

HIPAA AND HUMAN SUBJECTS RESEARCH

This document provides guidance for researchers wishing to use, disclose or create Protected Health Information (PHI). Should you need additional assistance, please contact OPHS at 510-642-7461 or ophs@berkeley.edu.

Table of Contents

- A. [Introduction/When Do Researchers Need to Apply to CPHS?](#)
- B. [Important Concepts](#)
 - 1. [What Is a Covered Entity?](#)
 - 2. [Is UC Berkeley a Covered Entity?](#)
 - 3. [What is PHI?](#)
 - 4. [What is De-Identified Health Information?](#)
 - 5. [When is Research at Berkeley Subject to HIPAA Privacy Requirements?](#)
- C. [How Can PHI Be Accessed for Research?](#)
 - 1. [Authorization Form](#)
 - 2. [HIPAA Waiver or Alteration of Authorization](#)
 - 3. [Limited Data Set With a Data Use Agreement](#)
 - 4. [Activities Preparatory to Research](#)
 - 5. [Decedents' PHI](#)
- D. [Training](#)
- E. [Additional Information](#)

A. Introduction

In response to a congressional mandate in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), HHS issued regulations known as the **Privacy Rule** (45 CFR parts 160 and 164) to protect the private health information of individuals. HIPAA's Privacy Rule establishes the conditions under which a *covered entity* can provide researchers access to and use of *protected health information (PHI)* when necessary to conduct research. The Privacy Rule applies only to PHI held or maintained by a covered entity, its business associate, and anyone "downstream" of a business associate (e.g., a sub-contractee who maintains PHI) acting for the covered entity.

When Do Researchers Need to Apply to CPHS?

If a study conducted by a UC Berkeley researcher will involve use, disclosure, or creation of UCB PHI, or use of PHI held by an outside institution (non-UCB PHI), a biomedical application must be submitted to CPHS for review and approval. Studies using non-UCB PHI should adhere to the record holder's institutional policies regarding compliance with HIPAA. In certain circumstances involving use of non-UCB PHI, it may be appropriate for CPHS to review the corresponding HIPAA authorization waiver or alteration of authorization.

Studies may be eligible for exempt-level review if the health records are de-identified or constitute a Limited Data Set with a data use agreement. If a HIPAA Authorization or a waiver or alteration of Authorization is needed, a non-exempt application must be submitted.

B. Important Concepts

1. What Is a Covered Entity?

A **covered entity** is a *health plan*, a *health care clearinghouse*, or a *health care provider* who electronically transmits health information in connection with a transaction for which the US Department of Health and Human Services (HHS) has adopted a standard (e.g., transactions concerning billing and payment for services or insurance coverage). A covered entity can be an institution, organization, or individual.

2. Is UC Berkeley a Covered Entity?

The Regents of the University of California is a covered entity. In 2002, the Board of Regents elected to make the University of California a “*hybrid entity*” under HIPAA, which means the University has both covered and non-covered functions. Most HIPAA regulations only apply to covered functions. Berkeley units within UC’s health care component are ***University Health Services*** (including its health care services on behalf of ***Intercollegiate Athletics***) and the ***Optometry Clinic***.

Additionally, to the extent that other campus units perform services to these covered components (e.g., storage of PHI, legal, audit, accounting, information technology, Institutional Review Boards, etc.), they are part of the health care component and must comply with the Privacy Rule. Disclosures of PHI by these covered functions to the rest of the University are regulated by the Privacy Rule and treated like disclosures to entities outside the University.

3. What Is PHI?

Protected Health Information (PHI) is *individually identifiable health information* (see [list of Personal Identifiers under HIPAA](#)) transmitted or maintained in any form or medium (electronic, oral, or paper) by a covered entity or its business associates. The Privacy Rule protects the PHI of both living and deceased individuals.

Health information means any information, including demographic information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Individually identifiable health information is information that is a subset of health information (defined above) that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

List of 18 Identifiers

1. Names;
2. All geographical 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: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is 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. Phone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

4. What Is De-Identified Health Information?

De-identified health information is a record in which identifying information has been removed to render the health information not subject to HIPAA's Privacy Rule. Researchers may use or disclose de-identified health information, without restriction, since it is not PHI and thus is not protected by the Privacy Rule.

Covered entities seeking to release health information to researchers must determine that the information has been de-identified using either of the following methods: (1) by removing all 18 elements that could be used to identify the individual or the individual's relatives, employers, or household members, or (2) by using statistical methods to establish de-identification.

5. When is Research at Berkeley Subject to HIPAA Privacy Requirements?

Research is subject to HIPAA privacy requirements when it is conducted together with the provision of health care services by individuals who are part of a covered component (UHS or Optometry Clinic).

For example, an optometrist who conducts a clinical trial with experimental contact lenses in the course of provisioning routine care to patients would be subject to the HIPAA Privacy Rule and would produce Protected Health Information (PHI) as part of the study.

Researchers should be aware that student health records at postsecondary institutions receiving funding from the U.S. Department of Education (DoED) are considered “education records” under the US Family Educational Rights and Privacy Act (FERPA). [Student health records](#) from UHS and the Optometry Clinic are subject to FERPA, while non-student records are subject to HIPAA.

C. How Can PHI Be Accessed for Research?

1. Obtaining Subject Permission through an Authorization Form
2. Obtaining an IRB Waiver or Alteration of Authorization
3. Using a Limited Data Set with a Data Use Agreement
4. Using PHI for Activities Preparatory to Research
5. Use or Disclosure of Decedents’ PHI

1. Authorization Form

An **Authorization Form** is a form through which a research subject’s signed permission is obtained to allow a covered entity to use and disclose his/her PHI for research purposes. In the case of minors, a signed Authorization Form is obtained from the minor’s parent or legal guardian.

Obtaining HIPAA Authorization is required in addition to obtaining informed consent to participate in research. An Authorization Form focuses on privacy risks and states how, why, and to whom the PHI will be used and/or disclosed for research. This Authorization pertains to a specific research study.

The subject must be given a copy of the signed form to keep for his/her records. Also, the researcher must retain the signed form for six (6) years from the date of creation or the date it was last in effect, whichever is later.

UC HIPAA Authorization Form templates (including translated versions) are available at: <http://www.ucop.edu/ethics-compliance-audit-services/compliance/hipaa/hipaa-authorization-forms.html>

2. HIPAA Waiver or Alteration of Authorization

A **Waiver or Alteration of Authorization** can be requested when researchers are unable to use de-identified health information and the research could not practicably be conducted if research participants’ authorization were required.

For research uses and disclosures of UC Berkeley PHI, the CPHS may approve a waiver or an alteration of the Authorization requirement in whole or in part. A complete waiver is when the CPHS determines that no Authorization is required for use or disclosure of PHI for a particular research project. A partial waiver of Authorization occurs when the CPHS determines that a covered entity does not need Authorization for certain PHI uses and disclosures for research purposes, such as disclosing PHI for research recruitment purposes. An Alteration of Authorization

occurs when CPHS is asked to waive one or more required elements of informed consent. For example, if the purpose of the study will not be disclosed to participants in order to avoid bias, this is an alteration because disclosure of the "purpose" is a required element of participant authorization. The CPHS may also approve a request to alter or waive the requirements for Authorization under the condition that some PHI be removed from the proposed use or disclosure.

All of the following criteria must be met for CPHS approval of a waiver or alteration of Authorization requirements for use or disclosure of UC Berkeley patient data:

1. The use or disclosure of the PHI involves no more than minimal risk to the privacy of individuals based on the presence of, at minimum, 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); and
 - 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.

If a researcher has used or disclosed PHI for research with CPHS approval of a waiver or alteration of Authorization, documentation of that approval must be retained by the researcher for six (6) years from the date of its creation or the date it was last in effect, whichever is later.

3. Limited Data Set with a Data Use Agreement

With the establishment of an appropriate data use agreement (i.e., meets HIPAA requirements, including limiting further use or disclosure of PHI) between the holder of the PHI and the researcher, a Limited Data Set may be used or disclosed for research purposes without obtaining either an individual's Authorization or a waiver or an alteration of Authorization.

A Limited Data Set refers to PHI that excludes 16 of the 18 direct identifiers under HIPAA. Identifiers that may remain in a Limited Data Set include:

- all elements of dates, such as birth date, admission date, discharge date, and date of death;
- town or city, state, and ZIP Code

4. Activities Preparatory to Research

For activities involved in preparing for research, covered entities may disclose PHI to a researcher without an individual's Authorization, a waiver or an alteration of Authorization, or a data use agreement. However, the covered entity must obtain from the researcher written or oral 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, physically or electronically, in the course of review; and (3) the PHI for which use or access is requested is necessary for the research.

5. Decedents' PHI

The Privacy Rule protects the PHI of deceased individuals. Research that uses or discloses decedent PHI must comply with applicable HIPAA regulations. (Note that HIPAA protections cease for PHI of individuals deceased for more than 50 years.)

Use of decedent health information does not require CPHS review and approval if it has been de-identified before receipt by the researchers or does not meet the definition of PHI, as described in the sections above. However, if the study involves the researchers having direct access to decedent medical records or PHI, even if identifiers will not be recorded by the researchers, an application must be submitted for CPHS review and approval.

Authorization from the personal representative or next of kin, a waiver or alteration of the Authorization, and/or a data use agreement are not required by HIPAA in order to use decedent PHI. Before releasing decedent PHI, the covered entity must obtain from the researcher: (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 of the death of the individuals whose PHI is sought by the researchers.

D. Training

Researchers who plan to use PHI are subject to the requirements of HIPAA and must complete Health Privacy(HIPAA) Training through CITI before their CPHS protocol will be approved. For more information, refer to the [Education and Training](#) page.

E. Additional Information

For additional information on research and HIPAA, please visit the links below and/or contact the Office for Protection of Human Subjects.

- [DHHS HIPAA website](#)
- [DHHS OCR Summary of the HIPAA Privacy Rule](#)
- [NIH HIPAA Privacy Rule website](#)
- [University of California HIPAA website](#)
- [State of California Office of Health Information Integrity](#)
- [HIPAA vs. FERPA](#)
- [For HIPAA-related definitions see CPHS/OPHS Glossary](#)

For other HIPAA related questions, please contact the Berkeley Campus Privacy Office at privacyoffice@berkeley.edu.