utmb Health

Institutional Handbook of Operating Procedures Policy 06.02.29	
Section: Compliance Policies	Responsible Vice President: Senior Vice President & General Counsel
Subject: Privacy Related	Responsible Entity: Office of Institutional Compliance

I. Title

De-Identification of PHI

II. Policy

UTMB has a duty to protect the confidentiality and integrity of protected health information (PHI) as required by law, professional ethics, and accreditation requirements.

When identifying characteristics are completely removed from PHI and is rendered anonymous the information is considered de-identified. Information that has been de-identified in accordance with this policy is no longer PHI and is not be subject to the same requirements as PHI.

Whenever possible, de-identified PHI shall be used by UTMB workforce members.

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. Guidelines

All personnel must strictly observe the following guidelines relating to the de-identification of PHI:

A. De-identification requires the elimination of primary or obvious identifiers and secondary identifiers through which a user could determine the patient's identity. For information to be de-identified the following identifiers of the individual (and/or of relatives, employers, or household members of the individual) must be removed:

- **i.** Names;
- **ii.** Address information smaller than a state, including street address, city, county, zip code (Except if by combining all zip codes with the same initial three digits, there are more than 20,000 people.) If there is a question regarding the permissive use of a zip code, contact the IRB or the Privacy Office;
- **iii.** Names of relatives and employers;
- **iv.** All elements of dates (except year), including DOB, admission date, discharge date, date of death; and all ages over 89 and all elements of dates including year indicative of such age except that such ages and elements may be aggregated into a single category of age 90 or older;
- **v.** Telephone numbers;
- **vi.** Fax numbers;
- **vii.** Email addresses;
- **viii.** Social Security Number (SSN);
- **ix.** UH number (medical record number);
- **x.** Health beneficiary plan number;

- **xi.** Account numbers;
- **xii.** Certificate/License Number;
- **xiii.** Vehicle identifiers, including license plate numbers;
- **xiv.** Device ID and serial number;
- **xv.** Universal Resource Locator (URL);
- **xvi.** Identifier Protocol (IP) addresses;
- **xvii.** Biometric identifiers, including finger and voice prints;
- **xviii.** Full face photographic images and comparable images; and
- **xix.** Any other unique identifying number characteristic or code.

B. UTMB has developed a De-identification Checklist to assist employees in determining whether the necessary identifiers have been removed to render the information de-identified.

C. The information is not de-identified if all of the identifiers above have been removed but UTMB has any actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

D. Whenever possible, de-identified PHI should be used for quality assurance monitoring and routine utilization reporting. If de-identified PHI cannot be used, a limited data set should be used whenever possible. See IHOP 6.2.13, Uses and Disclosures of PHI for Limited Data Sets.

E. PHI used for research, including public health research, should be de-identified at the point of data collection for research protocols approved by the IRB, unless the participant voluntarily and expressly consents to the use of his/her personally identifiable information or an IRB waiver of authorization is obtained. If de-identified PHI cannot be used for research, a limited data set should be used whenever possible. See IHOP 6.2.13, Uses and Disclosures PHI for Limited Data Sets.

F. If an authorized user wishes to encrypt PHI when creating de-identified information the authorized user must ensure that:

- **i.** The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
- **ii.** UTMB does not use or disclose the code or other means of record identification for any purpose and does not disclose the mechanism for re-identification.

G. If de-identified Information is re-identified by UTMB, a Business Associate or other valid requestor, the re-identified information is considered PHI and must be treated as such.

IV. Relevant Federal and State Statutes

45 C.F.R. §164.502(d) *Standard: Uses and disclosures of de-identified protected health information*
45 C.F.R. §164.514
45 C.F.R. §164.512(i) *Standard: Uses and disclosures for research purposes*

V. Related UTMB Policies and Procedures

IHOP - 06.02.13 - Use and Disclosure of PHI for Limited Data Sets

VI. Additional Resources

Deidentification Checklist

VII. Dates Approved or Amended

Originated: 5/12/2003	
Substantive Revisions	*Non-Substantive Revisions*
9/2/2011	11/26/2014
	03/15/2019

VIII. Contact Information

Office of Institutional Compliance
(409) 747-8700