



Privacy Administration

Policy # 1.3

Reporting, Investigating, & Documenting Suspected Breaches of PHI

Original Effective Date: 6/21/2016

Revised Date: 5/19/2017

Purpose: 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 day any workforce member in the covered component becomes aware of the breach **OR**, the first day 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:

Table 1: reporting suspected breaches of PHI

POTENTIAL BREACH	REPORT TO
Suspected virus, spyware, and other intrusions	ITS Service Desk at Extension 49175 <i>For after-hours calls, follow the prompts to report the incident as “critical.”</i> 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	Non-Commissioners Court Departments: Department Privacy Liaison Commissioners Court Department: Privacy Officer

	<p>STARFlight crews should notify STARFlight command staff of issues requiring immediate attention after hours.</p>
<p>Loss or theft of computer equipment, mobile device, or tablets</p>	<p>Immediate: ITS Service Desk at Extension 49175 <i>For after-hours calls, follow the prompts to report the incident as “critical.”</i></p> <p>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.</p> <p>Then:</p> <ul style="list-style-type: none"> • Supervisor(s) • Department Privacy liaison for non-Commissioners Court Departments • Privacy Officer for Commissioners Court Departments
<p>An event or incident that the workforce member is unsure of where to report</p>	<p>Non-Commissioners Court Departments: Supervisor or Department Privacy Liaison</p> <p>Commissioners Court Department: Supervisor and/or Privacy Officer</p>

1. All reports must first be made by phone. Workforce members must leave voicemails and may follow up with email communications.
2. Managers, Privacy Liaisons, and IT personnel who receive reports of suspected breaches must immediately inform the Privacy Officer of any suspected breach. Appropriate department IT personnel should also be notified of any suspected breaches by the Privacy Officer, workforce members (such as IT personnel).
3. The Privacy Officer is responsible for ensuring timely checking of messages and will confirm receipt of reports with the workforce member.

Investigation of suspected breaches of PHI

1. The 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 Privacy Officer uses his or her 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.

2. The Privacy Officer or Privacy Liaison investigates the potential breach. Although the Privacy Liaison is responsible for investigations in non-Commissioners Court Departments, the Liaison may request assistance from the Privacy Officer or Security Officer at any time. The Privacy Officer or Privacy Liaison 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 Privacy Officer, Security Officer, or Privacy Liaison.
4. The Privacy Officer ensures that all investigations are completed as soon as possible; and no later than 30 days after discovery of the suspected breach for Commissioners Court Departments unless circumstances absolutely do not permit this deadline to be met. The 30 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 Privacy Officer as soon as enough technical information is available for the 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 Privacy Officer for inclusion in that report. Draft documents and findings are provided to Legal Counsel for review.
3. The 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 Privacy Officer will appropriately document the violation and recommend any corrective actions to prevent similar occurrences in the future.
5. If the incident is determined to be a breach, the Privacy Officer and the Security Officer follow procedures in the policy entitled [Mitigation of Harm Resulting from PHI Breaches](#). The Privacy Officer

maintains a log of all breaches. The log contains the following information with respect to each breach:

- A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
 - A description of the types of unsecured protected health information that were involved in the breach (such as full name, social security number, date of birth, home address, account number, other).
 - A description of the action taken with regard to notification of patients regarding the breach.
 - Steps taken to mitigate the breach and prevent future occurrences.
6. The Privacy Officer informs all appropriate parties of his or her determination in the event a breach has occurred. The Privacy Officer, in consultation with the Risk Manager, Legal Counsel, Security Officer, and other appropriate parties as necessary, will recommend corrective actions to help prevent future recurrences.
7. The Privacy Officer reports any violations or breaches that involve business associates to the Purchasing Agent and to the Department.