



University of California  
San Francisco

Published on *UCSF Institutional Review Board* (<https://irb.ucsf.edu>)

[Home](#) > [Recruitment, Consent & HIPAA](#) > [HIPAA REQUIREMENTS](#)

---

## **HIPAA Requirements and Forms for Research**

**HIPAA Forms**

**What Is HIPAA?**

**HIPAA Research Training**

**FAQs**

**HIPAA Links**

**UCSF Privacy Office** <sup>[1]</sup>

### **HIPAA Forms**

Review your approval letter to determine whether subjects must sign a HIPAA authorization form.

---

## UCSF Forms

UCSF Subject Authorization for Release of PHI for Research (PDF) <sup>[2]</sup> or Word version <sup>[3]</sup> (***UCSF Health Version 2016 clarifies Instructions for Researchers Item 3b. There are no other changes to the document.***) You must use the UCSF HIPAA form for research conducted at UCSF. See the instructions on page 4 of the form. The authorization form cannot be changed except to fill in the blanks. Submit this form as an Other Study Document in iRIS. See more info below.

Translated versions of the form <sup>[4]</sup>

Review the instructions on the Non-English Speakers page <sup>[5]</sup> if you are obtaining HIPAA authorization from a non-English speaker and/or if the language you need is not listed below. Additional translated versions will be posted in the future.

---

Cambodian <sup>[6]</sup>

Russian <sup>[7]</sup>

---

Farsi <sup>[8]</sup>

Spanish <sup>[9]</sup>

---

Chinese (Mandarin/Cantonese) <sup>[10]</sup> Vietnamese <sup>[11]</sup>

---

UCSF Cancellation of Permission to Use Personal Health Information for Research <sup>[12]</sup>

---

Data Use Agreement <sup>[13]</sup>

---

## SFVAMC Forms

SFVAMC Authorization for Release of PHI for Research <sup>[14]</sup> ? Submit as an Other Study Document or VA Form in iRIS. Open the file in Adobe Reader.

---

SFVAMC Revocation of Authorization for Release of PHI <sup>[15]</sup> ? Open the file in Adobe Reader.

---

## Authorizations to Be Used at Other Hospitals or Institutions

Other hospitals, medical centers, institutions or clinics will likely have their own HIPAA authorization forms. Those forms should be used at the other sites, just as the UCSF form must be used at UCSF.

## What Is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) <sup>[16]</sup>, also known as "The Privacy Rule," set standards and regulations to protect patients from inappropriate disclosures of their protected health information (PHI) that could cause harm to their insurability, employability and/or their privacy.

HIPAA allows for researchers to access and use PHI when necessary to conduct research. Not all research is subject to HIPAA regulations; HIPAA only affects research that uses, creates or discloses PHI. Review the sections below and visit the UCSF HIPAA website <sup>[17]</sup> for more info.

What is PHI?

Protected health information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used or disclosed in the course of providing a health care service such as diagnosis or treatment.

HIPAA defines 18 specific identifiers that create PHI when linked to health information. HIPAA regulations allow researchers to obtain approval to access and use PHI when necessary to conduct research.

Examples of studies that involve the use of PHI:

- Studies that involve the review of existing health records, such as retrospective chart review or other studies that involve the abstraction of data from the subject's health record for research purposes.
- Studies that create new medical information because a health care service is being performed as part of research. For example, most studies that diagnose a health condition or involve new drugs or devices create PHI that will be entered into the medical record.

What is the list of 18 identifiers?

HIPAA defines 18 specific identifiers that create PHI when linked to health information:

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)

There are also additional standards and criteria to protect individual's privacy from re-identification. Any code used to replace the identifiers in datasets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed. For example, the unique code cannot include the last four digits (in sequence) of the social security number. Additionally, the researcher must not have actual knowledge that the research subject could be re-identified from the remaining identifiers in the PHI used in the research study. In other words, the information would still be considered identifiable if there was a way to identify the individual even though all of the 18 identifiers were removed.

What is not PHI?

Some research studies do not use, create or disclose PHI and are not subject to HIPAA regulations.

