Institutional Handbook of Operating Procedures Policy 06.02.10	
Section: Compliance	Responsible Vice President: Senior Vice President & General Counsel
Subject: Privacy	Responsible Entity: Office of Institutional Compliance

I. Title

Physical Protections/Safeguards for Protected Health Information (PHI).

II. Policy

The HIPAA Rules require that UTMB have reasonable safeguards in place to protect PHI, in all formats (i.e. written, oral, or electronic), from intentional or unintentional use or disclosure that is in violation of the Privacy Rules. As part of UTMB's commitment to maintain patient confidentiality, UTMB employees, including administration, faculty, fellows, residents, and students as well as university and hospital subcontractors, independent contractors, and consultants. are expected to comply with the UTMB the guidelines below for safeguarding the use and disclosure of PHI.

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. General Safeguards

UTMB workforce are instructed to maintain the privacy and confidentiality of PHI as follows:

1. UTMB workforce members will discuss PHI with other workforce members only when the other person is authorized to have access to PHI for purposes of performing job responsibilities related to UTMB's treatment, payment, or health care operations, or for other authorized purposes.
2. UTMB workforce members must avoid unnecessary disclosures of PHI through oral communications. Conversations, both phone and face-to-face, involving PHI shall take place in low tones and in closed offices or cubicles when possible.
3. When having a conversation in a public area with a patient, the patient's family members, or other conversations in which PHI is discussed, conduct the conversation in a lowered voice, to the extent possible, and avoid using patients' names or the names of patients' family members when persons who are not authorized to receive the information are present.
4. PHI will not be disclosed to any workforce member of UTMB for purposes of employment matters, or other decisions regarding the individual who is the subject of the PHI, unless the individual has signed an authorization permitting such use or disclosure.
5. PHI may be released over the telephone in the same manner that it may be released in person, in accordance with the policies regarding disclosures of PHI, and will be documented as appropriate. When handling a call that involves PHI efforts to verify the identity and authority of the caller will be made prior to discussing the PHI. (See IHOP 6.2.32 *Verification Requirements Prior to Disclosing PHI*.)
6. PHI mailed either within UTMB or outside UTMB must be in sealed envelopes and no PHI can be visible.
7. Locate computer screens and monitors in areas or at angles that minimize viewing by persons who do not need the information or utilize privacy screens.

8. Locate whiteboards and scheduling boards that display PHI in areas that minimize viewing by persons who do not need the information or de-identify the PHI.
9. Bulletin boards located in areas that may be seen by patients or visitors should not contain any documents containing PHI, unless the patient has agreed to the display by written or documented verbal permission. This would include baby pictures, cards and notes of appreciation and children's signed art work.

IV. Guidelines for Printing PHI

1. PHI should not be printed or copied indiscriminately or left unattended and open to compromise. The original media should be used (e.g., hardcopy medical record, EPIC, MyUTMB) and only reproduced when absolutely necessary.
2. Printers and copiers used for printing of PHI should be in a secure location. If the equipment is in a non-secure location, the information being printed or copied is required to be strictly monitored.
3. PHI printed to a shared printer should be promptly removed.
4. PHI in hardcopy format must be disposed of in accordance with records retention schedules managed by UTMB Records Management, and the Disposal of PHI policy.
5. Only the minimum amount of PHI should be printed or copied.
6. Reports of individuals who are inappropriately printing or copying PHI should be made in accordance with IHOP Policy 6.2.39, *Privacy Incident Response and Breach Notification*.
7. Health Information Management (HIM) as the custodian of the medical record has the sole authority to disclose PHI when a patient authorization is required. See IHOP 6.2.1, *Use and Disclosure Based on Patient Authorization* for limited exceptions.

V. Guidelines for Securing and Storing PHI

UTMB workforce must follow these standards relating to securing and storing of PHI:

1. Keep track of all PHI in your possession, whether on or off UTMB premises, and secure it when in public locations. PHI that is left unattended in public or dropped or misplaced can result in disciplinary action.
2. Store paper PHI in areas that are not accessible to unauthorized individuals, preferably in a locked room or filing cabinet.
3. Any documents containing PHI should be placed with the PHI face down on counters, desks, and other places where patients or visitors might see them. Documents should not be left out on desks or countertops after business hours but should be placed in locked file cabinets, locked desk drawers, or other secure areas (e.g., the individual office can be locked).
4. Do not leave materials containing PHI in conference rooms, out on desks, or on counters or other areas where the PHI may be accessible to persons who do not have a need to know the information.
5. When transporting medical records, they should never be left unattended and records should be covered or turned over so that PHI is not visible to casual observers.
6. PHI stored in medical equipment (e.g. EKG, Ultrasound) must be kept secure and disposed in a way that preserves the confidentiality of the PHI.
7. PHI should not be stored on portable electronic devices (e.g., laptop computers, USB drives). Exceptions must be approved by the UTMB Information Security Officer. (See Information Resources Practice Standard 1.19 *Portable Computing* for additional information.)
8. If PHI is stored on CD-ROM or other removable data storage media, it cannot be commingled with other electronic information.

