THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: H135 - Breach Notification	
Version 2	**Publication Date: 07/18/2024**

Responsible Office: Institutional Compliance Office	**Last Review:** 07/17/2024 **Next Review:** 07/17/2027
Contact: Melanie Burlison, Privacy Officer	**Phone:** 901.448.8030 **Email:** institutional.compliance@uthsc.edu
Related Policies: FI0160 - HIPAA Re-designation and General Policy	

Objective

To ensure that affected individuals, the media, and the Secretary of Health and Human Services (HHS) are appropriately notified of any Breach of unsecured protected health information (PHI) in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), Breach Notification Rule, FTC Health Breach Notification Rule and all applicable regulations and guidance.

Scope

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

UTHSC 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 procedure. This procedure outlines the reporting responsibilities and potential penalties to both UTHSC and/or workforce members if breaches are not appropriately handled in accordance with federal regulatory requirements and UTHSC procedures.

Definitions

- **Breach** - unauthorized acquisition, access, use or disclosure of protected health information and personally identifying information.
- **Disclosure** - the release, transfer, provision of access to, or divulging of information.
- **Use** - the sharing, utilization, examination, or analysis of PHI within an entity that maintains PHI.
- **Business Associate** - a person or entity, including their subcontractors, who provide certain functions, activities, or services for UTHSC involving the use and/or disclosure of protected health information. This includes but is not limited to, lawyers, auditors, third party administrators, healthcare clearinghouses, data processing firms, billing firms, health information organizations, and other covered entities. A business associate is not a UTHSC employee.
- **Protected Health Information** - Individually identifiable health information, including demographic data, that is maintained in any medium that related to:
  a. The individual's past, present or future physical or mental health or condition
  b. The genetic information of the individual

c. The provision of health care to the individual, and/or
d. The past, present, or future payment for the provision of health care to the individual and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

Protected health information does not include individually identifiable health information of persons who have been deceased for more than 50 years.

- **Personally Identifying Information** - Individual personal information, such as Social Security number, driver's license or identification number, date of birth, address, phone number or other personal information.
- **Reasonable Cause** - An act or omission that by exercising reasonable diligence would have known it violated a provision, but did not act with willful neglect.
- **Reasonable Diligence** - Business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.
- **Subcontractor** - A person to whom a business associate delegates a function, activity or service, other than in the capacity of a member of the workforce of such business associate.
- **Willful Neglect** - Conscious, intentional failure or reckless indifference to the obligation to comply with the provision violated.

Procedure

I. Determining If a Breach Occurred

It is the responsibility of all supervisors and employees to immediately report any breaches. The UTHSC Privacy Officer, along with other institutional officials, will determine if a breach of information has indeed occurred. Any 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.

II. Exceptions To Breach Notifications

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 UTHSC Privacy Officer and Legal Counsel. UTHSC 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.

III. Breach Notification Requirements

The UTHSC 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 UTHSC Privacy Officer that a breach has occurred. Below is a summary of the required notifications that will be handled by the UTHSC Privacy Officer in coordination with appropriate institutional officials.

IV. Individual Notice

The UTHSC Privacy Officer must notify affected individuals following the discovery of a breach of unsecured protected health information. The UTHSC Privacy Officer must provide the individual(s) notice in written form by first-class mail. If UTHSC has insufficient or out-of-date contact information for 10 or more individuals, the UTHSC Privacy Officer must provide substitute individual notice by providing the notice on the home page of UTHSC Web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If UTHSC has insufficient or out-of-date contact information for fewer than 10 individuals, the UTHSC Privacy Officer may provide substitute notice by an alternative form of written, telephone, or other means.

The individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what UTHSC is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information. Additionally, a substitute notice provided via UTHSC Web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact UTHSC to determine if their protected health information or personally identifying information was involved in the breach.

V. Media Notice

UTHSC is required to provide notice to prominent media outlets serving the state or jurisdiction for a breach affecting more than 500 residents of a state or jurisdiction, in addition to notifying the affected individuals. UTHSC would provide this notification in the form of a press release to appropriate media outlets serving the affected area. 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.

VI. Notice To United States Department of Health & Human Services

In addition to notifying affected individuals and the media, when appropriate, the UTHSC Privacy Officer must notify the Secretary of the United States Department of Health & Human Services (Secretary) of breaches of unsecured protected health information. The UTHSC Privacy Officer will be required to provide this notification by submitting an electronic breach notification. If a breach affects 500 or more individuals, the UTHSC Privacy Officer must notify the Secretary without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. All notification requirements will be handled by the UTHSC Privacy Officer.

VII. Notification By a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify UTHSC, without unreasonable delay and in no case later than 5 days, following the discovery of the breach. To the extent possible, the business associate should provide UTHSC with the identification of each individual affected by the breach, as well as any information required to be provided by UTHSC in its notification to affected individuals.

VIII. Penalty/Disciplinary Action for Non-Compliance

The United States Office of Civil Rights (OCR) 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.

A. **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.
B. **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.
C. **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.
D. **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.

**The minimum and maximum limits may be increased annually to account for inflation.*