Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) contains provisions to protect the confidentiality and security of personally identifiable information that arises in the course of providing health care and research. The intention of HIPAA is to protect the privacy rights of patients including the prevention of inappropriate disclosures of Protected Health Information (PHI) that can cause harm to a person's reputation, insurability, employability, etc.

The DFCI IRB acts as the HIPAA Privacy Board for research occurring within DF/HCC. The Privacy Board reviews and approves the use of PHI in research and may act upon requests for a waiver or an alteration of the Authorization requirement under the Privacy Rule. PHI is private information that is subject to special treatment under the HIPAA Privacy Regulations. PHI can only be used or disclosed in research if one of the following applies:

1. Written Authorization for the use and disclosure of PHI has been obtained from the patient-participant.
2. DFCI IRBs receive a satisfactory representation from the investigator that the research involves only a Review Preparatory to Research.
3. DFCI IRBs approve and document a formal Waiver or Alteration of Authorization.
4. DFCI IRBs receive a satisfactory representation from the investigator that the research involves only Decedents' Information.
5. DFCI IRBs determine that the research involves only a Limited Data Set(s) accompanied by a Data Use Agreement.
6. DFCI IRBs determine that the research involves only deidentified information.

Privacy Rule requirements are in addition to human subject protection requirements. The following chart provides a brief overview of the six mechanisms identified above:

Mechanism	Minimum Necessary Standard	Accounting of Disclosures	Submission Requirements	Documentation Requirements	Retention Requirements
Authorization	Does Not Apply	No	IRB for processing	Patient-Participant Authorization(s)	6 years
Waiver/Alteration of Authorization	Applies	Yes, but simplified if 50 or more individuals	IRB for required determinations	IRB Documentation	6 years
Review Preparatory to Research	Applies	Yes, but simplified if 50 or more individuals	IRB for approval	PI Representation & IRB Approval	6 years
Research Using Decedents' Info	Applies	Yes, but simplified if 50 or more individuals	IRB for approval	PI Representation & IRB Approval	6 years
Research Using De-Identified Info	Does Not Apply	No	IRB for approval	PI Representation (or Statistician's Determination) & IRB approval	6 years
Research Using Limited Data Set	Applies	No	IRB for approval	PI Representation & Data Use Agreement & IRB approval	6 years

Minimum Necessary Standard. A Covered Entity must use, disclose, or request the least amount of information needed for the intended purpose. If the entire medical record is desired, it must be justified as the minimum necessary. Although the Minimum Necessary Standard does not apply to uses or disclosures under an authorization, all uses and disclosures are limited to the purposes described in the authorization.

Accounting for Disclosures. The Privacy Rule generally grants individuals the right to a written "Accounting of Disclosures" of their PHI made in the six years prior to their request for an accounting. Accountings are required for disclosures made under a waiver of authorization, research on decedents' information, and reviews preparatory to research.

PHI from Other Covered Entities. DF/HCC institutions have entered into an "Organized Health Care Arrangement." Under the agreement, the sharing of PHI between DF/HCC sites for DF/HCC supported research is not considered sharing outside of this Covered Entity. Investigators must observe the Privacy Rule requirements of any Covered Entity from which they access PHI. If the investigator removes PHI from another Covered Entity, then the DF/HCC Privacy Rule requirements also apply. Privacy Rule requirements are in addition to any human subject protection requirements with the DF/HCC and the other entity.

This guidance covers each of the above circumstances, as well as additional considerations for the use of PHI in research and general FAQs.

Written Authorization for the use of PHI

The HIPAA Privacy Rule requires written authorization for use or disclosure of PHI for the purposes of research. If no PHI is used during the research, HIPAA may not apply to the study.

The DF/HCC institutions have provided approved HIPAA authorization language in the written consent form templates. This language contains the six required elements of authorization, as well as the three required statements, enumerated below. In some circumstances, this authorization may be updated to be appropriate to the context of the research, provided all elements and statements are provided for review. OHRS can provide guidance on whether this language may be altered for a specific research protocol.

The Authorization Core elements and Required Statements that are mandated by HIPAA are enumerated in 45 CFR 164.508.

The following six elements are required in the HIPAA authorization:

1. A specific and meaningful description of the information to be used or disclosed.
2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
3. The name or other specific identification of the persons(s), or class of persons, to whom the covered entity may make the requested use or disclosure (i.e., the intended recipients).
4. Description of each purpose of the requested use or disclosure. (A brief introduction of the clinical research study should work).
5. Must contain an expiration date or an expiration event that is related to the individual or the purpose of the use or disclosure. (For research purposes, statements such as 'end of research study' or 'no expiration date' will satisfy this requirement).
6. The signature of the individual and the date (If the Authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must be provided).

