HIPAA Privacy Rule Guidance for Brown University Researchers

Last Updated: July 2019

The **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** and its regulations, including the Privacy Rule and the Security Rule, as well as the Health Information Technology for Economic and Clinical Health (HITECH) Act, govern the way certain health information is collected, maintained, used, and disclosed. The Privacy Rule establishes a set of safeguards around certain types of health information known as Protected Health Information (PHI) and sets forth a national minimum level of protection for PHI. It also describes ways in which a Covered Entity can use or disclose PHI for research purposes.

Brown University is not a Covered Entity under HIPAA for the purpose of research. As a Brown researcher, you may wish to receive PHI from a Covered Entity and therefore must understand your obligations to ensure that PHI is released to you in a manner that complies with HIPAA and that you appropriately protect those data at Brown once received.

When PHI is communicated inside of a Covered Entity, this is called a **use** of the information. When PHI is communicated to another person or organization that is not part of the Covered Entity, this is called a **disclosure**. HIPAA allows both use and disclosure of PHI for research purposes, but such uses and disclosures must adhere to HIPAA regulations and be part of a research plan that is reviewed and approved by an Institutional Review Board (IRB) or a Privacy Board.

This Guidance provides information to assist the Brown research community with understanding the relationship between PHI that is covered by HIPAA and research. This includes describing various ways in which PHI may be obtained and used for research purposes and the compliance obligations of the Brown research community related to the use of PHI in research.

### Definitions

**Authorization:** Under HIPAA, the granting of rights to access PHI. Authorization is required by HIPAA for disclosures or uses other than for Treatment Payment Operations (TPO), which are covered in the Notice of Privacy Practices. Treatment cannot be conditioned on granting of an authorization. An authorization is a specific, detailed document requesting patient-subject permission for the use of covered PHI.

**Covered Entity:** An organization (e.g., a health plan, a health care clearinghouse, or a health care provider) that must comply with HIPAA. Brown University is not a Covered Entity for the purpose of research. However, a Brown Principal Investigator (PI) may wish to receive PHI from
a Covered Entity to conduct research at Brown, and therefore must understand the obligations to ensure that such data are released to the PI/Brown in a manner that complies with HIPAA and that the data are appropriately maintained and ultimately destroyed at Brown.

**Disclosure:** The release, transfer, provision of access to, or divulging in any other manner of PHI outside the Covered Entity holding the information. Disclosure of PHI requires a specific authorization under HIPAA except if disclosure is related to the provision of TPO (Treatment Payment Operations) of the entity responsible for the PHI or under a limited set of other circumstances, such as public health purposes.

**Minimum Necessary Standard:** The least information reasonably necessary to accomplish the intended purpose of the use, disclosure, or request of PHI. For both healthcare and for research, HIPAA requires that PHI be communicated on a need to know and minimum necessary basis.

**Protected Health Information (PHI):** any individually identifiable health information collected or created as a consequence of the provision of health care by a Covered Entity, whether verbal or recorded in any form or medium (e.g., narrative notes; X-ray films or CT/MRI scans; EEG / EKG tracings, etc.), that may include demographic information. PHI identifies the individual directly or contains sufficient data so that the identity of the individual can be readily inferred.

### What Types of Activities Are Considered Research?

The HIPAA Privacy Rule is primarily concerned with information generated in the course of providing health care services. However, HIPAA does recognize and endorse the fact that some research may create, use, and disclose PHI.

The Privacy Rule also defines the means by which individuals will be informed of uses and disclosures of their PHI for research purposes, and their rights to access information about them held by Covered Entities. Where research is concerned, the Privacy Rule protects the privacy of individually identifiable health information, while at the same time ensuring that researchers continue to have access to medical information necessary to conduct vital research.

In order for HIPAA rules to apply to a research project, it is first necessary to determine if the activity meets the federal definition of research as defined by the Common Rule (45 CFR 46), which is *a systematic investigation designed to contribute to generalizable knowledge*.

### Research that is covered by HIPAA

HIPAA affects research which uses, creates, or discloses PHI. In general, there are two ways a research study would involve PHI:

1. The study involves review of medical records as one (or the only) source of research information. Retrospective studies involve PHI in this way. Prospective studies may do this also, such as when a researcher contacts a participant's physician to obtain or verify some aspect of a person's health history.
2. The study creates new medical records because as part of the research a health-care service is being performed at a Covered Entity, such as testing of a new way of diagnosing a health condition or a new drug or device for treating a health condition.

