HIPAA Privacy Breach Notification Policy - UTDBP3093

HIPAA regulations require Covered Entities and their Business Associates to investigate and mitigate any security or other incidents that involve potential unauthorized access of Protected Health Information (PHI). Except in very limited instances, any unauthorized access to a Covered Entity's PHI constitutes a breach. Breaches impacting 500 or more individuals must be reported to the U.S. Department of Health & Human Services, the media and the impacted individuals within 60 days of discovery. Breaches impacting fewer than 500 individuals must be reported to the impacted individuals within 60 days of discovery and reported on an annual basis to HHS.

The University of Texas at Dallas is a Covered Entity and is required to comply with these regulations. It is the policy of the University to comply with these regulations at all times. This policy applies to all University officers, faculty, staff, students, volunteers, or any other individual or contractor who provides services to or conducts business on behalf of the University.

Definitions

**Breach** – any unauthorized use, access, or disclosure of information maintained by the University, or for the University by a third party, that is protected by a federal or state privacy law that requires the University to provide breach notifications to an affected individual or any third party.

**Incident** – any act, such as an unauthorized use or disclosure, or any other occurrence that could reasonably involve PHI and indicates that a Breach has occurred.

Responsibility to Notify University Officials

All individuals covered by this policy are required to report possible Incidents of advertent or inadvertent disclosure to the HIPAA Privacy Officer IMMEDIATELY upon discovery. Examples include:

- Accessing and reading medical records out of curiosity
- Faxing a patient's information to the wrong person or agency
- Improper disposal of patient information

Notification to the HIPAA Privacy Officer should be made by phone call, if possible, at 972-883-3601, and must be followed-up with an encrypted email to HIPAAPrivacyOfficer@utdallas.edu describing the Incident in detail.

The responsibility to report Incidents to the HIPAA Privacy Officer includes reporting by the Chief Information Security Officer (CISO) or the CISO's designee when the Incident involves an electronic information resource that may involve PHI.

The responsibility to notify the HIPAA Privacy Officer is in addition to any reporting required by the University's Information Security Polices or other applicable University or UT System Policies.

Business Associate Agreements executed by the University shall require the contractor to notify
the University of any unauthorized use or disclosure by the business associate or its workforce, agents or subcontractors that violates the HIPAA Privacy or HIPAA Security Rules, including any remedial action proposed or taken. The HIPAA Privacy Officer and the HIPAA Security Officer must each receive any contractor reports pertaining to the potential access of electronic PHI.

The HIPAA Privacy Officer must notify legal counsel, the Executive Director of the Callier Center, and the President, without delay, of any reported Incident that upon preliminary analysis could reasonably constitute a Breach.

**Breach Response Team, Investigation, and Risk Analysis**

The HIPAA Privacy Officer will convene a Breach Response Team to immediately investigate and respond to any potential Breach. The composition of the Breach Response Team will depend on the nature of the potential Breach. For example, the HIPAA Security Officer will be a member of the Breach Response Team in instances involving access of PHI through an electronic information resource. Other members may include University legal counsel, the Executive Director of the Callier Center, other Callier administrators, the Chief Compliance Officer, the Vice President for Communications, and the President, if necessary.

The responsibility of the Breach Response Team includes, at a minimum:

- Ensuring that all appropriate actions are immediately taken to prevent any further unauthorized exposure of PHI;
- Investigating the Incident, which may include conducting interviews to learn about circumstances surrounding the Incident; reviewing logs, tapes, and other resources;
- Conducting a risk analysis to determine whether a Breach has occurred;
- Identifying and engaging non-University consultants, as necessary to assist the University in its investigation or risk analysis;
- Conducting a root cause analysis of the Incident;
- Developing a mitigation plan to prevent further exposure of PHI and/or risk of harm to anyone affected by the Breach, which may include revision of the policies and additional workforce training;
- Determining the appropriate notification required and developing an action plan for the delivery of such notices;
- If the Incident involves violations of other University Policy, referring the individual to the appropriate body for disciplinary action, including sanctions in accordance with Section 31 of this manual;
- If the Incident involves a Business Associate or its subcontractor, amending the terms of the Business Associate Agreement or terminating the agreement;
- Keeping the President and senior administration informed.

The Breach Response Team will notify law enforcement, including University Police, local law enforcement agencies, or federal law enforcement agencies, as appropriate, if it determines that the Incident may have been the result of criminal action.
Timeliness

A Breach will be treated as discovered by the University (or a Business Associate or the Business Associate's subcontractor) on the first day such breach is known or should reasonably have been known to have occurred by the University (or its Business Associate or the Business Associate's subcontractor), even if it is initially unclear whether the Incident constitutes a Breach.

Notification to Individuals

Timing: Upon determining a Breach has occurred, the University or Callier Center (or the Business Associate) will make the required individual notifications as soon as reasonably possible after the Covered Entity takes a sufficiently reasonable time to investigate the circumstances surrounding the Breach in order to collect and develop the information required to be included in the notice to the individual, except in no case shall notifications be given later than 60 days following the discovery of a Breach (unless a law enforcement agency requests a delay). Any delay based on a request from law enforcement must be documented in writing by the requesting law enforcement agency. The University or Callier Center may provide the required information in multiple mailings as the information becomes available.

Process: Unless otherwise determined by the President, the Breach Response Team will determine the University office or department responsible for ensuring that the required reporting to individuals and media occurs. Notification to a significant number of individuals and/or the media will be conducted under the direction of the Office of Communications, working with the HIPAA Privacy Officer and University legal counsel.

- In the case of a Breach involving a Business Associate, notifications may be handled by the University or the Business Associate, depending on the terms of the Business Associate Agreement in place and the circumstances surrounding the incident.
- The HIPAA Privacy Officer is responsible for reporting to the Department of Health and Human Services.

Policy History

- Issued: 2014-03-04
- Editorial Amendment 2019-10-29

Policy Links

- Permalink for this policy: https://policy.utdallas.edu/utdbp3093
- Link to PDF version: https://policy.utdallas.edu/utdbp3093/makepdf
- Link to printable version: https://policy.utdallas.edu/utdbp3093/makeprint