For example, some studies use individually identifiable health information that includes personal identifiers such as name, date of birth or address. However, it is not considered to be PHI because the data are not (i) obtained or generated as part of a health care service (treatment, payment, operations, medical records), (ii) entered into a medical record, or (iii) used to make treatment decisions.

Examples of studies that use research health information only and are not subject to HIPAA:

- Studies that obtain data from subjects during interviews or surveys, and the investigators do not review or alter the subjects' health records or make treatment decisions as part of the research.
- Studies that obtain data from records open to the public or existing research records.
- Studies that use tests that do not go into the medical record because they are part of a basic research study and the results will not be disclosed to the subject.

Also, health information by itself without the 18 identifiers is not considered to be PHI. For example, a dataset of vital signs by themselves do not constitute protected health information.

However, if the vital signs dataset includes medical record numbers, then the entire dataset must be protected since it contains an identifier.

Data that is not subject to HIPAA is generally still regulated by other human subjects protection regulations. Please protect and manage the data with the same level of data security and care as PHI.

Does HIPAA apply to my research?

The chart below summarizes to which studies HIPAA regulations may apply. There may be exceptions to these very general guidelines.

Study data are ... <ul style="list-style-type: none"><li>• Derived from a medical record.</li><li>• Added to the hospital or clinical medical record.</li><li>• Created or collected as part of health care.</li><li>• Used to make health care decisions.</li></ul>	<b>HIPAA regulations apply.</b>
Study data are only ... <ul style="list-style-type: none"><li>• Obtained from the subject, including interviews, questionnaires.</li><li>• Obtained from a foreign country or countries only.</li><li>• Obtained from records open to the public.</li><li>• Obtained from existing research records.</li></ul>	<b>HIPAA regulations do not apply.</b>

If HIPAA applies, how do I obtain approval to use and/or disclose PHI from research subjects?

The IRB will act as a Privacy Board (required by HIPAA) to review the use and disclosure of PHI. The IRB will determine whether you can access PHI by one or both methods:

- The research subject (or legal representative, when approved) signs the UCSF Subject Authorization for Release of PHI for Research [18] or SF VAMC Authorization for Release of PHI for Research [19] to grant permission to use PHI for research.
- The IRB grants a waiver of authorization for the entire study *or* for recruitment purposes only.

Your approval letter will identify which method(s) the IRB approved.

## HIPAA Research Training

**Research Aspects of HIPAA Tutorial (UCSD)** [20]: Investigators, research staff, coordinators and administrators who need to know HIPAA research procedures should take this tutorial [21].

The UC San Diego (UCSD) Human Subjects Protection Program developed this training and made it available to the research community at all the UC Medical Centers. It is targeted to research investigators, but anyone interested may complete the training. After you finish the tutorial, you will receive a completion certificate.

**Tracking:** Individual departments are required to track the HIPAA training for their staff. The IRB does not track HIPAA training, although it does expect researchers to complete training. Do not submit HIPAA training certificates to the IRB.

**Non-Research HIPAA Training:** There are other non-research-related HIPAA training requirements [22] for members of the UCSF workforce, which are tracked and managed by the UCSF Privacy Office [23].

## FAQs

What is individually identifiable health information?

?Individually identifiable health information? is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, medical record number).

What is the subject's authorization? What do I use at UCSF, SFVAMC, and other institutions or for sponsors?

The subject's authorization for release of personal health information is a required supplement to the standard consent form. It does not change any of the information or permissions described in the consent document.

The authorization form includes all of the elements required by the federal government [24]. It describes the different ways that the researcher, research team and the research sponsor may use the subject's PHI for the research study. The subject grants their permission to access their information when they sign this subject authorization form.

**UCSF:** The University of California has developed the authorization form used at UCSF [25]. All UCSF-affiliated research investigators obtaining subject authorization to use PHI in their studies must complete and use this form without altering the standard text in the form.

**SFVAMC:** The SFVAMC-specific authorization [19] is required at that site. Therefore, if you are enrolling subjects at the SFVAMC and UCSF, you will use separate HIPAA authorizations at each site.

