

Section 26: Privacy and Confidentiality

26.1 Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the first comprehensive act of federal legislation dealing with the privacy of health information. The HIPAA Privacy Rule was created to provide strong protections that do not interfere with patient access to, or the quality of, health care delivery. The entire health care field is affected by the Rule, including research.

Under HIPAA, trial subjects are required to authorize the use and disclosure of their protected health information (PHI). According to the Rule, trial participants have the right to:

1. Access their PHI;
2. Request amendment of their PHI;
3. Receive an accounting of disclosures of their PHI;
4. Request restrictions on the uses and disclosures of their PHI;
5. Request receipt of communications of their PHI by alternative means or at alternative locations; and
6. Revoke their authorization for use and disclosure of their PHI.

Access: Research participants are entitled to access (i.e., inspect and copy) their PHI that is maintained in a designated record set. The Rule defines a designated record set as the provider's health care and billing records about individuals and any records used by the provider to make health care decisions about individuals. Therefore, the designated record set includes PHI that is generated in research and recorded in the medical record or in billing records as well as PHI that is recorded elsewhere, such as the trial files, but is also used to make health care or billing decisions. It is important to note that information that is generated in research and lacks clinical validity or clinical utility generally will be considered outside the designated record set (unless it is recorded in the medical or billing records), and thus the Rule's right of access generally does not apply to such information.

The Rule permits researchers conducting clinical trials to suspend participants' rights of access temporarily, for as long as the research is in progress, if the participant specifically agrees to this suspension in the research authorization. The right of access must be reinstated when the research is complete.

Amend: Research participants are entitled to request that the researcher amend their PHI that is maintained in a designated record set. Participants may only amend PHI to which they have a right of access under the Rule. If the participant's request to amend is granted, the researcher must inform the participant, the people or entities the participant identifies as needing the amendment, and others who may rely on the information of the amendment.

Accounting: Research participants generally are entitled to request a list of disclosures by the researcher of any of their PHI (not limited to PHI in a designated record set) made over the previous 6 years in connection with the research. The right to accounting does not apply to disclosures of PHI made pursuant to the participant's authorization or disclosures of limited data sets. However, the right to accounting does apply to disclosures of PHI made pursuant to a waiver of authorization (even disclosures pursuant to

grand-fathered waivers under the Rule's transition provisions), disclosures of PHI in adverse event reports made without authorization, and disclosures of decedents' PHI.

The accounting of disclosures must contain:

1. The date of the disclosure;
2. The name of the person or entity who received the information, including address; and
3. A brief description of the PHI disclosed and a brief state of the purpose of the disclosure.

The Rule allows a "modified accounting method" for research that involves 50 or more people and for which authorization has been waived. For these large trials, the institution does not have to maintain a list of the specific persons about whom PHI has been disclosed but must make the following information available upon request to any individual who's PHI may have been included:

1. The name and description of all protocols involving 50 or more people for which authorization has been waived, including the purpose of the research and the criteria for selecting records;
2. A brief descriptions of the type of PHI disclosed;
3. The dates or periods during which disclosures occurred;
4. Contact information for sponsors and recipient researchers; and
5. A statement that the individual's PHI may or may not have been disclosed for a particular protocol.

In addition, the hospital or researcher must assist in contacting the sponsor and recipient researcher if it is reasonably likely that an individual's PHI was disclosed to them.

Restrict: Research participants are entitled to request that the researcher restrict the uses and disclosures of their PHI. However, the researcher is not required to agree to the restriction. If the researcher does not agree, the participant can decide whether he or she still wants to participate in the research. If the researcher does agree, the restrictions must be followed except if necessary to provide emergency treatment to the participant. Researchers must also communicate any restrictions to which they have agreed to other individuals or entities to which they permissibly disclose the participant's PHI.

Alternate means or locations: Research participants are entitled to request receipt of communications of PHI from the researcher by alternative means or alternative locations (at a home address versus a work address). The researcher must accommodate such requests if reasonable but may require the participant to specify an alternate address or other method of contact. The researcher may not require the participant to explain the basis of the request.

Revoke: Research participants have the right to revoke their authorization for the researcher to use and disclose PHI in connection with the research, except to the extent that the researcher has already relied on the authorization. As a result, if the PHI has already been used to perform an analysis or other evaluation for the trial, the results of that analysis can be retained but the researcher must notify the IRB regarding the participant's revocation. The researcher may also continue to use the participant's PHI as necessary to account for the participant's withdrawal from the trial or to report adverse events. However, the researcher generally may not use or disclose the PHI in new ways after the revocation. Researchers must inform other individuals or sites involved in the research of any revocation of authorization.

