Institutional Handbook of Operating Procedures Policy 6.2.39	
Section: Compliance Policies	Responsible Vice President: Senior Vice President & General Counsel
Subject: Privacy Related	Responsible Entity: Office of Institutional Compliance

I. Title

Privacy Incident Response and Breach Notification

II. Policy

A. Texas Business and Commerce Code Chapter 521, Unauthorized Use of Identifying Information, and the Health Insurance Portability and Accountability Act (HIPAA), protect an individual's personal information. UTMB is required to notify individuals when their PHI or other sensitive personal information has been acquired as a result of a breach. Unauthorized access to PHI or other sensitive personal information, such as social security or bank account numbers, could lead to significant financial, reputational, or other harm to the individual. UTMB shall contact affected individuals so that those individuals, whose PHI or sensitive personal information has been or may have been breached, have the opportunity to mitigate any potential harm.

B. Violation of this policy may result in disciplinary action up to and including termination for employees; a termination of employment relationship in the case of contractors or consultants; or suspension or expulsion in the case of a student. Additionally, individuals may be subject to loss of access privileges and civil and/or criminal prosecution.

III. Notification to Office of Institutional Compliance (OIC)

A. Any UTMB workforce member must notify the OIC immediately if he or she knows, believes or suspects a breach of an individual's PHI or other sensitive personal information has occurred. Retaliation against a workforce member who in good faith reports a security breach is prohibited (*see* IHOP 03.02.09, *Non-Retaliation Policy*).

B. The OIC will work with other officials and departments, including the Information Security Officer, Information Services, and Legal Affairs to conduct a thorough investigation to determine whether a reportable breach has occurred and notification requirements. As part of its investigation, the OIC will take all necessary steps to mitigate any known harm.

IV. Notification to Patients

A. In the event of reportable breaches, the OIC will notify each individual whose PHI or other sensitive personal information has been breached. The notification will be made without unreasonable delay but no later than sixty (60) days of discovery, unless a law enforcement official determines that a notification would impede a criminal investigation.

B. Notification will be by first-class mail and will include the following information, if known:
   1. Circumstances of the breach
   2. Date of the breach
   3. Date the breach was discovered

4. Types of PHI or sensitive information involved
5. Steps individual should take to protect themselves
6. Steps UTMB is taking to mitigate harm and to protect against future breaches
7. How the individual can obtain additional information about the breach (e.g. toll free number, secure email address or postal address.)

C. In situations deemed urgent by the OIC, such as the possibility of imminent misuse, notice by telephone or other method may be used in addition to the above methods.

V. Notification to Health and Human Services (HHS)

A. The OIC will maintain a log of breaches of unsecured PHI affecting fewer than 500 individuals and report such breaches annually to HHS in accordance with HHS guidelines.

B. If a breach of unsecured PHI affects 500 or more individuals, the OIC will notify HHS in accordance with HHS guidelines.

VI. Notification to the Media

The OIC will notify Public Affairs of reportable breaches affecting more than 500 residents of a state or other jurisdiction (i.e. county, city, or town). Public Affairs will notify prominent media outlets serving that state or jurisdiction. OIC and Public Affairs, at their discretion, may elect to notify media in other circumstances.

VII. Notification to the IRB

The OIC will notify the Institutional Review Board (IRB) of any breach involving human subject research.

VIII. Breaches Involving Business Associates

The OIC will work with Business Associates to ensure that any suspected or actual breaches of PHI or other sensitive personal information are reported promptly to the UTMB Privacy Officer or Information Security Officer. All contracts with Business Associates will require Business Associates to report to the UTMB Privacy Officer or Information Security Officer within five (5) calendar days following the discovery of a suspected breach. Workforce members who receive a report of a suspected breach from a Business Associate must notify the OIC immediately.

IX. Definitions

Breach: the unauthorized acquisition, access, use or disclosure of Protected Health Information (PHI) or other sensitive personal information that compromises the security or privacy of such information.

Business Associate (BA): is a person or entity that UTMB contracts with to provide services that require the BA to access, create, receive, maintain, or transmit UTMB's PHI. UTMB workforce members are not considered business associates.

Examples of business associate functions or activities include: claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, software hosting. Examples of business associate services include: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

Protected Health Information (PHI): Individually identifiable health information transmitted or maintained in any form or medium, including oral, written, and electronic. Individually identifiable health information relates to 1) the past, present, or future physical or mental health, or condition of an

individual; 2) provision of health care to an individual; or 3) past, present, or future payment for the provision of health care to an individual. Information is considered PHI where there is a reasonable basis to believe the information can be used to identify an individual.

Sensitive Personal Information: Individual's first name or first initial and last name in combination with any one or more of the following items: a) social security number; driver's license number or government-issued identification number; or account number, credit or debit card number; or b) information that identifies an individual and relates to: the physical or mental health or condition of the individual; the provision of health care to the individual; or payment for the provision of health care to the individual.

Unsecured PHI: PHI that is not made unusable, unreadable, or indecipherable to unauthorized individuals through a technology standard developed or endorsed by a standards developing organization accredited by the American National Standard Institute.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UTMB or a business associate, is under direct control or UTMB or a business associate,, even if they are not paid by UTMB or business associate.

X. Relevant Federal and State Statutes

45 Code of Federal Regulations Part 164 – Security and Privacy
Texas Business & Commerce Code Chapter 521
Texas Government Code Section 2054.1125

XI. Dates Approved or Amended

Originated: 7/5/2010	
Substantive Revisions	*Non-Substantive Revisions*
8/14/2014	

XII. Contact Information

Office of Institutional Compliance
409.747.8700 (ext. 78700) or cpo@utmb.edu