**Other Sites:** Other non-affiliated medical centers and institutions may require you to use their version of the authorization form to access their medical records. The authorization form originates from the covered entity that owns the PHI (usually medical records) for which you are requesting access. However, smaller clinics may accept the UCSF authorization in lieu of their own. You should determine in advance what the HIPAA authorization requirements would be for medical records access.

**Sponsors:** Industry sponsors may want you to use the sponsor's authorization form. At UCSF, research investigators will only be allowed to use UCSF authorization form (or SFVAMC form for research conducted there). Contact the IRB with questions about sponsor authorization forms.

Can I obtain verbal authorization?

Yes, but only if you have an IRB-approved waiver of authorization that waives the HIPAA requirement for a written authorization.

What is a waiver of authorization? How do I request a waiver?

A waiver of authorization may be granted in situations where an individual's authorization to access their PHI will not be obtained. The IRB may waive authorization for an entire study or just for recruitment purposes.

There are several types of research studies that may need a waiver of authorization such as:

- Reviews of medical records for data collection (chart reviews)
- Access to databases that have PHI in them
- Studies that access clinical databases, hospital medical records, appointment logs and other similar databases to identify potential subjects for recruitment or screening purposes
- Studies that enroll subjects with verbal consent

Note: If the clinic does not have an IRB-approved recruitment protocol, then each research study will have to obtain an IRB-approved waiver of authorization to screen the clinic's records for subjects for recruitment purposes. If these potential subjects are later enrolled in research studies, they must sign both the informed consent form and the authorization form.

The UCSF IRB, as the Privacy Board for research, is allowed to grant a waiver of authorization if it can certify that the research meets the following criteria [26]:

1. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
  - an adequate plan to protect the identifiers from improper use and disclosure;
  - 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

- adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, 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 PHI.

The IRB will also expect the research to satisfy the current human subject protection regulations including that the waiver will not adversely affect the rights and welfare of the subject and that the risks are reasonable in relation to the anticipated benefits of the research. Requests for waiver of authorization must be submitted to the IRB and be approved prior to accessing the health information.

The IRB Application in iRIS includes questions to determine whether HIPAA authorization is required, or if a waiver of authorization can be granted for the entire study or for recruitment purposes only. The IRB approval letter will document these determinations.

Is IRB approval required for decedent research at UCSF?

It depends on whether PHI will be accessed and/or whether state, county or local death data files will be accessed, as both the federal and state privacy laws apply. See the FAQ section on the Research Needing IRB Review <sup>[27]</sup> page for more information.

What is de-identified data?

HIPAA allows the patient information to be "used and disclosed freely, without being subject to the Privacy Rule's protections" if has been de-identified. De-identified PHI has all identifying information removed but the data could be re-identified if necessary, usually through means of a code. This code cannot be derived from any of the elements removed during de-identification, e.g. a unique code cannot be created using the last four digits of a social security number.

However, the UC authorization for release of personal health information form does allow for the use of initials, date of birth and dates of medical care as "personally unidentified study data." Typically, this type of data is used in case report forms (CRF) for quality control purposes where the CRF is verified with the source documents, especially for sponsors.

There are two acceptable methods for creating de-identified data (PHI) including the removal of 18 primary and secondary identifiers from the dataset, or, using statistical methods of verifying that the data could not be used to re-identify a research subject. Additionally, the researcher must not have actual knowledge that the research subject could be re-identified from the remaining identifiers in the PHI used in the research study.

If you are working with a non-UCSF partner and you want to share your data, the UCSF Privacy office **requires** that your data are "certified," meaning your dataset is correctly de-identified. UCSF has a Data De-identification Validation Service <sup>[28]</sup> that allows you to verify that your datasets have been de-identified in accordance with HIPAA regulations and obtain

the required certification.

Some research involving only de-identified data is not human subjects research [29] and does not require IRB review. This determination may depend on the source of the data, who de-identifies the data and the method(s) used to de-identify the data. Review the not human subjects research guidance [29] to determine whether your study needs IRB review.

What specific identifiers must be removed to create de-identified data?

The 18 identifiers listed above must be removed for de-identification. If you are working with a non-UCSF partner and you want to share your data, the UCSF Privacy office requires that your data are "certified," meaning your dataset is correctly de-identified. UCSF has a Data De-identification Validation Service [28], which enables you to verify that your datasets have been de-identified in accordance with HIPAA regulations and obtain the required certification.

