HIPAA: What Researchers Need to Know

The Health Insurance Portability and Accountability Act (HIPAA) protects individuals’ medical records from unauthorized use. Medical records, however, are often integral to learning more about important research questions. This guide is intended to serve as a primer for researchers who seek to use medical records in their research, especially researchers who wish to conduct research with their own clinical records.

Please note that the standards here apply even where you do not intend to use the identifiable information. Any time you will have access to individually identifiable health information for research purposes, it must be in compliance with the HIPAA requirements detailed below.

Medical Records and Research: The Basics

HIPAA is a lengthy and complex set of statutes and regulations protecting medical records in many different contexts. The Privacy Rule is a subpart of the broader HIPAA structure, and it specifically protects the use of individually identifiable health information in research. In order to use this kind of information in research, investigators can take one of the following four steps:

1. Obtain authorization for use or disclosure of that information from the individual
2. Obtain a waiver from the Utah State University Institutional Review Board to access that information without authorization from the individual
3. Obtain a limited data set with a limited data use agreement from the covered entity providing the information
4. Obtain a completely deidentified data set which is not able to be reidentified based on other information available to you

Below, we will detail some basics relating to each of these options for using individually identifiable health information in research.

Medical Records and Research: How to Get Access in Compliance with HIPAA

HIPAA Authorizations

The HIPAA Authorization process closely mirrors the Informed Consent process required in almost all Human Subjects Research projects. A HIPAA Authorization (“Authorization”) is a document that individuals whose medical information you hope to use can sign to grant you legal access to those records for research purposes.

An Authorization must contain the following elements, and can be combined with your Informed Consent document:

- A specific description of the information that will be accessed and used for the research
- A specific description of who will have access to the aforementioned information
- A statement that the individuals receiving the protected health information may not be required to protect the information in the same way that the providing entity must protect it
A statement that if the treatment or intervention is being offered only for research purposes, declining to sign this Authorization may mean that the individual would not receive the treatment or intervention; OR that the researcher cannot refuse or alter treatment on the basis of whether the individual signs the Authorization (this depends on the circumstances of the treatment or intervention)

When the authorization expires (this can be “when the research has ended”)

A statement that the individual may revoke their Authorization at any time, that the disclosed information prior to revocation may still be used for the research purposes described previously, and who the individual should contact to revoke the Authorization

The following elements of an Authorization are optional, but should be included where relevant:

- Any circumstances where the researcher would be required by law to release the health information (for example, Tarasoff reporting requirements, child abuse, etc.)
- That the individual’s information will not be shared in publications or presentations in an identifiable way
- That if the information received is later deidentified to HIPAA standards, it can be shared or disclosed for other purposes
- When, if ever, the records received for research purposes will be made available to the individual giving Authorization for access

In crafting your Authorization, it is important to note that the Office for Civil Rights requires that researchers only use the minimum necessary information contained in the individual’s medical records for research purposes. In most cases, this will not allow researchers to simply receive access to entire medical records; the information requested and specified in the Authorization must be the minimum necessary to address the research question.

**Waiver or Alteration of HIPAA Authorization**

The Utah State University Institutional Review Board may waive the requirement to obtain an Authorization if the following three criteria can be demonstrated by the Principal Investigator and documented by the IRB:

- The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals;
- The research could not practicably be carried out without the waiver; AND
- The research could not practicably be carried out without access to and use of the protected individually identifiable health information.

Practicability does not mean mere difficulty. Instead, the IRB must make a determination that obtaining an Authorization presents an “extreme circumstance of expense or difficulty.”

In order to determine whether the use or disclosure involves no more than a minimal risk to the individuals whose information would be released, HIPAA requires that the PI demonstrate:

- An adequate plan to protect the identifiers from improper use and disclosure
- An adequate plan to destroy the identifiers at the earliest opportunity
- Written assurances to the IRB that the protected health information will not be reused or disclosed to any other person or entity, or for other research purposes.
Please note that waivers to HIPAA Authorizations are not the norm, but rather, the exception. The best way to exercise Respect for Persons as outlined in the Belmont Report is to obtain an Authorization whenever possible.

