

UNIVERSITY OF OKLAHOMA

HIPAA Policies

Title: De-Identification /Re-Identification of PHI	Approved: October 8, 2002
Effective Date: April 1, 2003	Last Revised: 2/1/2016;4/1/2018, 2/15/19, 7/22/22

I. PURPOSE

To establish the method and policy for de-identifying and re-identifying Protected Health Information.

II. POLICY*

De-Identified Information/Re-Identification

Health Care Components can Use and Disclose de-identified Protected Health Information, defined below, without complying with the University's HIPAA policies or the HIPAA Regulations as long as the code or other means of re-identification is not disclosed with the de-identified PHI.

Health Care Components may Use Protected Health Information to de-identify it or may Disclose Protected Health Information to a contracted Business Associate to de-identify it for the Health Care Component.

If de-identified information is re-identified, its Use and Disclosure become subject to the HIPAA policies and regulations.

Health Information that does not identify an individual and that there is no reason to believe can be used to identify the individual is “de-identified information” and is not individually identifiable, so it is not considered Protected Health Information. It is not subject to the requirements of the HIPAA Policies or Regulations. Prior to sharing de-identified information outside the University, Health Care Components must either:

- 1) Have IRB approval with authorization to share de-identified data for a research purpose; or**
- 2) Have a data sharing, data use, or limited data set agreement in place signed by an authorized University signatory; or**
- 3) Consult the applicable campus Data Governance Committee or the Clinical Research Informatics Committee.**

III. PROCEDURE

*Capitalized terms are defined in HIPAA *Definitions* Policy

A. De-Identification

NOTE: Regardless of method of de-identification of PHI used below, if the Health Care Component has actual knowledge that the remaining information can be used alone or in combination with other information to identify the patient, the information is not considered de-identified.

Health Information can be de-identified by using one of the two methods listed below:

1. **Removal of Identifiers.** The following identifiers of the patient **or of the relatives, employers, or household members of the patient** are removed and the University, through its campus Covered Entities (“University”), has no actual knowledge that the information could be used alone or with other information to identify the individual:
 - a. Names
 - b. All geographic subdivisions smaller than a state, including street address, city, county, precinct, and zip code and equivalent geocodes, except for the initial 3 digits of a zip code if, according to current publicly available data from the Census Bureau:
 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 3 digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000 (example, for the zip code 73069, all areas using the zip code beginning with 730 have more than 20,000 in the aggregate).
 - c. All elements of dates (except year) for dates directly related to the patient, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age. (Exception: Ages and elements may be aggregated into a single category of age 90 or older.)
 - d. Telephone numbers
 - e. Fax numbers
 - f. E-mail addresses
 - g. Social Security Numbers
 - h. Medical record numbers
 - i. Health plan beneficiary numbers
 - j. Account numbers
 - k. Certificate/license numbers
 - l. Vehicle identifiers, serial numbers, including license plate numbers

*Capitalized terms are defined in HIPAA *Definitions* Policy

Page 2

NOTE: Clinical work performed by dually-employed Workforce Members at the affiliated institution, OU Medicine, Inc. (d/b/a OU Health and OU Health Physicians) must be done in compliance with OU Medicine, Inc. (d/b/a OU Health and OU Health Physicians) policies and procedures.

- m. Device identifiers and serial numbers
- n. Web Universal Resource Locators (URLs)
- o. Internet Protocol (IP) address numbers
- p. Biometric identifiers, including fingerprints and voiceprints
- q. Full face photographic images and other comparable images
- r. All other unique identifying numbers, characteristics, or codes (except as permitted by III B below)

2. Alternative Method of De-Identification. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable must apply those principles and methods and determine 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 the individual who is the subject of the information. The person making this determination must be an *independent third party* and must document the methods and results of the analysis that justify the determination.

B. Re-Identification

A Health Care Component may assign a code or other means of record identification to allow de-identified information to be re-identified (and therefore subject to HIPAA), provided that:

1. Derivation. 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

2. Security. The code and/or mechanism for re-identification is not Used or Disclosed for any other purpose.

IV. REFERENCES

- A. HIPAA Privacy Regulations, 45 CFR 164.502(d)
- B. HIPAA Privacy Regulations, 45 CFR 164.514 (a) – (c)