There are two critically important points that are often overlooked when evaluating whether health information collected during the course of research is subject to HIPAA requirements:

1. Health information obtained by the researcher directly from the research subject (i.e. self-report) solely for research purposes does not require the researcher to follow the HIPAA Privacy Rule because that information is not being obtained from a Covered Entity.

2. However, if researchers are not obtaining medical record information but are placing research results into the subject’s medical record at a Covered Entity, HIPAA compliance is required.

### Use and Disclosure of PHI for Research

HIPAA permits the use or disclosure of PHI for research under the following circumstances and conditions:

1. If the subject of the PHI has granted specific written permission for the use of PHI for research through an Authorization; OR

2. If the IRB has granted a waiver of the authorization requirement; OR

3. If the PHI has been de-identified in accordance with the standards set by HIPAA (and, therefore, no longer meets the definition of PHI); OR

4. If the information is released in the form of a limited data set, with certain identifiers removed, and with a data use agreement between the researcher’s organization (Brown) and the Covered Entity.

The following information describes in detail how PHI may be used or disclosed for research purposes.

### I. Obtaining Authorization to Use PHI

The principle of respect for persons means that, if it is feasible to get the consent of someone before using their PHI for research, then consent should be obtained.

HIPAA refers to consent for use of information as an “Authorization,” and requires that the following elements be present in an Authorization to use PHI for research purposes:

- A description of information to be used or released; and
- The name of person(s) or class of persons (e.g., project staff) who will use the information; and
• The name of persons or organizations to whom PHI will be released. (e.g., central coordinating offices of multi-center trials); and
• The expiration date or event that ends authorization to use PHI (e.g., completion of the research), or statement that authorization does not expire; and
• A statement that the research participant has the right to revoke authorization (as part of withdrawal from study procedures); and
• A statement that if information will be disclosed to other organizations the information may no longer be protected.
• A statement that individuals may inspect or copy their records. The researcher may stipulate that records will not be available until after the study is complete.

A. The PI of the study is responsible for identifying and complying with all HIPAA policies and procedures, as well as applicable State or Federal regulations governing access to PHI. This includes the responsibility to describe to the Brown IRB all proposed access to PHI which will occur during the course of the research, i.e. access to paper and electronic medical records for the purpose of subject identification or screening, any intended addition of information into medical records, and any collection or use of human specimens with individually identifiable health information attached.

B. Brown created an “Authorization to Use Protected Health Information in Research” form to be presented to the study participant for review and to provide permission for access to their PHI.

When participants in a research study sign an Authorization to have a copy of their PHI used for research purposes, the information transcribed into the research record is subsequently governed by the terms of their Authorization and is no longer PHI subject to HIPAA. Although the HIPAA Privacy Rule no longer applies to this information as it is maintained in research records, best practices for research involving human subjects requires that the confidentiality of the information continue to be protected.

II. Waiver of Authorization

The Privacy Rule permits Covered Entities to use and disclose PHI without Authorization for certain types of research activities. For example, PHI can be used or disclosed for research if the Covered Entity obtains documentation that an IRB or Privacy Board has waived the requirement for Authorization or allowed an alteration to Authorization.

A. In many situations, research cannot be conducted using health information that has been de-identified and it may not be feasible to obtain a signed Authorization for all PHI needed for the conduct of your research. Therefore, the Privacy Rule contains criteria for waiver, partial waiver or alterations of Authorizations by an IRB, or by another review body called a "Privacy Board."

B. For disclosure of PHI for research purposes, an IRB or Privacy Board may approve a waiver or an alteration of the Authorization requirement in whole or in part.

A complete waiver occurs when the IRB or Privacy Board determines that no
Authorization will be required for a Covered Entity to use and disclose PHI for a particular research project.

A partial waiver of Authorization occurs when an IRB or Privacy Board determines that a Covered Entity does not need Authorization for all PHI uses and disclosures for research purposes, such as disclosing PHI for research recruitment purposes. An IRB or Privacy Board may also approve a request that removes some PHI, but not all, or alters the requirements for an Authorization (an "alteration").

