How the HIPAA Rules Affect Clinical Research

How the HIPAA Rules will affect clinical research depends on who you are, where you work, and the type of information you use, collect, or release.

What is identifiable Human Data?

Identifiable data in health care and health/medical research either

1. directly identify an individual through one of the 18 identifiers listed below, **or**
2. enable someone to conclude on a reasonable basis the data can be used to identify an individual, including coded health information.

List of 18 Identifiers

The following identifiers apply to the individual or of relatives, employers, or household members of the individual:

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)

NOTE: Information on providers, including physician or hospital name and contact information is also typically removed due to highly identifiable nature of this information.

How the HIPAA Rules Affect Clinical Research

Identifiable human data and Fred Hutch

FH manages or holds two types of identifiable human data:

1. Data which does not fall under HIPAA; and
2. Data which does fall under HIPAA.
   This data comes from a covered entity. What is a covered entity? It is an entity which:
   a. Furnishes or provides, bills or receives payment for health care (care, services or supplies),
   b. Includes direct providers (physicians, nurses, social workers, pharmacists, etc.) and indirect providers (health plans, pharmaceutical companies, DME suppliers, etc.), even if provided only in clinical trials; **AND**
   c. Electronically transmits health information for a HIPAA "transaction" (billing/admin. for health care)

FH is not a covered entity. However, FH has a single approach to managing any kind of identified human data:

All identifiable human data is considered Strictly Confidential Information under the FH Information Classification standard. FH takes the security and confidentiality of patient/participant data seriously; workforce members are to treat all forms of identified human data is if it is falls under HIPAA.

How to Protect Patient/Participant Data under HIPAA

Removal of 18 identifiers from health information de-identifies the data. One may also use a limited data set. Note, LDS are still considered PHI under federal law.

Alternatively, PHI could be statistically de-identified where a statistician certifies that there is a "very small" risk that the information could be used to identify the individual. (Note: HIPAA does not define "very small". However, Medicare and Medicaid consider cell size of 11 and larger within aggregated data to be de-identified.)

Any code used to replace the identifiers in datasets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed. (See Coded Data) For example, a subject's initials cannot be used to code their data because the initials are derived from their name.

Additionally, the researcher must not have actual knowledge that the research subject could be re-identified from the remaining identifiers in the research study data. For example, data includes the name of a famous hospital, or name of celebrity.

In other words, the information could still be considered identifiable is there was a way to re-identify the individual despite removal of all 18 identifiers.

HIPAA/PHI and Research

How the HIPAA Rules Affect Clinical Research

Regulations allow researchers to access and use individually identifiable human data/PHI when necessary to conduct research. However, HIPAA affects research that uses, creates, or discloses PHI that will be entered in to the medical record or will be used for healthcare services, such as treatment, payment or operations.

Examples of research health information not subject to HIPAA include such studies as

- Those which use of aggregated data
- diagnostic tests that do not go into the medical record because they are part of a basic research study and the results will not be disclosed to the subject
- testing done without the PHI identifiers
- Research studies use data that is person-identifiable because it includes personal identifiers such as name, address, but it is not considered to be PHI because the data are not associated with or derived from a healthcare service event (treatment, payment, operations, medical records), not entered into the medical records, nor will the subject/patient be informed of the results.

Examples of research health information subject to HIPAA include such studies as

- PHI is used in research studies involving review of existing medical records for research information, such as retrospective chart review or use of EHR which is not sufficiently de-identified.
- Studies that create new medical information because a health care service is being performed as part of research, such as diagnosing a health condition or a new drug or device for treating a health condition, create PHI that will be entered into the medical record. For example, sponsored clinical trials conducted by a physician or at a hospital that submit data to the U.S. Food and Drug Administration may involve PHI and are therefore subject to HIPAA regulations.

HIPAA/PHI, Research and Authorization

A researcher may not use PHI without participant/patient authorization – unless the research has a waiver of authorization approved by an IRB. Use of this data under research is restricted to:

Minimal use for intended purposes only.

The researcher must limit PHI to the minimum amount necessary to accomplish the intended purpose. Meaning:

1. A researcher may not use an entire medical record unless it can justify that it is the minimum necessary.

2. Patient consent/authorization (or IRB approval of waiver of consent/authorization) circumscribes the breadth of data usage:

    - The activities the patient (or the IRB approval) has authorized as presented in the protocol's consent/HIPAA authorization are the activities for which the researcher is bound. Any activity with the data beyond what is described to the patient (or approved by the IRB) is unauthorized use of the data. For example, a researcher can not provide his/her data set to another researcher for a different research purpose or a non-research purpose.

    - Unauthorized and unsecured use of PHI within research triggers a HIPAA event, including notification. For example, if a researcher has identified research data on an unsecured laptop or mobile phone, loss or theft of that device triggers a HIPAA-level response.

Accounting of Disclosures

As per the HIPAA regulations, owners of PHI are allowed an accounting of every time their PHI is used/disclosed for 6 years prior to the date of the request.

If a researcher uses data from a covered entity and the protocol has an approved waiver of consent/authorization, the researcher must record and retain an accounting of who's PHI was used. (Note, no accountings are needed when a patient has signed a consent/authorization). It is the responsibility of the PI to maintain this activity. The following information is included in an accounting; suggestions on responses are italicized. (Often researchers state the information below within a spreadsheet and then simply list names of individuals whose data were used.).

Date of the disclosure: *end and start date of the research protocol*
Name of the entity or person who received the PHI: *name of PIs*
Phone Number of the entity or person who received the PHI: *PIs FH phone number*
Email address of the entity or person who received the PHI: *PI FH Address and contact information*
Physical Address of the entity or person who received the PHI: *FH address, with Division, Unit/Lab*
Brief description of the PHI disclosed: *medical record, including pathology, radiology, etc. If different parts of the medical record will be accessed at different times, may simply state "full medical record"*
Brief purpose statement that reasonably informs the individual of the basis for the disclosure: *clinical research, with title of protocol and short description of the protocol.*

Resources:

How the HIPAA Rules Affect Clinical Research

HHS and Research: Special Topics

HHS Research Uses and Disclosures

HIPAA and NIH (recommended)

Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule