HIPAA DE-IDENTIFICATION

There are two methods to de-identify protected health information (PHI) under HIPAA:

Statistician Method

This method is to have an expert with the appropriate statistical and scientific knowledge for data de-identification certify that the risk for re-identifying individuals is very low.

Safe Harbor Method

An alternative method to de-identify PHI is to remove 18 identifying data elements that HIPAA specifies and have no actual knowledge that the remaining data could be used to identify the individual. Pursuant to HIPAA, "the following identifiers of the individual or of relatives, employers, or household members of the individual, are removed":

1. Names;

2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (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 three digits of a zip code for all such geographic units containing 20,000 or fewer people is 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. Phone numbers;

5. Fax 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 finger and voice prints;

17. Full face photographic images and any comparable images; and

18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)