I. 11.2.9 De-identification of Protected Health Information

Chapter 11 - Patient Privacy	Original Effective Date: April 2003
Section: 11.2 Uses and Disclosures of Protected Health Information	Date Last Reviewed: August 2026
Responsible Entity: Chief Compliance and Privacy Officer	Date Last Revised: August 2026

II. Purpose

UT Health San Antonio (UTHSA) has a duty to protect the confidentiality and integrity of protected health information(PHI) as required by law, professional ethics, and accreditation requirements. Whenever possible, UTHSA will use PHI that is de-identified. 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 protected health information.

III. Scope

This policy applies to all Workforce Members—including faculty, staff, students, healthcare providers, contractors, and researchers—who have direct or indirect access to Protected Health Information (PHI). This includes all PHI maintained by UTHSA and its controlled affiliates, such as clinics, hospitals, and research facilities.

IV. Policy

A. Uses and Disclosures of De-identified Protected Health Information

1. UTHSA may use PHI to create information that is not individually identifiable health information or disclose PHI only to a business associate for such purpose, whether the de-identified information is to be used by UTHSA. The requirements do not apply to information that has been de-identified as described below, provided that:

   a. Disclosure of a code or other means of record identification designed to have information re-identified constitutes disclosure of PHI; and,

   b. If de-identified PHI is re-identified, use or disclosure of such re-identified information may only be permitted as required by UTHSA policies on use and disclosure of PHI.

2. Whenever possible, de-identified PHI should be used for quality assurance monitoring and routine utilization reporting.

B. Requirements for De-identification of Protected Health Information

1. UTHSAmay determine that health information is not individually identifiable if:

a. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable by:

i. Applying such principles and methods 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

ii. Documents the method and results of the analysis that justify such determination; or,

iii. UTHSA does not have 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; or,

iv. The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(1) Names;

(2) Address information smaller than a state, including state address, city, county, precinct, zip code (except if by combining all zip codes with the same initial three digits, there are more than 20,000 people);

(3) Names of relatives and employers;

(4) All element of dates (except year), including date of birth, 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;

(5) Telephone numbers;

(6) Fax numbers;

(7) E-mail addresses;

(8) Social Security Number (SSN);

(9) Medical record number;

(10) Health beneficiary plan number;

(11) Account numbers;

(12) Certificate/License Number;

(13) Vehicle identifiers, including license plate numbers;

(14) Medical device ID and serial number;

(15) Uniform Resource Locator (URL);

(16) Identifier Protocol (IP) addresses;

(17) Biometric identifiers (such as fingerprints, retinal scans, etc.);

(18) Full face photographic images and other comparable images; and

(19) Any other unique identifying number characteristic or code.

2. PHI used for research, including public health research, should be de-identified at the point of data collection for a research protocol 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.
3. UTHSA may maintain some patient information in limited data sets, which do not contain direct identifiers, such as name, address, social security number, but may contain date of birth and dates of treatment. See Institutional Handbook of Operating Policies policy 11.2.13 Limited Data Sets for guidance.

C. Re-identification of Protected Health Information

1. If an authorized user encrypts PHI when creating de-identified information, the authorized user must ensure that:
   a. 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 to identify the individual; and
   b. No one involved in the de-identification process discloses the code or other means of record identification and does not disclose the mechanism to accomplish re-identification.
2. A person may not re-identify or attempt to re-identify an individual who is the subject of any PHI without obtaining the individual's consent or authorization if required under state or federal law

D. Artificial Intelligence (AI) and De-identified Protected Health Information

1. Prior to using de-identified PHI in any AI technology, workforce members must contact the Office of Information Security to initiate an AI risk assessment. This requirement applies to all AI use cases, including vendor-provided AI solutions, internally developed AI or machine learning (ML) models, research activities, and AI systems used for clinical care, operations, or administrative functions.
2. Workforce members must not use AI platforms to process, create, or share identifiable PHI unless explicitly approved by the Office of Information Security in accordance with IHOP 5.8.33 Acceptable Use of Artificial Intelligence Platforms.
3. If de-identified PHI will be used to train or improve an AI model, UTHSA must have a written agreement, reviewed by the Office of Legal Affairs, that clearly identifies the value the University receives in return in accordance with state regulatory requirements.

a. Most free AI tools do not have agreements with UTHSA and therefore generally do not provide these contractual protections to ensure compliance with state regulatory requirements.

V. Definitions

Terms used in this document have the meaning set forth in the Patient Privacy Policies Glossary *unless a different meaning is required by context.*

VI. Related References

For questions regarding this policy, contact the Privacy Program Director at 210-567-2014 or compliance@uthscsa.edu.

Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, *U.S. Department of Health and Human Services*, HHS. gov.

VII. Review and Approval History

The approving authority of this policy is the University Executive Committee.

Effective Date	Action Taken	Approved By	Approved Date
04/2003	Policy Origination		
02/2006	Policy Revision		
03/2013	Policy Revision		
01/2023	Policy Review	ICPO	01/13/2023
08/2026	Policy Revision	Executive Committee	08/31/2026