11.1.1 Notification of Privacy and Security Breaches

Chapter 11 - Patient Privacy	Original Effective Date: February 2010
Section: 11.1 General and Oversight Policies	Date Last Reviewed: January 2023
Responsible Entity: Chief Compliance and Privacy Officer	Date Last Revised: January 2023

I. Purpose

This policy outlines the reporting responsibilities and potential penalties to both UT Health San Antonio and employees if breaches are not appropriately handled in accordance with federal regulatory requirements and institutional policies.

II. Scope

This policy applies to all faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other individual (collectively, Workforce Member, including employees and non-employees) who has direct or indirect access to patient protected health information (PHI) created, held or maintained by any UT Health San Antonio controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

A. Requirements

UT Health San Antonio is required to report all breaches of protected health information and personally identifying information to the Department of Health & Human Services (HHS). A report of all breaches involving less than 500 individuals per incident is required annually. Breaches involving 500 or more individuals have additional notification requirements as outlined in this policy.

1. Whenever a breach of protected health information and personally identifying information occurs, workforce members are to immediately notify their supervisor, who will notify the chief compliance and privacy officer by completing the Institutional Compliance and Privacy Office Report Form, calling the Compliance Hotline at (877) 507-7317, or emailing compliance@uthscsa.edu. If the supervisor is not available, the workforce member should contact the chief compliance and privacy officer.

2. In addition, if personally identifying information is lost or stolen, a report should be made with the proper law enforcement authorities where the incident occurred and with University Police.

3. Each employee is required to cooperate with institutional officials in identifying what information was stolen and/or compromised. By federal regulations, an individual whose information was breached shall be notified by the chief compliance and privacy officer within sixty (60) days following a discovery of a breach.

B. Determining if a Breach Occurred

1. It is the responsibility of all supervisors and workforce members to immediately report any breaches. The chief compliance and privacy officer, along with other institutional officials, will determine if a breach of information has indeed occurred.

2. All stolen and lost electronic devices shall be reported to the appropriate officials as defined in this policy.

3. An inadvertent or unauthorized access, use or disclosure of information will be evaluated and analyzed to determine when individuals whose information was breached need to be notified.

C. Exceptions to Breach Notifications

1. In accordance with federal regulations, there are some exceptions when an individual(s) does not need to be notified of a breach. However, this determination will be made by the chief compliance and privacy officer and Legal Affairs.

2. UT Health San Antonio has the burden of proving why a breach notification was not required and must document why impermissible use or disclosure fell under one of the exceptions.

3. The chief compliance and privacy officer will conduct a breach risk assessment to determine if a breach occurred.

D. Breach Notification Requirements

The chief compliance and privacy officer must provide notification of a breach of unsecured protected health information to affected individuals, the Secretary of the United States Department of Health & Human Services, and in certain circumstances breaches affecting more than 500 individuals, to the media. Also, business associates must notify the chief compliance and privacy officer that a

breach has occurred. Below is a summary of the required notifications that will be handled by the chief compliance and privacy officer in coordination with appropriate institutional officials.

1. Individual Notice

   The chief compliance and privacy officer must provide notification of a breach of unsecured protected health information to affected individuals, the Secretary of the United States Department of Health & Human Services, and in certain circumstances breaches affecting more than 500 individuals, to the media. Also, business associates must notify the chief compliance and privacy officer that a breach has occurred. Below is a summary of the required notifications that will be handled by the chief compliance and privacy officer in coordination with appropriate institutional officials.

2. Substitute Notice

   a. If UT Health San Antonio has insufficient or out-of-date contact information for fewer than 10 individuals, or if some notices are returned as undeliverable, the chief compliance and privacy officer may provide substitute notice by an alternative form of written notice, by telephone, or other means.

   b. In the event of 10 or more individuals, either with out of date contact information or undeliverable returned notices, then UT Health San Antonio will provide substitute notice through either a conspicuous posting for a period of 90 days on the UT Health San Antonio home page or conspicuous notice in a major print of broadcast media in geographic areas where the individuals affected by the breach likely reside. UT Health San Antonio will provide a toll-free phone number in the notice, active for 90 days, where an individual can learn whether their unsecured protected health information may be included in the breach.