C. Documentation of the waiver or alteration of Authorization must include a statement identifying the IRB or Privacy Board that made the approval and the date of approval. Among other things, the documentation must also include statements that the IRB or Privacy Board has determined that the waiver or alteration of Authorization, in whole or in part, 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:
   - An adequate plan to protect health information identifiers from improper use and disclosure.
   - 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).
   - 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; **AND**

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 PHI.

D. Many research projects take place at multiple sites and/or require the use and disclosure of PHI created or maintained by more than one Covered Entity. The Privacy Rule does not require approval of a waiver or an alteration of Authorization by more than one IRB or Privacy Board; a Covered Entity may rely on a waiver or an alteration of Authorization approved by any IRB or Privacy Board, without regard to the location of the approver.

E. In order for the Brown University IRB to consider approving a waiver of authorization, it is the PI’s responsibility to complete the “Waiver or Alteration of HIPAA Research Authorization” Appendix and submit it with your IRB Application.
III. De-Identified Data: Research that is not covered by HIPAA

Health information that has been de-identified may be used or disclosed without restriction under the HIPAA Privacy Rule (the health information is no longer PHI). Health information that is de-identified can be used and disclosed by a Covered Entity without Authorization or any other permission specified in the Privacy Rule. There are two ways to de-identify data:

1) The Safe Harbor Method
This method provides that **all** of the following elements are removed from a data set:

- Name
- All geographic subdivisions smaller than a state (street address, city, county, precinct)
  *Note: zip code or equivalents must be removed, but can retain first 3 digits of the geographic unit to which the zip code applies if the zip code area contains more than 20,000 people*
- Dates directly related to individual, all elements of dates, except year (date of birth, admission date, discharge date, date of death)
- All ages over 89 or dates indicating such an age
- Telephone number
- Fax number
- Email address
- Social security number
- Medical record number
- Health plan number
- Account numbers
- Certificate or license numbers
- Vehicle identification/serial numbers, including license plate numbers
- Device identification/serial numbers
- Universal Resource Locators (URLs)
- Internet Protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographs and comparable images
- Any other unique identifying number, characteristic, or code. (This effectively is a “catch-all” provision and is intended to include items that are not otherwise specified but could make a data set identifiable.)

2) Statistical Method
Using the Statistical Method, certification is provided by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable so that there is a “very small” risk that the information could be used by the recipient to identify the individual.

IV. Limited Data Set with a Data Use Agreement

When only certain identifiers are needed, a Covered Entity may provide a researcher with a **Limited Data Set.**
A. A Limited Data Set is PHI that excludes 16 categories of the direct identifiers noted above, (which may apply both to information about the individual and to information about the individual's relatives, employers, or household members) but may include: city, state, ZIP code, elements of date, and other numbers, characteristics, or codes not listed as direct identifiers. The direct identifiers listed below apply both to information about the individual and to information about the individual's relatives, employers, or household members.

B. An Authorization or documentation of a waiver or alteration of Authorization is not required for Brown / a researcher to receive a Limited Data Set when the data is accompanied by a Data Use Agreement. A Data Use Agreement is a formal, written agreement into which the covered entity enters with Brown and the researcher and establishes specific ways in which the data may be used and how it must be protected. At Brown, Data Use Agreements are formally negotiated between the providing party and the Office of Research Integrity. Questions about this process should be directed to DUA@Brown.edu.

**Business Associate Agreements**

It is rare that Brown (or an investigator) is truly acting in the capacity of a Business Associate in the conduct of research at Brown; researchers are not business associates solely by virtue of their own research activities (although one may become a business associate in some other capacity, e.g., if you are de-identifying PHI on behalf of a Covered Entity).

You may find Covered Entities that are inexperienced with providing PHI to research institutions insist that entering into a Business Associate Agreement is the only way to provide PHI to Brown. This is not the case. Brown is able to appropriately protect these sensitive data without engaging in a Business Associate Agreement. If a data provider requests a Business Associate Agreement, you must contact the Office of Research Integrity at DUA@Brown.edu. Brown’s Office of General Counsel must review such requests; this review will be coordinated by the Office of Research Integrity.