The following three Required Statements are also required:

1. Individual's right to revoke the Authorization in writing (subject to the reliance exception, which permits the continued use and disclosure of PHI already obtained.
2. Clarification that the covered entity is not permitted to condition the provision of treatment on the execution of a valid Authorization. However, for Authorizations granted for research

purposes, covered entities are permitted by the Privacy Rule to condition the provision of research related treatment on the execution of a valid Authorization.
3. An explanation that there is a potential that the information may be re-disclosed by the recipient of the information and that the recipient may not be required to comply with the Privacy Rule.

Different platforms may be used to obtain valid electronic signatures. If your study is FDA-regulated and obtaining HIPAA authorization, the platform must be secure and compliant with 21 CFR Part 11 (sometimes referred to as "Part 11"). If you are conducting a FDA-regulated study and utilizing an electronic platform to collect research signatures, assurances must be made that the platforms are Part 11 compliant.

Preparatory to Research Provision

During recruitment, researchers often review medical records, clinic appointment logs, and other documents to identify and confirm eligible participants. The process of screening participants in this manner constitutes use or disclosure of PHI and is covered by the HIPAA Privacy Rule.

Under the provision, a researcher who is an employee or a member of the covered entity's workforce is able use PHI to contact prospective research subjects. However, when using PHI in preparation for research, PHI must not be removed from the covered entity's site. As such, DF/HCC institutions have entered an "Organized Health Care Arrangement." Under the agreement, the sharing of PHI between DF/HCC sites for DF/HCC supported research is not considered sharing outside of this Covered Entity. Covered health care providers and patients may discuss the option of enrolling in a clinical trial without patient authorization, and without a waiver of authorization granted by the Privacy Board.

Because of the preparatory to research provision, DF/HCC researchers ***do not*** need to request a partial HIPAA waiver to access medical records for recruitment purposes. This provision extends to all members of the workforce, not just treating physicians if:

- the sole purpose of the record review is to identify prospective research participants;
- the patient information to be reviewed is necessary to identify prospective participants for the study; and
- neither the patient records nor any patient-identifiable information will be copied or removed from the DF/HCC entities (e.g., the patient identifiers are not written down, or if so, the PHI is saved in a manner that it represents only a limited dataset).

Please Note: Per the preparatory to research provision, personnel at DF/HCC sites may access PHI, but the information may not be removed or shared externally from DF/HCC sites, and IRB approval is required. Only members of the workforce at DF/HCC sites may contact prospective research participants under this option. Prospective participants may not be contacted by sponsors or any other persons who are not personnel of the covered entity.

A researcher who is not a part of the covered entity may not use the preparatory research provision to contact prospective research subjects. Should the PHI used for research purposes need to be shared outside the institution, the IRB as the Privacy Board may permit a partial waiver of authorization for the purposes of allowing a researcher to obtain protected health information as necessary to recruit potential research subjects (please see the following section). For example, even if an IRB does not waive informed consent and individual authorization for the study itself, it may waive such authorization to permit the disclosure of protected health information as necessary for the researcher to be able to contact and recruit individuals into the study.

If the screening information is to be shown or given to the sponsor or collaborators other than in a deidentified format, a request for Waiver of Authorization must submitted.

Formal Waiver or Alteration of Authorization

The IRB may approve a waiver or alteration of HIPAA Authorization provided that the research meets the criteria outlined in 45 CFR 164.512(i)(2)(ii).

1. The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;
    a. An adequate plan to protect the identifiers from improper use and disclosure;
    b. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
    c. Adequate written assurances that the protected health information will not be reused or disclosed to 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 protected health information would be permitted by this subpart;
2. The research could not practicably be conducted without the waiver or alteration; and
3. The research could not practicably be conducted without access to and use of the protected health information

Partial HIPAA Waiver of Authorization

The IRB may approve a waiver of the requirement for signed HIPAA Authorization provided the research meets the criteria for waiver as described above. The most common waiver to obtain HIPAA Authorization is issued when consent is not required for screening procedures limited to:

- obtaining information through oral or written communication with the prospective subject or legally authorized representative, or
- obtaining identifiable private information or identifiable biospecimens by accessing records or stored identifiable biospecimens.

Demonstrating that the "research could not practicably be conducted without the waiver or alteration" is the main obstacle to approving a partial waiver of authorization. If the subject is physically present, it is usually practicable to obtain written HIPAA Authorization. Research teams may request a Partial HIPAA waiver in circumstances where their recruitment activities are not covered by the Preparatory to Research Provision.

Waiver of HIPAA Authorization

The IRB may approve a waiver of the requirements for HIPAA Authorization to use and disclose protected health information. The most frequent situation where the IRB approves a full waiver of HIPAA is when the research also qualifies for a waiver of the requirements for consent. Both waivers must demonstrate that it would not be practicable to conduct the research without the waiver, so if the research qualifies for one waiver, it will usually qualify for the other. A full Waiver of HIPAA Authorization is often provided for retrospective studies using existing PHI.

