



## Uses and Disclosures

### Policy # 2.6

## De-Identificaton of PHI

Original Effective  
Date:

10/24/2016

Revised Date:

**Purpose:** Establish methods for properly de-identifying PHI such that it is no longer PHI under HIPAA.

**Policy:** Travis County de-identifies PHI when it is possible and appropriate prior to disclosing data. If, at any time, a workforce member suspects that data to be released or that has been released is not de-identified, then the workforce member is required to report this suspicion to the Privacy Officer immediately.

#### Procedures:

1. PHI may be de-identified in one of two ways: a) the safe harbor method or b) the expert determination method.
  - a) Safe Harbor Method. Covered Components, in consultation with the Privacy Officer or the Covered Component Privacy Liaison (if applicable), remove the following 18 specific identifiers:
    - i. Names (including initials or partial names)
    - ii. All geographic subdivisions smaller than a state (including street address, city, county, precinct, zip code, and their equivalent geocodes), except for the first three digits of a zip code.
      - Note: For the following 17 partial Zip Codes, even the first three digits are considered an “identifier” and must be instead changed to “000” in order for it to meet the De-Identification standard: 036, 059, 063, 102, 203, 556, 692, 790, 821, 823, 830, 831, 878, 879, 884, 890, and 893.
    - iii. All elements of dates, except year, directly related to an individual (for example, birth date, admission date, discharge date, Treatment dates, date of death).
      - Note:
        - Ages 89 and less may be used, but ages 90 and greater must be changed to “90 or older.”
        - It is permissible to convert dates to time periods using years (for example, “years between diagnosis and death: 3”).
    - iv. Telephone numbers.
    - v. Fax numbers.
    - vi. E-mail addresses.
    - vii. Social Security numbers.

- viii. Medical record numbers.
  - ix. Health plan beneficiary numbers.
  - x. Account numbers.
  - xi. Certificate/license numbers.
  - xii. Vehicle identifiers and serial numbers, including license plate numbers.
  - xiii. Device identifiers and serial numbers.
  - xiv. Web Universal Resource Locators (URLs).
  - xv. Internet protocol (IP) address numbers.
  - xvi. Biometric identifiers including finger and voice prints.
  - xvii. Full face photographic images or other identifying images (for more information on de-identifying images, see procedure 2(c)).
  - xviii. Any other unique identifying number, characteristic or code (for example, study ID numbers), except as permitted under procedure 3 below.
- b) Expert Determination Method. Covered Components may request written approval from the Privacy Officer to utilize the expert determination method when:
- i. A person (“expert”) with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable can be utilized to de-identify the information;
  - ii. The expert applies generally accepted statistical and scientific principles to determine the risk is very low 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 the subject of the information; and
  - iii. The expert documents the methods and results of the analysis that justify such determination.
- c) De-identifying Images
- i. Covered Components remove identifiable traits on images of individuals such that it is not possible for someone (including an individual in the image) to recognize the individuals.
    - For example, Covered Components obscure identifying markings such as the face, tattoos, birth marks, scars, and fingerprints. If, after obscuring the individual’s face, the individual’s body is still unique enough to be recognizable, the image is not considered de-identified.

- ii. Covered Components remove all identifying writing from diagnostic images, including the data and time that the image was taken, or any other number assigned to the image for identification purposes.
  - iii. Covered Components de-identify images such that the image cannot be easily restored to its identified state. Common methods such as layering shapes over the image in a computer “paint” program are not sufficient to de-identify the image.
3. In the event that a Covered Component wishes to re-identify the individuals whose PHI is to be disclosed, the Covered Component may assign a unique code to each individual. The code will not be a “specific identifier” as described in procedure 2(a) provided that:
  - The code 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.
  - Covered Components do not use or disclose the code for any other purpose and do not disclose the mechanism for re-identification.
  - Covered Components restrict access to the code to those workforce members who require it.
  - Covered Components do not provide the code to the researcher receiving the de-identified data.
4. The Covered Component consults with the Privacy Officer or Privacy Liaison to ensure that the information or image has been properly de-identified.
  - Note: Workforce members are strictly prohibited from disclosing identifiable data or a unique access code assigned to de-identified data without first consulting with the Privacy Officer or Privacy Liaison.