What is the statistical method of de-identification?

A statistical expert must certify that the risk is "very small" that anyone could re-identify the research subjects from the PHI identifiers used in the study. They must document the methods used to determine that data has been rendered de-identified. A statistical expert is someone with "appropriate knowledge and experience with statistical and scientific principles and methods for rendering information not individually identifiable".

What is a limited dataset?

A limited dataset is a limited set of identifiable information in which most of the identifiers for the individual, the individual's relatives, employers and household members have been removed. The only allowable health information identifiers are:

- 5 digit zip code (the 4 digit extension is not allowed)
- dates of birth, death, admission, discharge
- all geographic subdivisions other than street address

The advantages of using a limited dataset include that the disclosures are not subject to HIPAA accounting requirements and that an individual's authorization does not need to be obtained. However, you may be asked to sign a Data Use Agreement [30] by the purchasing or contracts office of the university or other covered entities to give assurances that the information will be protected.

An IRB application is required for studies involving limited datasets.

Does HIPAA apply to my international study?

No. U.S. Federal laws do not apply to studies conducted in foreign countries. The standard

methods of protecting confidentiality and privacy for research in human subjects still apply and you should have these in place. However, the research subjects do not need to sign an authorization to allow access to their PHI.

Can databases or registries be created under HIPAA?

Yes. HIPAA allows for the creation of databases for research purposes. A research database can be created without obtaining individual authorizations, but only with an IRB-approved waiver of authorization. The PHI maintained in the research database may be disclosed for future research studies if the investigator either obtains an individual's authorization or an IRB-approved waiver of authorization.

How do I protect the PHI in my study?

Investigators are advised to analyze the flow of PHI through their research projects and develop security policies for both electronic <sup>[31]</sup> and hard copy PHI. Simple steps may be all that are required to accomplish the goals of tracking, recovery and security.

- **A tracking system** is necessary to account for how the PHI is stored, used, and shared, e.g. flow of PHI through your project.
- **A recovery plan** simply means having the capability to recover data if you lose your primary database for both your research and for HIPAA accountability of any PHI disclosures.
- **A security system** that prevents inadvertent disclosure, loss or theft of PHI from your project is required. For example, to secure physical data, keep files in locked cabinets and locked offices/suites. See the Electronic Data Security <sup>[31]</sup> section of our website and consult with your IT professional for more information on securing data electronically.

What is a privacy breach? What should I do if PHI may have been disclosed to unauthorized individuals?

A privacy breach refers to any unauthorized access to PHI and commonly (but not always) is related to electronic files or devices that contain PHI.

Contact the HIPAA Privacy Office <sup>[32]</sup> (415-353-2750) and the IRB <sup>[33]</sup> (415-476-1814) **immediately** if you are concerned that there may have been a breach of security for your research files. These offices will work with you to assess the situation to determine who else may need to be notified.

Common examples of breaches:

- Talking to the wrong person or sending an email, letter or fax to the wrong address, person or number
- Lost/stolen or improperly disposed paper documents
- Lost/stolen unencrypted laptops, tablets, cell phones, media devices (video and audio recordings)

- Lost/stolen unencrypted CDs, flash drives, memory sticks
- Hacking of unprotected computer systems

Can I send PHI via email?

Please refer to the UCSF Privacy Office <sup>[34]</sup> and ITS <sup>[35]</sup> sites for guidance.

Can I send PHI via FAX?

Yes, but only to secured fax machines. Never fax information to an unsecured fax machine. A secured fax machine is one that is located in a restricted environment. Recommended best practices include:

- Always check the destination fax number before faxing.
- The first time you use a fax destination number, send a cover sheet requesting confirmation that the fax number is authorized to receive the PHI. After you receive the fax number confirmation, keep a copy in your files.
- Use cover sheets containing the confidentiality statement:

*This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message*

- Return items you receive that were faxed to the wrong location or improperly faxed and advise the sender of the error.

Do I need a Business Associate Attachment (BAA) for my research?