Research on Decedent's Information

The Human Subject Protection regulations apply to research involving "living human beings." Accordingly, Human Subject Protection requirements typically do not apply to research involving decedents unless the research also involves information that identifies living individuals. However, the Privacy Rule does apply to decedents' information. Researchers have the following options to meet the Privacy Rule requirements:

DF/HCC investigators can submit a **representation that the research involves Decedents' Information** to the DFCI IRB when all of the following circumstances are satisfied:

- The information is solely for research on the protected health information of decedents; AND
- Documentation of the death of such individual is available at the request of the covered entity; AND
- The protected health information is necessary for the research.

Decedents' Information may also be accessed through use of a Waiver of Authorization, a Limited Data Set, or a De-identified Data Set.

Limited Data Sets

A Limited Data Set is a limited set of identifiable patient information as defined in the HIPAA Privacy Regulations. A Limited Data Set of information may be disclosed to an outside party without a patient's authorization if certain conditions are met. First, the purpose of the disclosure may only be for research, public health or health care operations. Second, a Data Use Agreement must be negotiated between the parties prior to sharing the Limited Data Set. This agreement has specific requirements which are discussed below.

A Limited Data Set is information from which direct identifiers have been removed. All of the following identifiers must be removed to meet the requirements of a Limited Data Set:

- names;
- street addresses (other than town, city, state and zip code);
- telephone numbers;
- fax numbers;
- e-mail addresses;
- Social Security numbers;
- medical records numbers;
- health plan beneficiary numbers;
- account numbers;
- certificate license numbers;
- vehicle identifiers and serial numbers, including license plates;
- device identifiers and serial numbers;
- URLs;
- IP address numbers;
- biometric identifiers (including finger and voice prints); and
- full face photos (or comparable images).

The health information that may remain in the information disclosed includes:

- dates such as admission, discharge, service, DOB, DOD;
- city, state, five digit or more zip code; and
- ages in years, months or days or hours.

It is important to note that this information is still considered PHI; the data would not be considered deidentified, therefore is still subject to HIPAA regulations.

Deidentified Data Sets

Many studies involve the collection and use of existing deidentified health information, often from a data registry or tissue repository. It is very important to distinguish deidentified information (as defined under the HIPAA Privacy Rule) from "non-identifiable" or "anonymous" information (as used under the human subject protection regulations). In the case of "non-identifiable" or "anonymous" information, there is no way to link the information to the individual from whom it was derived. However, deidentified information may include a code or link that permits the information to be reidentified, i.e., linked back to the individual from whom it was derived. Thus, deidentified information is potentially identifiable and cannot be considered anonymous from a human subject protection standpoint.

A deidentified data set is a data set that does not identify any individual that is a subject of the data, nor does it provide any reasonable basis for identifying any individual that is a subject of the data. Deidentified data sets do not include any PHI, and therefore are not subject to the HIPAA regulations. In order to deidentify a dataset, the data may not contain any of the following:

- Names

- 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:
    - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is 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
- Fax 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 finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

Additional Considerations

Research Waiving Documentation of Consent. The DF/HCC consent template has the HIPAA authorization language built into the document. However, there are cases in research where written consent may be waived. While written documentation of consent may not be required for minimal risk research, it must still be impracticable to gain written authorization in order to waive HIPAA authorization. Therefore, there may be some circumstances where a signature on a consent document is not required, but a signed HIPAA authorization is still required. The following steps may be taken to get HIPAA authorization.

- Create a standalone HIPAA authorization form.
- Request the HIPAA authorization form be signed via mail and returned.
- Have the HIPAA authorization signed at a later date (e.g., when the participant is in clinic).
- Use a Part 11 compliant electronic consent portal to have participants sign only the HIPAA authorization.

Online Research. Research not subject to Part 11 Compliance (e.g., non-FDA regulated research or social behavioral research) is still governed by the HIPAA Privacy Regulations. This means that HIPAA authorization must still be obtained to use or disclose PHI. The Privacy Officer has indicated that participants may provide their typed name followed by a statement such as the following, in lieu of a part 11 compliant electronic signature:

"By checking this box and typing my name below, I am electronically signing the HIPAA Authorization to allow for the research team to access my medical records."

Overview of Accounting of Disclosures

Accounting of Disclosures. The Privacy Rule generally grants individuals the right to a written "Accounting of Disclosures" of their Protected Health Information made in the six years prior to their request for an Accounting. Accountings do not go back before April 14, 2003. In general, an Accounting of Disclosures must be provided within 60 days of receipt of the request.