VI. Guidelines for Disposal of PHI

PHI may only be disposed of by means that ensure confidentiality so that it will not be accidentally released to an outside party. UTMB workforce must strictly observe the following standards relating to disposal of hardcopy and electronic copies of PHI:

1. UTMB Department Heads shall provide users with access to shredders or secured recycling bags for proper disposal of confidential printouts containing PHI.
2. Convenience copies containing PHI may be disposed of by shredding or in secure recycle bags. However, for official UTMB records, documentation of destruction may be required. (See IHOP 9.2.14, *Medical Record Retention* and IHOP 6.1.5, *Records and Information Management and Retention* for additional information on the destruction of official records.)
3. Only those items that have no PHI or have had identifiable PHI obliterated so that it is no longer recognizable (for example, IV bags that have privacy stickers adhered) may be placed in appropriate trash bins, unsecured recycle bags or be disposed of through other methods.
4. Microfilm or microfiche must be cut into pieces or chemically destroyed.

Secured Recycling Bags

1. While on the floor, secured recycling bags should be placed in an area where unauthorized persons cannot easily view or access the PHI contained in the secure recycle bag.
2. When a recycling bag is full, the bag should be zipped closed and locked with the locking mechanism provided by UTMB. Bags shall be stored in a secure location until they are picked up by Housekeeping staff. When bags are ready to be picked up call ext. 24040 to arrange for collection.
3. The recycle bags on campus are considered protected property of UTMB and are not to be tampered with. The contents of the recycle bags may contain confidential information and were disposed of with the expectation of privacy and non-removal. Any UTMB workforce or other individuals removing items from the secured recycle bags will be subject to disciplinary action. All instances of tampering with secured recycle bags must be reported to the Office of Institutional Compliance or the Fraud, Abuse and Privacy Hotline.

Electronic PHI

Secure methods, in compliance with NIST 800-88 Guidelines for Media Sanitization, will be used to dispose of electronic data and output of PHI. Deleting data or reformatting the disk is NOT a sufficient method of removing electronic PHI. Electronic PHI must be completely removed before devices are redeployed, donated, sold, recycled or otherwise discarded. Examples of devices which may include electronic PHI include, but are not limited to: computer hard drives, fax machines, photocopy machines, medical equipment devices, CDs, and USB drives.

Methods to remove electronic data include:

1. Zeroing, a data removal Service software, to write “zero” to all areas of a disk overwriting any data that may be on the disk.
2. “Degaussing” (removing or neutralizing the magnetic field) computer tapes to prevent recovery of data;
3. Physical destruction of CDs, portable storage media, or other hardware.

UTMB service providers (e.g. Information Services, Hospital Clinical Engineering, etc.) will remove electronic PHI for equipment that they support. These service providers will also provide guidance and/or assistance in removing electronic PHI to departments for equipment not centrally supported.

VII. Definitions

Privacy Stickers: refer to special white labels with a black backing available through Materials Management (MM). The privacy sticker inhibits view of the patient's printed label from both sides of a plastic bag and leaves a black film if removed further obliterating PHI.

Safeguards: Rules and methods to protect PHI from unauthorized access, accidental or intentional use, disclosure, transmission, or alteration, and inadvertent or incidental disclosure.

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

VIII. Relevant Federal and State Statutes

45 C.F.R. § 164 Subpart E—Privacy of Individually Identifiable Health Information

IX. Related UTMB Policies and Procedures

IHOP - 06.01.05 - *Records and Information Management and Retention*
IHOP - 06.02.00 - *Maintaining Patient Confidentiality through the Appropriate Use and Disclosure of PHI*
IHOP - 06.02.01 - *Use and Disclosure Based on Patient Authorization*
IHOP - 06.02.32 - *Verification Requirements Prior to Disclosing PHI*
IHOP - 09.02.14 - *Medical Record Retention*
Information Resources Practice Standard 1.4, *Portable Computing*

X. Additional References

NIST 800-88 Guidelines for Media Sanitization

XI. Dates Approved or Amended

Originated: 04/11/2003	
Reviewed with Changes	*Reviewed without Changes*
08/02/2012	08/27/2015
	01/10/2020

XII. Contact Information

Office of Institutional Compliance
(409) 747-8700