

**Texas Tech University Health Sciences Center
HIPAA Privacy Policies**

Administration	Policy 1.5
De-Identification of Protected Health Information	Effective Date: May 1, 2015 Reviewed Date: August 8, 2017
References: http://www.hhs.gov/ocr/hipaa HSC HIPAA website http://www.ttuhscc.edu/hipaa/policies_procedures.aspx	

Policy Statement

Texas Tech University Health Sciences Center (HSC) is committed to ensuring the privacy and security of patient health information. Federal law allows certain healthcare organizations to use or disclose personal health information (PHI) for the purpose of creating de-identified information – that is, information that has been stripped of any elements that may identify the patient, such as name, birth date, or social security number. HSC will, from time to time, use de-identified data for various purposes such as utilization research. In doing so, HSC will ensure that the appropriate administrative and technical processes are in place to properly de-identify PHI, as well as to secure any methods to re-identify, as required under 45CFR§164.514(a) and other applicable federal, state, and/or local laws and regulations.

Scope and Distribution

This policy applies to all health care clinical service areas owned and/or operated by TTUHSC. It does not apply to inmates seen or treated by TTUHSC.

Definitions

Refer to [HPP 1.1](#) for Glossary of HIPAA Terms

See [Old/New HIPAA Policy Number Cross Reference Chart](#)

Procedure

- A. The following individually identifying elements will be removed or otherwise concealed from PHI in order to create *de-identified* information:
- Names
 - All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all elements of dates (including year) for all ages over 89, except that such ages and elements may be aggregated into a single category of 90 or older.
 - Telephone numbers
 - Fax numbers
 - Electronic mail (email) addresses
 - Social Security numbers
 - Medical record numbers
 - Health plan beneficiary numbers
 - Account numbers

**Texas Tech University Health Sciences Center
HIPAA Privacy Policies**

- Certificate/license numbers
 - Vehicle identification and serial numbers, including license plate numbers
 - Device identifiers and serial numbers
 - Web Universal Resource Locators (URLs)
 - Internet Protocol (IP) address numbers
 - Biometric identifiers, including finger or voice prints
 - Full face photographic images and any comparable images
 - All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and equivalent geocodes
 - Any other unique identifying numbers, characteristic, or code, other than a code assigned to a record to permit TTUHSC to re-identify the information
 - The initial three digits of a zip code may be used if, according to the publicly available data from the Bureau of the Census:
 1. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
 2. The initial three digits of a zip code for all such geographic units containing 20,000 few people changes to 000
- B. If any listed identifiers are not removed, then the information will only be disclosed when the Institutional Privacy Officer or the campus' Regional Privacy Officer:
1. Determines that the risk is very small that the information could be used alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
 2. Document the methods and results of the analysis that justify such determination.
- C. Knowledge of a violation or potential violation of this policy must be reported directly to a Regional Privacy Officer, the Institutional Privacy Officer or to the employee Compliance Hotline at (866) 294-9352 or at the [Texas Tech University Compliance Hotline website](#).

Approval Authority

The TTUHSC Privacy and Security Committee has authority for HIPAA policy approval.

Responsibility and Revisions

Questions regarding this policy may be addressed to the Regional Privacy Officer ([Amarillo](#), [Permian Basin](#) [Lubbock](#)), the [Institutional Privacy Officer](#), or the [Institutional Compliance Officer](#).

This policy may be amended or terminated at any time.