26.2 What Constitutes PHI?

The following are all considered PHI:

- Names
- Addresses
- Dates that directly relate to the individual including birth date, death date, discharge dates
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers
- Medical record and pathology record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- VINs, serial numbers, and license plate numbers
- Device identifiers and serial numbers
- URLs
- IP addresses
- Biometric identifiers including finger and voice prints
- Full-face photographic images and comparable images
- Any other unique identifier, characteristic, or code

26.3 “Minimum Necessary” Standard for Research Activities

The Rule requires that researchers make all reasonable efforts to use or release only the minimum necessary identifiable health care information to achieve the intended purpose. The minimum necessary standard does not apply to treatment-related requests or disclosures of health care information or to situations in which an individual specifically has authorized the use or disclosure.

1. If a researcher obtains written authorization from subjects to use or disclose their PHI, the minimum necessary standard does not apply. However, the authorization must describe in a reasonably specific way what information will be used or disclosed, by whom and to whom, and for what purposes.
2. If the researcher requests that the IRB approve a waiver of individual authorization, then the minimum necessary standard applies. The researcher must describe in the waiver request specifically what health care information is necessary for the research. If the researcher requests

access to electronic health care information, the researcher must identify the fields that will be requested to conduct the research. If the researcher requires access to paper records, then the researcher must identify the specific information that he or she will look for and retain to conduct the research.

3. Researchers using a limited data set must still apply the minimum necessary standard. The researcher must determine what types of data are necessary to conduct the research and must clearly describe those in the protocol submitted to the IRB/Privacy Board.

26.4 De-identified Information for HIPAA Privacy Rule

PHI is considered not identifiable and not covered by the Rule if the information does not identify the individual and there is no reasonable basis for believing the individual can be identified from the information collected. The Rule outlines two ways in which information can be de-identified:

1. A person with appropriate statistical expertise can render information “not identifiable” if he or she can determine that the risk is very small that an anticipated recipient of the information could identify the individual by the information alone or in combination with reasonably available information. This same person must document the methods and results of the analysis to justify this determination; or
2. Alternatively, the following identifiers of the individual and his or her relatives, employers, or household members must be removed:
 - a. Names
 - b. Geographic subdivisions smaller than a state, including street, city, county, precinct, and ZIP code (the first three digits of the ZIP code can be used if its geocode includes more than 20,000 people; if not, then 000 must be used)
 - c. All elements of dates, except year, related to an individual, including birth date, date of admission, discharge dates, date of death (for individuals greater than 89 years of age, year of birth cannot be used – all elements must be aggregated into a category of 90 or older)
 - d. Telephone numbers
 - e. Fax numbers
 - f. Email addresses
 - g. Social security numbers
 - h. Medical record numbers and pathology record numbers
 - i. Health plan beneficiary numbers
 - j. Account numbers
 - k. Certificate/license numbers
 - l. VINs, serial numbers, and license plate numbers
 - m. Device identifiers and serial numbers
 - n. URLs

- o. IP addresses
- p. Biometric identifiers, including finger and voice prints
- q. Full-face photographic images and comparable images
- r. Other unique identifier, characteristic, or code

The IRB and the privacy committee will determine that these issues have been met prior to determining that data have been de-identified.

26.5 The Limited Data Set Option

The HIPAA Privacy Rule allows the use of select types of health care data without triggering all of its requirements. This option is available for research, health care operations, and public health purposes only.

Specifically to use or disclose a limited data set, a researcher does not need an individual's authorization. However, to ensure some privacy protections, researchers must use or disclose only the minimum necessary data to accomplish the purpose of the research.

The IRB will determine upon review whether the limited data set includes identifiable information. The IRB will determine whether consent can be waived.

The Rule defines a limited data set as PHI that excludes the direct identifiers of an individual or of relatives, employers, or household members of the individual previously listed in What Constitutes PHI.

Unlike the de-identified data set, the limited data set permits the inclusion of town, city, state, and ZIP code. The limited data set also allows the use and disclosure of dates.

Important uses and restrictions for limited data sets

1. The limited data set cannot be used to re-identify or contact individuals.
2. The minimum necessary standard applies to the limited data set.
3. The requirement for accounting for all disclosures of PHI does not apply.
4. Researchers using a limited data set must sign a data use agreement.