Required Accountings. According to the Privacy Rule, an Accounting of Disclosures is required for:

1. Routinely Permitted Disclosures (e.g., under public health authority, to regulatory agencies, to persons with FDA-related responsibilities) with limited exceptions (e.g., law enforcement, national security, etc.)
2. Disclosures made pursuant to:
    a. Waiver of Authorization
    b. Research on Decedents' Information
    c. Reviews Preparatory to Research

Elements of Accounting. When an Accounting of Disclosures is made, the Accounting must include the following elements:

1. All Disclosures of the individual's Protected Health Information made by the Covered Entity, including Disclosures to or by the Covered Entity's Business Associates
2. Date of each Disclosure
3. Name and address, if known, of the person or entity receiving the information
4. Brief description of the Protected Health Information disclosed, and
5. Brief statement of the purpose of and basis for the Disclosure, or a copy of the written request for the Disclosure.

Elements of Simplified Accounting for Multiple Disclosures to the Same Person/Entity. Where multiple Disclosures of an individual's Protected Health Information have been made to the same person or Entity for a single purpose, a full Accounting of the first Disclosure is required as described in the section above. Accounting for subsequent Disclosures may be accomplished by providing the following:

1. The frequency, periodicity, or number of Disclosures made.
2. The date of the last Disclosure.

Elements of Simplified Accounting of Disclosure of Protected Health Information for 50 or More Individuals. Where Disclosures of Protected Health Information for 50 or more individuals have been made for a single purpose, the Accounting may be accomplished by providing the following:

1. Name of the protocol or research activity
2. Brief description of the purpose of the research and criteria for record selection.
3. Brief description of the type of Protected Health Information disclosed.
4. Dates or time periods when Disclosure may have taken place.
5. Name, address, and phone number of sponsoring entity and research investigator.
6. Statement as to whether other Disclosures of the individual's Protected Health Information have been made.

HIPAA FAQs

1. How does written authorization differ from informed consent?

Informed consent is specified by required elements that ensure that the subject understands the nature of the research and its risks and potential benefits and agrees to participate in research. A participant's written Authorization is for the use and disclosure of PHI in the course of research that are not otherwise permitted under the Privacy Rule. An authorization specifies a set of core elements, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed.

There are circumstances where HIPAA authorization, but not a signed consent, may be required. This is often the case in minimal risk research where the IRB can waive the requirement that participants sign a consent form. In these cases, the research team must consider options for having participants sign the HIPAA authorization.

2. For my study overseen by the FDA, the study sponsor has asked for changes to the HIPAA authorization language in the DF/HCC template. Can we make those changes?

No. The language in the DF/HCC template has been approved by the HIPAA Privacy Officer and may not be changed. DF/HCC is the covered entity, and as such, has both the responsibility and the liability for complying with the HIPAA privacy rule, rather than the sponsor.

3. Do I need to HIPAA authorization to do study recruitment?

It depends.

If the investigator plans to conduct recruitment by monitoring the medical records of patients within their own clinic, then HIPAA authorization is not required for those recruitment purposes. The participants will have an opportunity, at the time of consent, to provide HIPAA authorization for participation in the study itself.

If the investigator intends to screen potential subjects for eligibility by asking them questions, these questions are considered part of the research. Consent and HIPAA authorization may have to be obtained for screening procedures.

4. As part of my protocol, I am indicating that I am relying on the Preparatory to Research provision so that I can review my records to identify how many potential subjects are in my clinic. What information, if anything can I retain when I'm done?

The data collected must be limited to the minimum necessary to meet the objectives of the Work Preparatory to Research (e.g., establish feasibility, plan the study, identify potentially eligible subjects, etc.). Study data may not be collected, but the investigator may retain names and contact information to be used, after the study is approved by the IRB, for recruitment purposes.

5. I am conducting a secondary use study, and there are decedents whose records will be included amongst those in the study; do we need to file the Decedents HIPAA Attestation?

The HIPAA attestation for the use of decadents PHI is only for research that will be exclusively limited to decedents. The attestation provides a means for the investigator to attest to their intent to adhere to the requirements of HIPAA related to the use of decedents PHI. The IRB receives the investigators attestation and checks it for appropriateness; it does not issue an approval. The investigator will receive the IRB's acknowledgment of receipt. If decedents PHI is used as part of a study that also enrolls human subjects, the investigator can request a waiver of HIPAA authorization for the use of decedents PHI.

6. When would I need a Data Use Agreement?

A data use agreement is needed when a researcher is conducting research using a limited data set with someone not otherwise involved in the research protocol (i.e., someone who is not mentioned as receiving PHI in the Authorization or in the waiver of Authorization approved by the IRB). If the person or entity at the other site is part of the trial and is included in the Authorization or waiver of Authorization approval for the trial, you do not need a data use agreement. Rather, a data use agreement is used when, for example, you want to share a limited data set of research data with a colleague at another institution not involved in the trial, or with a private registry not involved in the study.