Series 702 Research and Protected Health Information | Institutional Review Board

The Institutional Review Board from Series 702 of Research and Protected Health Information

Protected Health Information (PHI) is individually identifying information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations (PHI healthcare business uses). Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. PHI relates to physical records, while ePHI is any PHI that is created, stored, transmitted, or received electronically. For the purposes of this Standard Operating Procedure, both ePHI and PHI will be referred to, collectively, as “PHI.” PHI only relates to information on patients or health plan members maintained by a covered entity.

The use of Protected Health Information in research is subject to the requirements contained in the Health Insurance Portability and Accountability Act (HIPAA). The review and exemption or approval of human subjects research involving PHI regulated by HIPAA must be done in a manner that complies with HIPAA’s Privacy Rule (45 CFR 160, 164).

I. Privacy Board

A Privacy Board is a review body that acts upon requests for a waiver or an alteration of the Authorization requirement under the Privacy Rule for uses and disclosures of PHI for a particular research study. A Privacy Board may waive or alter all or part of the Authorization requirements for a specified research project or protocol. A covered entity may use and disclose PHI, without an Authorization, or with an altered Authorization, if it receives the proper documentation of approval of such alteration or waiver from a Privacy Board. The Privacy Board at Utah State University is the Institutional Review Board (IRB).

Before a covered entity at Utah State University can use or disclose PHI for research under a waiver or an alteration of Authorization, it must obtain documentation of approval of the waiver or an alteration of the Authorization requirement by the IRB. It is the PI’s responsibility to provide the USU covered entity with that documentation.

II. Using or Accessing Protected Health Information for Research

The Privacy Rule requires that appropriate systems and safeguards be in place to protect the privacy of the individuals whose medical records are maintained by a covered entity. It establishes five ways a researcher can use that information for research purposes:

1. The conduct of activities preparatory to research;
2. Obtain an Authorization for the Use of PHI from the individual whose records are being sought;
3. Obtain a Waiver of Authorization from the Institutional Review Board for the access, use, or disclosure of PHI
4. Obtain a Limited Data Set via an appropriate Data Use Agreement from the covered entity; or
5. Obtain a completely de-identified data set from the covered entity

All options except for that contained in Sections A and E, above, require a protocol submission to the Institutional Review Board prior to utilizing that option.

III. Activities Preparatory to Research

The HIPAA Privacy Rule contains a provision permitting access and use of PHI for activities preparatory to research (45 CFR 164.512(i)(1)(ii)). This provision permits a covered entity to allow access to and use of PHI to prepare for a research project. Such activities might include examining a covered entity's EMR to ensure sufficient numbers of clients with a particular diagnosis to address a research question the researcher is interested in pursuing. The Privacy Rule provision for activities preparatory to research does not permit a researcher to take that information outside of the covered entity, absent a Waiver of Authorization from the Institutional Review Board.

It is important to note that while the Privacy Rule would permit contact with the individuals whose records are being reviewed, the Common Rule does not. No participants should be contacted about their willingness to participate in a study, under activities preparatory to research, until a protocol has been reviewed and determined exempt or approved by the IRB. The Common Rule, USU Policy, and HRPP accreditation standards require that the IRB review the recruitment plan prior to engagement with human research participants.

IV. Authorizations for the Use of Protected Health Information

An Authorization for the Use of Protected Health Information ("Authorization") should be utilized whenever there are prospective interactions with research participants whose protected health information will be used in a research project. It may be paired with a waiver of Authorization, as discussed below, when appropriate. An Authorization must be reviewed and approved by the USU IRB prior to use with research participants.

If the research involves access, use, or disclosure of psychotherapy notes [1], the only way a research team may access them is via an Authorization. No other avenue exists for the access, use, or disclosure of psychotherapy notes in research, and an Authorization for the Use of Protected Health Information that includes psychotherapy notes cannot be combined with the Informed Consent document; it must separately be provided to the research participant or legally authorized representative.

