

Section 6 Subject 6.2	Compliance Policies Privacy Related	04/11/03- Originated 08/02/12- Reviewed w/changes - Reviewed w/o changes
Policy 6.2.10	Physical Protections/Safeguards for Protected Health Information (PHI)	09/07/12 -Effective Compliance Office - Author

Physical Protections/Safeguards for Protected Health Information (PHI)

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.

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, employees 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.

General Safeguards

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

UTMB employees will discuss PHI with other employees only when the other person is authorized to have access to PHI for purposes of performing job responsibilities related to UTMB’s

1. treatment, payment, or health care operations, or for other authorized purposes.
2. UTMB employees 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

UTMB HANDBOOK OF OPERATING PROCEDURES

Section 6 Subject 6.2	Compliance Policies Privacy Related	04/11/03- Originated 08/02/12- Reviewed w/changes - Reviewed w/o changes 09/07/12 -Effective Compliance Office - Author
Policy 6.2.10	Physical Protections/Safeguards for Protected Health Information (PH)	

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 shall have 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.

Guidelines for Securing and Storing PHI

All UTMB employees 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.

UTMB HANDBOOK OF OPERATING PROCEDURES

Section 6 Subject 6.2	Compliance Policies Privacy Related	04/11/03- Originated 08/02/12- Reviewed w/changes - Reviewed w/o changes 09/07/12 -Effective Compliance Office - Author
Policy 6.2.10	Physical Protections/Safeguards for Protected Health Information (PH)	

Guidelines for Securing and Storing PHI, continued

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 will 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 1.4.2 Portable Computing for additional information and see <http://www.utmb.edu/infosec/encryption/Index.asp> for instructions on encryption.)
8. If PHI is stored on CD-ROM or other removable data storage media, it cannot be commingled with other electronic information.

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. All UTMB employees 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 2.1.4 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

UTMB HANDBOOK OF OPERATING PROCEDURES

Section 6 Subject 6.2	Compliance Policies Privacy Related	04/11/03- Originated 08/02/12- Reviewed w/changes - Reviewed w/o changes 09/07/12 -Effective Compliance Office - Author
Policy 6.2.10	Physical Protections/Safeguards for Protected Health Information (PH)	

Guidelines for Disposal of PHI

- 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 employees are ready for the bags 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 personnel 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 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 services providers (e.g. Information Services, Clinical Equipment Services, 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.

References

IHOP 6.2.36 Maintaining Patient Confidentiality
IHOP 9.2.13 UTNB Medical Record Policy