**Obtaining Medical Information about Patients to Identify and Recruit Potential Research Participants under the HIPAA Preparatory to Research Exception**

The HIPAA Privacy Rule permits access to PHI, for the purpose of identifying potential research subjects, under the “Preparatory to Research Exception.” Note, however, that whenever medical records are reviewed for recruitment purposes, that activity is considered by the Office of Human Research Protections (OHRP) to be a research activity that falls under 45 CFR 46 and as such may require a “waiver of consent” to review medical records and to use information from those medical records for recruitment purposes. Examples that are illustrative of regulatory requirements for identifying patients from medical records for recruitment are included for guidance:
Example #1: A Brown Investigator proposes to obtain and record identifiable private information from medical records for the purpose of contacting these individuals to determine if they would be interested in participating in a research study. Consistent with 45 CFR 46 regulations, either (1) the subjects' informed consent is sought; or (2) Brown University IRB approves an informed consent procedure which does not include, or which alters, some or all of the elements of informed consent, or waives the requirement to obtain informed consent in accordance with the provisions of the HHS regulations.

Example #2: A Brown Investigator proposes to obtain and record identifiable private information from medical records to develop a database of potential research subjects for future research studies. Consistent with 45 CFR 46 regulations, either (1) the subjects' informed consent is sought; or (2) Brown University IRB approves an informed consent procedure which does not include, or which alters, some or all of the elements of informed consent, or waives the requirement to obtain informed consent in accordance with the provisions of the HHS regulations.

It should be noted that Authorization for use or disclosure of PHI under the Privacy Rule, and legally effective informed consent for research under HHS regulations at 45 CFR 46.116 and 46.117, are not the same. Any preparatory research activities involving human subjects research which are not otherwise exempt, must be reviewed and approved by an IRB and must satisfy informed consent requirements.

<table>
<thead>
<tr>
<th>Decedent PHI</th>
</tr>
</thead>
</table>

According to Federal policy, research involving deceased individuals is not considered human subjects research and therefore does not require IRB oversight unless the research study includes both living and deceased individuals.

45 CFR 46.102(f): A “Human Subject” is a living (emphasis added) individual about whom an investigator conducting research obtains:
- data through intervention or interaction with the individual, or
- identifiable private information.

For studies that involve BOTH living subjects and human decedents (cadavers, tissue or medical record data, including the use of fetal tissue), the IRB is the institutional committee with jurisdiction for oversight and approval. Therefore, a research study must be submitted to the IRB for review and approval before the study can be initiated.

The HIPAA Privacy Rule applies to the individually identifiable health information of a decedent for 50 years following the date of death of the individual. The Privacy Rule explicitly excludes from the definition of PHI individually identifiable health information regarding a person who has been deceased for more than 50 years.
Brown’s Human Research Protection Program (HRPP) requires that individuals responsible for the conduct of human subjects research activities receive appropriate instruction and education. PIs and research team members who will be collecting, accessing or receiving PHI as part of their proposed research must complete the CITI HIPAA module.

<table>
<thead>
<tr>
<th>Information Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA requires that research involving PHI use physical, technical and administrative safeguards to protect confidentiality.</td>
</tr>
</tbody>
</table>

**Physical safeguards** include storing of person-identifiable data in locked file cabinets, and restriction of access only to those project staff who have a need to access the files. Paper records must not be kept in public areas where passers-by may inadvertently see their content.

**Technical safeguards** apply to computer systems where PHI is stored, and include, for example, use of password-protected access, screensavers that have a timeout such that when a user walks away from the computer, locking access after a period of time, and audit trails that record who has created or changed PHI data in the system. Wherever feasible, personal-identifiable elements of the computerized research records should be stored separately, and if feasible, in an encrypted format.

Brown PIs must comply with Computing & Information Services’ Data Risk Classifications that specify the levels of risk for PHI and required minimum security standards for servers housing such data. De-identified PHI and/or Limited Datasets are Level 2 Risk, whereas PHI that does not constitute a Limited Dataset is classified as Level 3 Risk. Brown recommends that Level 3 Risk PHI be stored in Brown’s Stronghold Research Environment for Data Compliance. Request to store Level 3 Risk PHI in an environment other than Stronghold must be approved by CIS.

<table>
<thead>
<tr>
<th>Record Keeping</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA requires that certain records be maintained in both healthcare and research contexts. Authorizations for use of PHI must be kept in research records for at least six years. Brown recommends that signed informed consent documents be stored together with research Authorization forms.</td>
</tr>
</tbody>
</table>

The Brown PI may not share PHI beyond the members of the research study team without executing an Outgoing Data Use Agreement.