

HIPAA and PHI

PHI (Protected Health Information) means individually identifiable health information that is created or received by a health care provider, health plan, employer, or health care clearinghouse and that relates to the mental or physical health of the Individual, the provision of health care to the Individual, or Payment for the provision of health care to the Individual. In order to be de-identified, health information must be stripped of all of the following elements:

1. Names;
2. Social Security numbers;
3. Telephone numbers;
4. All geographic 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;
5. 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;
6. Fax numbers;
7. Electronic mail addresses;
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 research data)

A limited data set is described as health information that excludes the direct identifiers listed above, except that may include city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers. A data use agreement is needed to obtain satisfactory assurances that the recipient of the limited data set will use or disclose the PHI in the data set only for specified purposes.

HIPAA and PHI

WAIVER OF AUTHORIZATION

In order to access PHI under a waiver of authorization for research, the IRB must make the following determinations:

1. Use or disclosure involves no more than minimal risk to privacy for the individual based on:
 - (i) a plan to protect patient identifiers from improper use and disclosure;
 - (ii) a plan to destroy patient identifiers at the earliest opportunity, and
 - (iii) adequate written assurances that protected health information will not be reused or disclosed to others except as required by Law, for oversight of the research, or for other research that would be permitted by HIPAA.
2. The research could not practicably be conducted without the waiver;
3. The research could not practicably be conducted without access to protected health information; and
4. A brief description of the PHI necessary to do the research (i.e., minimum necessary); and
5. The privacy risks are reasonable in relation to the anticipated benefits to the individuals and the importance of knowledge gained through research.

DATA USE AGREEMENT

The Privacy Rule requires a data use agreement to contain the following provisions:

1. Specific permitted uses and disclosures of the limited data set by the recipient consistent with the purpose for which it was disclosed (a data use agreement cannot authorize the recipient to use or further disclose the information in a way that, if done by the covered entity, would violate the Privacy Rule).
2. Identify who is permitted to use or receive the limited data set.
3. Stipulations that the recipient will:
 - (i) Not use or disclose the information other than permitted by the agreement or otherwise required by law.
 - (ii) Use appropriate safeguards to prevent the use or disclosure of the information, except as provided for in the agreement, and require the recipient to report to the covered entity any uses or disclosures in violation of the agreement of which the recipient becomes aware.
 - (iii) Hold any agent of the recipient (including subcontractors) to the standards, restrictions, and conditions stated in the data use agreement with respect to the information.
 - (iv) Not identify the information or contact the individuals.