26.6 Data Use Agreement Requirements

Researchers using the limited data set must agree to a data use agreement that describes the permitted uses and disclosure of the information received and prohibits any attempt to re-identify or contact the individuals.

The data use agreement will:

1. Establish that the data will be used for research and further uses or disclosures are not permitted.
2. State specifically who will be permitted to use or receive the limited data set.

3. Provide that the limited data set recipient will:
 - a. Not use or further disclose the information other than as permitted by the data use agreement or as required by law;
 - b. Use appropriate safeguards to prevent use or disclosure of the information other than as provided in the agreement;
 - c. Report to the covered entity any identified use or disclosure not provided for in the agreement;
 - d. Ensure that any agents, including a subcontractor to whom the limited data sets are provided, agree to the same restrictions and conditions that apply to the recipient; and
 - e. Not identify or contact the individuals.

26.7 Accounting for Disclosures

Investigators and research teams must develop a system to account for disclosures of PHI. This accounting of disclosures must contain:

1. The date of the disclosure;
2. The name of the person or entity who received the information, including address; and
3. A brief description of the PHI disclosed and a brief state of the purpose of the disclosure.

This accounting must be maintained for six years. Participants may ask for an accounting of information unless they signed an authorization form within the consent form.

The Rule allows a modified accounting method for research that involves 50 or more people and for which authorization has been waived. For these large trials, the institution does not have to maintain a list of the specific persons about whom PHI has been disclosed, but it must make the following information available upon request to any individual whose PHI may have been included:

1. The name and description of all protocols involving 50 or more people for which authorization has been waived, including the purpose of the research and the criteria for selecting records;
2. A brief descriptions of the type of PHI disclosed;
3. The dates or periods during which disclosures occurred; and
4. Contact information for sponsors and recipient researchers and a statement that the individual's PHI may or may not have been disclosed for a particular protocol.

In addition, the hospital or researcher must assist in contacting the sponsor and recipient researcher if it is reasonably likely that an individual's PHI was disclosed to them.

26.8 Research on Deceased Persons

Identifiable health information of deceased individuals, including deceased participants in research, is protected by the Rule. The Rule extends privacy rights to decedents even though decedents are not considered human subjects protected under the Common Rule (regulations governing human participants research). Specifically, the Rule allows researchers to access identifiable health information of decedents without obtaining participants' or their representatives' authorization, but only if a covered institution obtains certain assurances from the research with regard to that access. These assurances are that the:

1. Requested use and disclosure is solely for research on the protected health information of decedents; and
2. PHI for which use or disclosure is sought is necessary for research purposes.

For research using PHI from deceased persons, the IRB/Privacy Board will review the protocol. The investigator will be asked to document the following in the application:

1. Statement that the records are needed for research and will be used solely for research.
2. Entities (i.e., DFCI, Partners) may request documentation of deaths. Therefore, investigators should be prepared to provide such documentation upon request.
3. In cases when all participants are deceased, a waiver of consent and authorization will be granted if the investigator can show how the research meets those requirements.
4. In cases where a participant had been living but then dies during the course of the trial and authorization was obtained for purposes of the trial, the authorization will cover such continued use/disclosure.
5. Disclosures of decedent information must be tracked in accordance with the accounting requirements of the Rule.

26.9 Waiver of Authorization for Research

Investigators will be required to apply for both a waiver of consent and a waiver of authorization to meet both requirements.

The criteria for demonstrating that this request is reasonable are listed below. The criteria for a Waiver of Authorization [[45 CFR 164.512\(I\)\(2\)\(ii\)](#)] are:

1. The trial involves no more than minimal risk.
2. The waiver or alteration will not adversely affect the rights and welfare of the research participants.
3. The research could not practicably be carried out without the waiver of consent or alteration to the consent information.
4. Whenever appropriate, the participants will be provided with additional pertinent information after participation.
5. This trial involves no more than minimal risk to privacy:

- The protocol includes an adequate plan to protect identifiers from improper use or disclosure.
 - The protocol includes an adequate plan to destroy the identifiers at the earliest opportunity. Identifiers may be maintained if there is a health or research justification or if law requires retention. The investigator must document such a justification and submit it to the IRB/Privacy Board for review and approval.
 - The protocol must include adequate written assurances that the identifiable information will not be reused or disclosed except as required by law, for authorized oversight of research, or for other research for which the use and disclosure would be permitted.
6. The research could not practicably be conducted without access to the use of this identifiable information.