An Authorization permits the covered entity to release PHI to the researcher as specified in the Authorization. The USU IRB makes a template Authorization available on its website, but this template is not required for use. Researchers should work with the covered entity holding the PHI to ensure that the Authorization they propose to use meets the requirements of the covered entity, many of which have standards for privacy and confidentiality that go above and beyond the baseline requirements of HIPAA.

To be valid under HIPAA, an Authorization must contain the following elements:

- A specific description of the health information that will be accessed and used for the research;
- A specific description of the individuals who will have access to the health information described in that document;
- A statement that the individuals receiving the protected health information, if not a part of that covered entity, may not be required to protect the information in the same manner as the covered entity;
- A statement that if the treatment or intervention being offered is being offered only for research purposes, declining to sign the Authorization may mean that the individual would not receive the treatment or intervention, OR that the researcher cannot refuse or alter treatment on the basis of whether the individual signs the Authorization – whichever is applicable to the individual circumstances of the research;
- When the Authorization expires; and
- A statement that the individual may revoke their Authorization at any time, who they should contact to revoke the Authorization, and (if the researcher chooses and the IRB agrees), that the disclosed information prior to revocation may still be used for the research purposes described in the Informed Consent document.

Additionally, it must be written in "specific" and "plain" language. The template that the USU IRB makes available is written at a 12th grade level, as that encompasses the vast majority of research populations the IRB is tasked with conducting reviews regarding. If the research team plans to involve different populations, they may need to rewrite or substantially alter some of the language used in the template. As with informed consent documents, it must also be understandable to the population being utilized; this may, at times, require professional translation of the document to other languages.

When Protected Health Information is being sought from non-English speakers, the same standards of translation expected by the Sorenson Center for Clinical Excellence are expected to be in place for the research information provided to prospective research participants.

An Authorization must contain the following elements where the elements are relevant or applicable to the research project:

- Any circumstances under which the research team would be required by law to release the health information (e.g. reporting requirements for imminent harm, child abuse, certain mandatorily reportable transmissible health conditions, etc.);
- That the individual's information will not be shared in publications or presentations in an identifiable manner;
- That information released to the researchers can be de-identified to HIPAA standards and made available to others for other purposes; and
- The timing within which the records received by the research team will be made available to the individual granting the Authorization.

V. Waivers and Alterations of Authorizations for the Use of Protected Health Information

The HIPAA Privacy Rule contains provisions for the access, use, and disclosure of PHI without the Authorization of the individual whose information is being sought. Such a process is referred to as a "Waiver" or "Alteration" of the requirement to obtain an Authorization. The Utah State University Institutional Review Board may waive or alter the requirements to obtain an Authorization if the following three criteria can be demonstrated by the Principal Investigator and documented by the IRB:

1. The use or disclosure of Protected Health Information involves no more than a minimal risk to the privacy of those individuals. Specifically:
    a. There is an adequate plan to protect identifying information (as defined by HIPAA) from improper use and disclosure;
    b. An adequate plan exists to destroy identifying information at the earliest opportunity; and
    c. The IRB receives written assurances that the PHI will not be reused or disclosed to any other person or entity, or for any other research purposes by the same people or entities
2. The research could not practicably be carried out without the waiver. Specifically:
    a. It would not be merely difficult to conduct the research without the waiver. The IRB must find and document that obtaining an Authorization presents an extreme and/or unforeseeable circumstance of expense or difficulty
3. The research could not practicably be carried out without access to and use of the PHI being sought.

All of these criteria must be provided by the Principal Investigator, and the IRB must agree with those determinations and document them before granting a waiver or alteration. Additionally, the researcher must demonstrate that the information they will access or use is the minimum necessary information to complete the research project. The minimum necessary standard is addressed in more detail in Section IX, below.

VI. Limited Data Sets & Protected Health Information

The HIPAA Privacy Rule permits a covered entity to use or disclose a Limited Data Set of PHI in research that has been approved or exempted by the Institutional Review Board. The release of a Limited Data Set ("LDS") must be accompanied by a Data Use Agreement ("DUA").