If the entity releasing PHI under a waiver or alteration is a USU entity, it is required to have policies and procedures in place to determine whether the information being disclosed is the minimum necessary information. The entity must review each disclosure or request for disclosure individually against the policies and procedures it has developed to ensure it is releasing only that information which is necessary to accomplish the purpose of the request or disclosure. It must also maintain records related to those disclosures. HIPAA requires that, at the request of any individual, the disclosing entity must account for all disclosures of protected health information for the previous six years.

**Limited Data Sets & Limited Data Use Agreements**

A limited data set allows a covered entity to release or use PHI without an Authorization from the individual whose records are sought for research use. At Utah State University, a limited data set may be used after obtaining a limited data use agreement that has been reviewed and approved by the USU Information Security Office.

The limited data set must exclude:

- Names
- Postal address information other than city, state, and zip code
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate or license numbers
- Vehicle identifiers/serial numbers, including license plate numbers
- URLs
- IP Addresses
- Biometric identifiers, including fingerprints and voiceprints
- Full-face photographic images and any comparable image

The limited data use agreement must be in place even if the researcher is a member of the covered entity releasing the data. The agreement is required to contain the following provisions:

- Specific permitted uses and disclosures if the limited data set which are consistent with the purpose for which the data will be disclosed. No further uses are permitted.
- Identification of who is permitted to use or receive the limited data set.
- Stipulations that the recipient will:
  - Not use or disclose the information other than permitted by the agreement or otherwise as required by law (e.g. mandatory reporting requirements or subpoena)
  - Use appropriate safeguards to prevent the use or disclosure of the information, except as provided for in the agreement.
  - Report to the covered entity and IRB any uses or disclosures in violation of the agreement upon discovery
  - Hold any agent of the recipient to the standards, restrictions, and conditions stated in the data use agreement with respect to the information
Not attempt to reidentify or contact the individuals.

Please note that if you are a part of the covered entity releasing PHI under a limited data use agreement or for any other reason without an Authorization, your entity must maintain records related to those disclosures. HIPAA requires that, at the request of any individual, the covered entity must account for all disclosures of their Protected Health Information for the previous six years.

**Deidentification**

Covered entities may use or disclose health information without restriction under HIPAA if the health information has been deidentified to HIPAA standards. There are two ways to accomplish this: 1) removal of all 18 HIPAA identifiers *plus* the inability to reidentify the data using actual knowledge; or 2) established statistical methods which allows some of the 18 HIPAA identifiers to remain in place, while ensuring reidentification risk is virtually impossible.

### HIPAA Identifier Removal

Removal of all 18 HIPAA identifiers may render otherwise protected health information unidentifiable, thus permitting its disclosure. Those 18 identifiers are:

- Names
- Geographic subdivisions smaller than a state (including address, city, county, precinct, zip codes [except for the initial three digits if all zip codes beginning with those numbers comprise areas with more than 20,000 inhabitants or by changing the first three digits to 000])
- All elements of dates, including DOB, admission date, discharge date, date of death, and all ages or dates indicative of an age over the age of 89
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate or license numbers
- Vehicle identifiers / serial numbers, including license plates
- Device identifiers or serial numbers
- URLs
- IP addresses
- Biometric identifiers including fingerprints and voiceprints
- Full-face or comparable photographic images
- Any other unique identifying number, characteristic, code, etc.

In addition to the removal of these identifiers, the covered entity can have no *actual* knowledge that the information remaining could render the information identifiable. In cases where researchers are working in their own clinics, for example, you must ensure that the information remaining could not be matched back to an identifiable medical file. In that case, researchers will almost always need to use an Authorization, waiver, or limited data use agreement.

### Established Statistical Methods

A second way to deidentify protected health information to allow its disclosure or use would be to use established statistical methods, which may allow you to leave certain identifiers above in the data set. This may be done so long as the statistician is a “person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for
rendering information not individually identifiable.” That individual must provide a certification that there is a “very small” risk that the information could be used by the researcher to reidentify the individual either alone or with the use of other information available to the researcher. The certification provided must include the methods used to make that determination, and provide the analysis that justifies the determination. Both the researcher and the covered entity must maintain that certification for at least six years after the release of the protected health information.

Successful deidentification of the protected health information may take you outside of the human subject research oversight requirements if the data are not within your own clinic and they are deidentified before you receive them. Otherwise, an Exempt 4 application may be appropriate.