

# Guidance for Investigators:

## De-Identifying PHI Under The HIPAA Privacy Rule

Covered entities may use or disclose health information that is de-identified without restriction under the HIPAA Privacy Rule. Covered entities seeking to release this health information must determine that the information has been properly de-identified using one of the following methods provided by the Privacy Rule.

### **De-Identification Method 1**

The first acceptable method for de-identifying PHI is to remove all identifiers of the individual and of the individual's relatives, employers, or household members. In addition to removing these identifiers, the covered entity must have no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual. Under this method, the 18 identifiers that must be removed are:

1. Names.
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
  - a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
  - b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. 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 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.
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. Social security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.
14. Web universal resource locators (URLs).
15. Internet protocol (IP) address numbers.
16. Biometric identifiers, including fingerprints and voiceprints.
17. Full-face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

### **De-Identification Method 2**

The second acceptable method for de-identifying PHI is to use statistical methods to establish de-identification instead of removing all 18 identifiers. The covered entity may obtain certification by "a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" that there is a "very small" risk that the information could be used by the recipient to identify the individual who is the subject of the information, alone or in combination with other reasonably available information. The person certifying statistical de-identification must document the methods used as well as the result of the analysis that justifies the determination. A covered entity is required to keep such certification, in written or electronic format, for at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.