HIPAA establishes a list of distinct identifiers which render health information individually identifiable (plus an "actual knowledge" component which may also render health information individually identifiable). An LDS may only include the following identifiers: city, state, zip code, elements of date, and other numbers, characteristics, or codes that are not listed as direct identifiers in HIPAA. LDS provisions apply both to information about the individual, as well as information about the individual's relatives, employers, or household members. The following identifiers must be removed from the data in order for it to quality as a LDS:

- Names
- Postal address information, other than town or city, state, and zip code
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers

- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers
- Biometric identifiers, including fingerprints and voiceprints
- Full-face photographic images and any comparable images

A valid data use agreement for the release and use of a limited data set must contain at least 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 (i.e. consistent with the protocol submitted to the IRB)
2. Identification of who is permitted to use or receive the limited data set
3. Stipulations that the Principal Investigator will not use or disclose the information other than permitted by the agreement or otherwise required by law
4. Stipulations that the Principal Investigator will use appropriate safeguards to prevent the use or disclosure of the information, except as provided for in the agreement. The disclosing entity must require the Principal Investigator to report to the covered entity (even if they are within the same covered entity) any uses or disclosures in violation of the agreement of which the recipient becomes aware
5. Statements that the Principal Investigator will hold any agent of theirs to the standards, restrictions, and conditions stated in the Data Use Agreement with respect to the information being provided
6. A statement that the Principal Investigator will not attempt to identify the information or contact the individuals

Data Use Agreements should be provided in the protocol submitted to the IRB as soon as possible, which sometimes may be via an amendment after approval has been granted.

VII. De-identification of Protected Health Information

Covered entities may use or disclose health information without restriction under HIPAA if the health information has been deidentified to HIPAA standards. There are two ways to accomplish this:

1. Removal of all 18 HIPAA identifiers plus the inability to reidentify the data using actual knowledge; or
2. Established statistical methods which allows some of the 18 HIPAA identifiers to remain in place, while ensuring reidentification risk is virtually impossible.

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. In other words, the covered entity must be assured that the research team can use “actual knowledge” to reidentify the information they will receive.

Under the de-identification method, the identifiers that must be removed are the following:

- Names.
- 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:
  - The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
  - The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
- 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.
- Telephone numbers.

- Facsimile numbers.
- Electronic mail addresses.
- Social security numbers.
- Medical record numbers.
- Health plan beneficiary numbers.
- Account numbers.
- Certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- Web universal resource locators (URLs).
- Internet protocol (IP) address numbers.
- Biometric identifiers, including fingerprints and voiceprints.
- Full-face photographic images and any comparable images.
- 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.

VIII. Electronic Authorizations

The HIPAA Privacy Rule requires a signature, printed name, and date in order for an Authorization to be effective. HIPAA is silent on the requirements for electronic signatures, and so the USU IRB permits electronic signatures to be utilized for HIPAA Authorizations. Such signatures must be in compliance with the Federal ESIGN Act, which requires verification of the identity of the individual signing. Such verification or authentication can include:

- Two factor or multifactor authentication (such as DUO or Microsoft MFA)
- Identity verification questions (such as requiring a person to verify their DOB or use of security questions such as those contained on myid.usu.edu) or
- Voice verification

In addition, the system used for electronic signatures must provide a signed and timestamped copy to both the signatory as well as the research team. The USU IRB will not approve an electronic Authorization process that does not meet the requirements of the Federal ESIGN Act.

IX. Minimum Necessary Standard

The HIPAA Privacy Rule imposes a “minimum necessary” standard on all permitted uses and disclosures of PHI by a covered entity. This means that the information sought by the research team must be “the information reasonably necessary to accomplish the purpose of [the research.]” The Privacy Rule permits the covered entity to outsource the task of determining the minimum necessary standard to the IRB. Because the USU IRB oversees waivers and alterations for a variety of covered entities, not just those located within Utah State University, it will always independently find and document that the PHI requested by the research team meets the minimum necessary standard.

---

[1]The Privacy Rule defines psychotherapy notes as notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the patient’s medical record. Psychotherapy notes do not include any information about medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, or results of clinical tests; nor do they include summaries of diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.