DE-IDENTIFICATION OF PHI

Covered entities may use or disclose health information that is de-identified without restriction under the Privacy Rule. Covered entities seeking to release this health information must determine that the information has been de-identified using either statistical verification of de-identification or by removing certain pieces of information from each record as specified in the Rule.

The Privacy Rule allows a covered entity to de-identify data by removing all 18 elements that could be used to identify the individual or the individual's relatives, employers, or household members; these elements are enumerated in the Privacy Rule. The covered entity also must have no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is the subject of the information. Under this method, the identifiers that must be removed are the following:

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.
12. Vehicle identifiers and serial numbers, including license plate numbers.
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.
Re-identification. The covered entity may wish to re-identify information previously de-identified, but is not required to do so. This re-identification may be accomplished through the use of a unique code, key or other means of record identification, provided that the following specifications are met:

- **Code Origin.** The code, key or other means of record identification is not derived from or related to the PHI about the individual, and is not otherwise capable of being translated so as to identify the individual. In other words, the unique code, key or record identifier must not be such that someone other than the covered entity could use it to identify the individual (such as a derivative of the individual’s name or social security number).

- **Code Security.** The covered entity does not use or disclose the code, key or other record identifier for any other purpose, and does not disclose the mechanism for re-identification. The code, key or other record identifier must be kept confidential and secure.

NOTE: If PHI cannot be de-identified, HIPAA Privacy and Security controls must be implemented.