3. Additional Notice in Urgent Situations

   In any case deemed by UT Health San Antonio to require urgency because of possible imminent misuse of unsecured protected health information, UT Health San Antonio may provide information to individuals by telephone or other means, as appropriate, in addition to the methods of individual written notification.

4. Deceased Individual Notice

   If UT Health San Antonio knows that the individual is deceased and has the address of the next of kin or personal representative of the deceased individual, written notification will be sent by first-class mail. In the case

where out-of-date contact information yields notices returned as undeliverable, verification will be attempted than the obligation ends.

5. Media Notice
    a. If UT Health San Antonio experiences a breach affecting more than 500 residents of a state or jurisdiction it is, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the state or jurisdiction. UT Health San Antonio would provide this notification in the form of a press release to appropriate media outlets serving the affected area.
    b. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

6. Notice to United States Department of Health and Human Services
    a. In addition to notifying affected individuals and the media, when appropriate, the chief compliance and privacy officer must notify the Secretary of the United States Department of Health & Human Services (Secretary) of breaches of unsecured protected health information. The chief compliance and privacy officer will be required to provide this notification by submitting an electronic breach notification.
    b. If a breach affects 500 or more individuals, the chief compliance and privacy officer must notify the Secretary without unreasonable delay and in no case later than 60 days following the breach.
    c. All notification requirements will be handled by the chief compliance and privacy officer in the Institutional Compliance and Privacy Office.

7. Law Enforcement Delay
    a. A temporary delay of notification is required in situations in which a law enforcement official provides a statement in writing that the delay is necessary because notification would impede a criminal investigation or cause damage to national security and specifies the time for which a delay is required. In such instances, UT Health San Antonio is required to delay the notification, notice, or posting for the time period specified by the official.
    b. If a law enforcement official states orally that notification would impede a criminal investigation or cause damage to national security a temporary delay of notification notice is required. This delay would be no longer than 30 days from the date of the oral statement and must include the identity of the official making the statement unless a written statement was received during that time for a specified delay time.

8. Notification by a Business Associate

    a. If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify UT Health San Antonio, without unreasonable delay and in no case later than 30 days, following the discovery of the breach.

    b. To the extent possible, the business associate should provide UT Health San Antonio with the identification of each individual affected by the breach, as well as any information required to be provided by UT Health San Antonio in its notification to affected individuals.

9. Content of the Notice

    The HIPAA breach notification will include, to the extent possible, the following elements:

    a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

    b. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, or other types of information were involved);

    c. Any steps the individual should take to protect themselves from potential harm resulting from the breach;

    d. A brief description of what UT Health is doing to investigate the breach, mitigate the harm to individuals, and to protect against any further breaches; and

    e. Contact procedures for individuals to ask questions or learn additional information, which must include a toll free telephone number, an e-mail address, website, or postal address.

10. Burden of Proof

    In the event of an inappropriate use or disclosure UT Health San Antonio or their business associate, as applicable, shall maintain documentation sufficient to meet the burden of proof demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach.

E. Potential Penalties for Breaches

The United States Office of Civil Rights can assess penalties for breach violations. The following tiers of penalties are cited in the Act. An individual employee and the institution may be held liable for not protecting information.

1. Category A: The individual did not know they violated the regulations and was exercising reasonable diligence and would have not known they violated the regulations. The penalty could be $100 and may not exceed $50,000, for each violation.
2. Category B: Violations due to reasonable cause and not to willful neglect. The penalty could be $1,000, and may not exceed $50,000, for each violation.
3. Category C: Violations due to willful neglect and was eventually corrected. The penalty could be $10,000, and may not exceed $50,000, for each violation.
4. Category D: Violations due to willful neglect and not corrected. The penalty could be $50,000 for each violation and may not exceed $1.5 million in a calendar year.

For all the categories above all such violations of an identical provision shall not exceed $1.5 million in a calendar year. In addition to the federal penalties, the State Attorney General may also levy fines and file a civil action on behalf of the individuals harmed.

IV. Definitions

Terms used in this document, have the meaning set forth in the Patient Privacy Policies Glossary *unless a different meaning is required by context.*

V. Related References

For questions regarding this policy contact the privacy program director at 210-567-2014 or compliance@uthscsa.edu.

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
02/2010	Policy Origination		
02/2016	Policy Revision		
01/2023	Policy Review, discretionary edits	ICPO	1/31/2023