

Section 3	Compliance Policies	00/00/03	- Effective
Subject 6.2	HIPAA: Privacy and Disclosure		- Revised
Policy 6.2.29	De-Identification of PHI		- Reviewed
		Compliance Office	- Author

De-Identification of PHI

Audience

The information in this document applies to all UTMB faculty, staff, students, volunteers, and any other contractors or agents granted access to Protected Health Information (PHI).

Definitions

Institutional Review Board (IRB): A committee group comprised of UTMB personnel and community representatives with varying backgrounds and professional experience that review and approve the research protocol involving human subjects.

Authorized User: An individual that is granted access to PHI for patients through an authorization, IRB waiver or who is performing an activity related to health care operations.

Health Care Operations: Activities related to UTMB's functions as a health care provider, including general administrative and business functions necessary for UTMB to remain a viable health care provider.

Limited Data Set: A compromise between protected health information (PHI) and de-identified information. For use only in public health, research, and health care operations.

Protected Health Information (PHI): Individually identifiable health information transmitted or maintained in any form or medium, including oral, written, and electronic communications. Individually identifiable health information relates to an individual's health status or condition, furnishing health services to an individual or paying or administering health care benefits to an individual. Information is considered PHI where there is a reasonable basis to believe the information can be used to identify an individual.

Policy

UTMB has a duty to protect the confidentiality and integrity of PHI as required by law, professional ethics, and accreditation requirements. Whenever possible, de-identified PHI should be used. De-identified PHI is rendered anonymous when identifying characteristics are completely removed. PHI must be de-identified prior to disclosure to non-authorized users. This policy defines the guidelines and procedures that must be followed for the de-identification of PHI.

Continued on next page

Section 6	Compliance Policies	00/00/03	- Effective
Subject 6.2	Privacy and Disclosure		- Revised
			- Reviewed
Policy 6.2.29	De-Identification of PHI	Compliance Office	- Author

De-Identification of PHI, Continued

Guidelines

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

- o De-identification requires the elimination not only of primary or obvious identifiers, such as the patient’s name, address, date of birth (DOB), and treating physician, but also of secondary identifiers through which a user could deduce the patient’s identity. For information to be de-identified the following identifiers of the individual (or of relatives, employers, or household member of the individual) must be removed:

- Names
- 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)
- Names of relatives and employers
- All element 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;
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security Number (SSN)
- UH number (medical record number)
- Health beneficiary plan number
- Account numbers
- Certificate/License Number
- Vehicle identifiers, including license plate numbers
- Device ID and serial number
- Uniform Resource Locator (URL)
- Identifier Protocol (IP) addresses
- Biometric identifiers
- Full face photographic images and other comparable images
- Any other unique identifying number characteristic, or code.

Section 6	Compliance Policies	00/00/03	- Effective
Subject 6.2	Privacy and Disclosure		- Revised
Policy 6.2.29	De-Identification of PHI	Compliance Office	- Reviewed
			- Author

De-Identification of PHI, Continued

Guidelines (cont'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 Limited Data Sets*.
- 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 of Limited Data Sets*.
- If an authorized user wishes to encrypt PHI when creating de-identified information the authorized user must ensure that:
 - 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
 - Anyone involved in the research project does not use or disclose the code or other means of record identification and does not disclose the mechanism to accomplish re-identification.

If removal of any identifiers is not practical or does not meet your business needs and you still wish to use PHI, you must obtain approval from the UTMB Privacy Office

Enforcement

All supervisors are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

References

45 C.F.R. §164.502(d)
 45 C.F.R. §164.514
 45 C.F.R. §164.512(i)