prompts to report the incident as "critical."*** ➢ **STARFlight: *Workforce members report directly to command staff, who then liaise with ITS. After hours, command staff should be paged to notify of incidents.***
Violations, or suspected violations, of access to confidential information and/or PHI	**1. ITS Service Desk at Extension = Internally: 4-9175** • **(Externally: 512-854-9175)** • ***For after-hours calls, follow the prompts to report the incident as "critical."*** ***2. AND Department Privacy Liaison or HIPAA Compliance and Privacy Officer*** ➢ **STARFlight: *Workforce members should notify STARFlight command staff of issues requiring immediate attention after hours.***
Loss or theft of computer equipment, mobile device, or tablets	➢ ***Immediate:* ITS Service Desk at Extension = Internally: 4-9175** • **(Externally: 512-854-9175)** • ***For after-hours calls, follow the prompts to report the incident as "critical."*** ➢ **STARFlight: *Workforce members report directly to command staff, who may enact security counter- measures and liaise with ITS. After hours, command staff should be paged to notify of incidents.*** **1. Then:** • **Supervisor(s)** • **Department Privacy liaison for non- Commissioners Court Departments** • **HIPAA Compliance and Privacy Officer for Commissioners Court Departments**
An event or incident that the workforce member is unsure of where to report	➢ ***Non-Commissioners Court Departments:*** **1. Supervisor and Department Privacy Liaison** ➢ **Commissioners Court Department:** **1. Supervisor and HIPAA Compliance and Privacy Officer**

1. Reporting a suspected breach can be made by phone, or email (privacy@traviscountytx.gov). Please keep in mind the severity of data disclosures. **It always recommended to speak to someone directly**.

2. Managers, Privacy Liaisons, and IT personnel who receive reports of suspected breaches must ***immediately*** inform the HIPAA Compliance and Privacy Office **(512-854-1114)**. Appropriate department IT/Security personnel should also be notified of any suspected breaches by the HIPAA Compliance and Privacy Office and workforce members.

3. The HIPAA Compliance and Privacy Office is responsible for ensuring timely checking of voice and email messages and will confirm receipt of reports with the workforce member.

Investigation of Suspected Breaches of PHI

1. The HIPAA Compliance and Privacy Officer informs the County Executive or Department Head responsible for covered components in which a breach is reported of any investigations of suspected breaches of PHI unless circumstances suggest that this action would adversely impact the investigation. The HIPAA Compliance and Privacy Officer uses their discretion at any point during the investigation about whether-or-not the Commissioners Court or sub-committee of the Commissioners Court should receive information pertaining to the potential breach or investigative process. Court or sub-committee of the Commissioners Court should receive information pertaining to the potential breach or investigative process.

2. The HIPAA Compliance and Privacy Officer or Privacy Liaison investigates the potential breach. The HIPAA Compliance and Privacy Officer is responsible for investigations in non-Commissioners Court Departments. The HIPAA Compliance and Privacy Officer coordinates with the Security Officer and will, in conjunction with the Security Officer and workforce members within the affected covered components, gather all relevant information related to the suspected breach.

3. Workforce members requested to provide information pursuant to a breach investigation must fully cooperate with the person making such requests and provide information within the timelines requested by the HIPAA Compliance and Privacy Officer **and/or** Security Officer.

4. The HIPAA Compliance and Privacy Officer ensures that all investigations are completed as soon as possible; and no later than sixty **(60)** days after discovery of the suspected breach for Commissioners Court Departments unless circumstances absolutely do not permit this deadline to be met. The sixty **(60)** day timeline begins from the **earlier of the first day a suspected breach is discovered** or **the first day a workforce member would have been aware of the breach by exercising reasonable diligence**.

Documentation and Determination of Breaches

1. The Security Officer reports technical information and conclusions to the HIPAA Compliance and Privacy Officer as soon as enough technical information is available for the HIPAA Compliance and Privacy Officer to determine if a breach has actually occurred.

2. The Privacy Officer documents all facts collected in the investigation in an internal report. The Security Officer provides a signed attestation of technical information and conclusions to the HIPAA Compliance and Privacy Officer for inclusion in that report. Draft documents and findings are provided to Legal

Counsel for review.

3. The HIPAA Compliance and Privacy Officer reviews relevant information and, in consultation with Legal Counsel, **as necessary**, determines whether-or-not a breach has occurred. A breach is presumed to have occurred in all cases where the risk of compromise to PHI is greater than low, as based on the following risk factors:
    a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification (e.g., social security numbers, financial data, clinical detail, diagnosis, treatment, medications).
    b) The unauthorized person who used the PHI or to whom the disclosure was made.
    c) Whether the PHI was actually acquired or viewed.
    d) The extent to which the risk to the PHI has been mitigated.

4. If the incident is determined to be a violation, **but not a breach**, the HIPAA Compliance and Privacy Officer will appropriately document the violation and recommend any Corrective/Disciplinary Actions to prevent similar occurrences in the future.

5. If the incident is determined to be a breach, the HIPAA Compliance and the Privacy Officer and the Security Officer follow procedures in the policy entitled Mitigation of Harm Resulting from Impermissible Use or Disclosure of PHI /PII. The HIPAA Compliance and Privacy Officer maintains a log of all breaches. The Log contains the following information with respect to each breach:
    a) A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of victims/records affected, if known.
    b) A description of the types of unsecured PHI that were involved in the breach (such as full name, social security number, date of birth, home address, account number, etc...).
    c) A description of the action taken in-regards-to notification of patients regarding the breach.
    d) Steps taken to mitigate the breach and prevent future occurrences.

6. The HIPAA Compliance and Privacy Officer informs all appropriate parties of his or her determination whether a breach has occurred or not. The HIPAA Compliance and Privacy Officer, in consultation with the Risk Manager, Legal counsel, Security Officer, and other appropriate parties, **as necessary**, will recommend Corrective/Disciplinary Actions to help prevent future recurrences.

7. The HIPAA Compliance and Privacy Officer reports any violations or breaches that involve business associates to the Purchasing Agent and to the Department.