Maybe. If your research project will contract a vendor outside of UCSF for research-related goods or services and the vendor may potentially be exposed to PHI, then the vendor must have a BAA with UCSF <sup>[36]</sup> before they begin.

Examples of such vendors include (but are not limited to) those that contract statistical services, data management, data hosting and data analysis. Equipment repair vendors that service machines that have PHI stored on them also need to have BAA in place. Additional examples are available on the Supply Chain Management website <sup>[37]</sup>.

The BAA is between the vendor and UCSF, not between the vendor and the investigator. If your project will need this type of research service, you should contact your Purchasing Officer who then will negotiate the BAA on your behalf with the vendor (see these instructions <sup>[37]</sup>).

## HIPAA Links

HIPAA Privacy Rule  
Information for Researchers  
(NIH) [41]

California Medical Information Act  
(CMIA) (Civil Code § 56.10) [42]

UCSF Privacy Office  
[32]

**Page last updated:**

Apr 17, 2019

[Home](#)

[Contact Us](#)

[UCSF Main Site](#)

© 2013 The Regents of the University of California

---

**Source URL:** <https://irb.ucsf.edu/hipaa>

**Links**

- [1] <http://hipaa.ucsf.edu>
- [2] [http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/ucsf-hipaa-authorization-research\\_1.pdf](http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/ucsf-hipaa-authorization-research_1.pdf)
- [3] <http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/ucsf-hipaa-authorization-research-feb-12-2019.docx>
- [4] <https://irb.ucsf.edu/#>
- [5] <https://irb.ucsf.edu/consenting-non-english-speakers>
- [6] <http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/cambodian-hipaa.pdf>
- [7] <http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/russian-hipaa.pdf>
- [8] <http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/farsi-hipaa.pdf>
- [9] <http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/spanish-hipaa.pdf>
- [10] <http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/mandarin-hipaa.pdf>
- [11] <http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/vietnamese-hipaa.pdf>
- [12] <http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/ucsf-authorization-cancellation.pdf>
- [13] <https://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/data-use-agreement-2007Dec.pdf>
- [14] <http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/SFVAMC-HIPAA-authorization.pdf>
- [15] <http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/sfvamc-authorization-revocation.pdf>
- [16] <http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html>
- [17] <http://hipaa.ucsf.edu/>
- [18] <http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/ucsf-hipaa-authorization-research.pdf>
- [19] <http://hrpp.ucsf.edu/sites/hrpp.ucsf.edu/files/SFVAMC-HIPAA-authorization.pdf>
- [20] <https://irb.ucsd.edu/hipaatutorial/login.shtml>
- [21] <http://irb.ucsd.edu/hipaatutorial/login.shtml>
- [22] <http://hipaa.ucsf.edu/education/>
- [23] <http://hipaa.ucsf.edu/privacyoffice/default.html>
- [24] <http://privacyruleandresearch.nih.gov/authorization.asp>
- [25] <http://irb.ucsf.edu/sites/hrpp.ucsf.edu/files/ucsf-hipaa-authorization-research.docx>
- [26] <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/research.html>
- [27] <http://hrpp.ucsf.edu/node/307#faqs>
- [28] <https://data.ucsf.edu/data-assets/de-identification>
- [29] <https://irb.ucsf.edu/not-human-subjects-research>
- [30] <http://hipaa.ucsf.edu/documentation/downloads/DataUseAgreement2007Dec.pdf>
- [31] <https://irb.ucsf.edu/electronic-data-security>

- [32] <http://hipaa.ucsf.edu/privacy-office>
- [33] <https://hrpp.ucsf.edu/contact-us?>
- [34] <http://hipaa.ucsf.edu/frequently-asked-questions#faq10>
- [35] <https://it.ucsf.edu/services/secure-email>
- [36] <http://policies.ucsf.edu/policy/200-28>
- [37] <http://supplychain.ucsf.edu/hipaa>
- [38] <http://www.hhs.gov/ocr/privacy/index.html>
- [39] <http://www.ohii.ca.gov/calohi/home.htm>
- [40] <http://www.universityofcalifornia.edu/hipaa>
- [41] <http://privacyruleandresearch.nih.gov/>
- [42] <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=00001-01000&file=56.10-56.16>