Institutional Handbook of Operating Procedures Policy 06.02.24	
Section: Compliance Policies	Responsible Vice President: Senior Vice President and General Counsel
Subject: Privacy Related	Responsible Entity: Office of Institutional Compliance

I. Title

Removal of Protected Health Information from UTMB Facilities

II. Policy

Original medical records shall not be removed from the premises of UTMB Hospitals and outpatient facilities except in accordance with a court order, subpoena or statute and must be approved by HIM. Other types of PHI, for example case management records, printouts from EPIC, handwritten case notes, or forms with PHI, should not be removed from UTMB premises except in accordance with this policy.

The safety and return of the medical records, including convenience copies, checked out or removed are the sole responsibility of the person who checked them out or removed them. Whenever a hardcopy version of PHI (for example, photocopies of records, handwritten notes or information printed from EPIC) or electronic PHI is removed from UTMB premises, it must be secured and protected at all times and must not be left unattended in places in which unauthorized persons can gain access. The storage and security of PHI must follow IHOP Policy 6.2.10, Physical Protections/Safeguards for PHI. UTMB policies, regarding the use, disclosure and protection PHI, are in effect whether the employee is working off-site or in a UTMB facility and include the following requirements:

1. Case Management Records, Source Data and any other information that contains PHI may not be removed from UTMB premises unless there has been prior approval from the custodian of the information and from the employee's supervisor. Also, removal of PHI from UTMB must be for a legitimate business reason. A Request for Use of PHI Offsite form should be completed.

In some instances the removal of Case Management Records and other PHI may require documentation and tracking as provided for in IHOP Policy 9.2.13, UTMB Medical Record Policy.

2. While transporting PHI in a personal motor vehicle, paper records and medical charts should not be left in automobiles or in view of passers-by. If possible, the information should be placed in the trunk of the automobile or if there is no trunk in an area of the vehicle that cannot be seen from the outside.

3. When employees use PHI at home, the information (whether it be paper, on a flash drive, or electronic) should be stored in a secure manner so no other individual(s) in the home will have access to the PHI. For example the information should be locked in a file drawer or briefcase when not in use. If UTMB computers or individual home computers are used to store PHI, the PHI must be stored and protected from any and all unauthorized access.

4. If UTMB PHI is stored on a laptop or other portable device, either UTMB owned or a personally owned, the device must have approval from the UTMB Information Security Officer and the device must be encrypted using a full disk encryption product approved by UTMB's Hardware and Software Standards

Committee. (*See* IHOP 6.2.10 Physical Protections/Safeguards for PHI and IS Practice Standard 1.4.2 Portable Computing.) All PHI must be returned to the UTMB custodian who granted the UTMB employee permission to remove the PHI, except for convenience copies.

5. In the case of convenience copies that are not required to be returned, the individual must dispose of the information in accordance with IHOP 6.2.10 Physical Protections/Safeguards for PHI. This requirement applies to electronic PHI, as well.

6. The theft or loss of any paper record or medical chart shall be reported immediately to HIM, or the UTMB Privacy Officer so that mitigation options can be considered and implemented. (See IHOP 6.2.39 Privacy Incident Response and Breach Notification.)

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. Definitions

Case Management Records (CMR): A medical record maintained by a specific physician or department that only includes copies of original patient care information already in the UMR. Commonly referred to as "shadow records," CMRs are considered convenience copies only and have no record retention schedule. CMRs should never contain original medical records

Convenience Copy: A copy of an original medical record, case management record or source data that was printed for a one time use. Convenience copies may be items like lab reports or other information found in an electronic system that are used for convenience but not required to be maintained in storage or in files.

Encryption: process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable ciphertext (ibid.). This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the ciphertext, should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm, to randomly produce keys.

Medical Record Custodian: The person or department responsible for the maintenance, retention, access, data integrity, and data quality of Protected Healthcare Information (PHI); including protecting patient privacy and providing information security, analyzing clinical data for research and public policy, preparing PHI for accreditation surveys, and complying with standards and regulations regarding PHI.

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. Demographic information on

patients is also considered PHI.

Unit Medical Record (UMR): The official UTMB medical record maintained by the Department of Health Information Management (HIM) that contains UTMB's original/official patient care information.

The UMR is designed to contain the written interpretations of all significant clinical information gathered for a given patient, whether as an inpatient, outpatient, or emergency care patient. The entire patient's medical record is thus in paper or electronic form under one hospital number. UMR's have a permanent retention schedule.

Source Data: Source Data is data from which interpretations, summaries, or notes are derived, regardless of media. This data includes health information stored in any original media. Examples of Source Data include, but are not limited to, paper diagnostic tests or tools, x-rays, videotapes, ultrasounds, fetal monitor strips, photographs (either conventional photos or digital images), and ancillary or supporting systems (e.g. pharmacy information systems and radiation oncology information systems). The UMR must contain a written interpretation of all Source Data. Source Data is distinct from the written interpretations of significant clinical information that has been forwarded to the UMR and is not part of the legal medical record.

IV. Related UTMB Policies and Procedures

IHOP - 06.02.10 - Physical Protections/Safeguards for Protected Health Information (PHI)
IHOP - 06.02.39 - Privacy Incident Response and Breach Notification
IS Practice Standard 1.4 - Portable Computing
IHOP - 09.02.13 - UTMB Medical Record Policy

V. Dates Approved or Amended

Originated: 12/10/2013	
Reviewed with Changes	*Reviewed without Changes*
01/10/2013	08/20/2018

VI. Contact Information

Office of Institutional Compliance
(409) 747-8700