HIPAA and Research

Modified: January 2017

Background:

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 protects certain health information, called Protected Health Information or PHI. The Privacy Rule was issued to protect the privacy of health information that identifies individuals who are living or deceased, and balances an individual’s interest in keeping his or her health information confidential with other social benefits, including health care research.

The Privacy Rule applies only to covered entities, which include health care providers like UF Health.

The following topics are intended to provide investigators with information on the most common issues related to HIPAA and research.

Q: Are Authorizations for research uses and disclosures the same as consent?

The Privacy Rule establishes the right of an individual, such as a research subject, to authorize a covered entity to use and disclose his/her PHI for research purposes. This requirement is in addition to the informed consent to participate in research required under the HHS Protection of Human Subjects Regulations and other applicable Federal and State law.

An Authorization differs from an informed consent in that an Authorization focuses on privacy risks and states how, why, and to whom the PHI will be used and/or disclosed for research. An informed consent, on the other hand, provides research subjects with a description of the study and of its anticipated risks and/or benefits, and a description of how the confidentiality of records will be protected, among other things.

Q: May the Authorization and consent form be combined?

At UF and Shands, the Authorization is combined with the informed consent document. The combined UF Consent and HIPAA Authorization includes all of the core elements and required statements in accordance with the Privacy Rule. The study subject only has to sign once, at the end of the combined consent form/Authorization.

At the VA Medical Center, the Authorization is a separate document and requires a separate signature from the study subject.

Q: Are Authorizations always required?

Sometimes, it may not be feasible for a researcher to obtain a signed Authorization for all PHI the researcher needs to obtain for the research study. The Privacy Rule permits waivers or alterations of Authorizations by an IRB or privacy board when certain criteria are met.
Requests for waivers or alterations of the HIPAA authorization must be reviewed and approved by a privacy board established in accordance with the Privacy Rule. UF’s IRB-01 and IRB-02 also serve as the Privacy Board for research involving PHI.

The IRB or privacy board may approve a waiver or alteration of the Authorization for a specific research study, which permits the investigator to collect, use and disclose PHI without the subject’s written authorization. Documentation of this approval must identify the IRB or privacy board that approved the waiver or alteration, the date of the approval, and that the IRB has determined that the request for the waiver or alteration satisfies the following criteria:

1. The use or disclosure of the PHI involves no more than minimal risk to the privacy of individuals based on, at least, the presence of the following elements:
   a. An adequate plan to protect health information identifiers from improper use and disclosure.
   b. An adequate plan to destroy identifiers at the earliest opportunity consistent with conduct of the research (absent a health or research justification for retaining them or a legal requirement to do so).
   c. Adequate written assurances that the PHI will not be reused or disclosed to (shared with) any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of the PHI would be permitted under the Privacy Rule.

2. The research could not practicably be conducted without the waiver or alteration.

3. The research could not practicably be conducted without access to and use of the PHI.

Q: Are reviews preparatory to research permitted under the Privacy Rule?

Preparatory to Research is allowed under the Privacy Rule, and is used only to determine the feasibility of conducting a research project. Such a request is submitted to the IRB on a “Preparatory to Research” form [Link to form] available on the IRB website. For activities involved in preparing for research, covered entities may use or disclose PHI to a researcher without an individual’s Authorization, a waiver or an alteration of Authorization, or a Data Use Agreement (DUA). However, the covered entity must obtain from the investigator, representations that:

1. the use or disclosure is requested solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research,
2. the PHI will not be removed from the covered entity in the course of review, and
3. the PHI for which use or access is requested is necessary for the research.

Any preparatory research activities involving human subjects research as defined by the Common Rule, which are not otherwise exempt, must be reviewed and approved by a UF IRB and must satisfy the informed consent requirements of HHS regulations.

Q: Is Decedent Research permitted under the Privacy Rule?

Decedent Research is allowed under the Privacy Rule. Such requests are submitted to the IRB on a “Decedent Research” form [Link to form] available on the IRB website. To use or disclose PHI of the deceased for research, covered entities are not required to obtain Authorizations from the personal
representative or next of kin, a waiver or an alteration of the Authorization, or a data use agreement. However, the covered entity must obtain from the researcher who is seeking access to decedents’ PHI:

1. oral or written representations that the use and disclosure is sought solely for research on the PHI of decedents,
2. oral or written representations that the PHI for which use or disclosure is sought is necessary for the research purposes, and
3. documentation, at the request of the covered entity, of the death of the individuals whose PHI is sought by the researchers.

Q: Is the use de-identified protected health information permitted under the Privacy Rule?

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.
Covered entities may also 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.

Q: What is a Limited Data Set?

The Privacy Rule permits a covered entity to use and disclose PHI without an Authorization or waiver or alteration of Authorization, if that data constitutes a limited data set (LDS), provided the disclosing covered entity and the recipient of the LDS enter into a Data Use Agreement (DUA). A template DUA is available on the Division of Sponsored Programs (DSP) website. 

Because a LDS includes identifiers, it is still considered PHI, however, certain listed direct identifiers (see below) are excluded. A LDS may include city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers. The direct identifiers listed in the Privacy Rule’s limited data set provisions apply both to information about the individual and to information about the individual’s relatives, employers, or household members.

The following identifiers **must be removed** from health information if the data are to qualify as a limited data set:

1. Names.
2. Postal address information, other than town or city, state, and ZIP Code.
3. Telephone numbers.
4. Fax numbers.
5. Electronic mail addresses.
7. Medical record numbers.
8. Health plan beneficiary numbers.
11. Vehicle identifiers and serial numbers, including license plate numbers.
12. Device identifiers and serial numbers.
13. Web universal resource locators (URLs).
14. Internet protocol (IP) address numbers.
15. Biometric identifiers, including fingerprints and voiceprints.
16. Full-face photographic images and any comparable images.

For more information on HIPAA and Research see the NIH FAQs. 