

**HIPAA AND RESEARCH FAQs**

1. **How does the HIPAA Privacy Rule affect research?**

A covered entity and its workforce members may not use or disclose individually identifiable health information (called “protected health information” or “PHI”) for research, except in one of the following circumstances:

1. The patient has signed a written Authorization containing all the elements specified in the Privacy Rule;
2. An IRB has waived or altered the requirement for HIPAA Authorization;
3. The covered entity has “de-identified” the data prior to its use or disclosure for research; or
4. The data are in the form of a “limited data set” containing no HIPAA “direct identifiers,” and” and the researcher has signed a HIPAA Data Use Agreement or DUA (if the data source is UVM Medical Center, the DUA would need to be signed by UVM Medical Center per hospital policy).
5. **What is the difference between HIPAA “Authorization” and informed consent?**

Informed consent is required under federal research regulations for the protection of human subjects. The HIPAA Privacy rule, a different regulation, separately requires that patients give written Authorization before a covered entity may use or disclose PHI for research. There are different requirements for the content of informed consent and HIPAA Authorization; however both may be combined in one form. An IRB may waive both consent and Authorization if the research meets all of the waiver criteria established by each of the applicable regulations.

1. **What are the required elements of a HIPAA “Authorization”?**

The core elements of a valid authorization include (Privacy Rule*,* 45 C.F.R.§164.508(c)(1)):

* 1. A meaningful description of the information to be disclosed
  2. The name of the entity(s) or individual(s) authorized to make the requested disclosure (UVM Medical Center)
  3. The name or other identification of the recipient(s) of the information (UVM, Sponsor, Agencies that regulate reseach)
  4. A description of the purpose of the disclosure (how it will be used for THIS study – not unspecified future research)
  5. An expiration date or an expiration event that relates to the individual (“end of the research study" or "this authorization does not expire" are permissible for research)
  6. A signature of the individual or their personal representative (someone authorized to make health care decisions on behalf of the individual) and the date.

1. **What statements are required to be included in the HIPAA “Authorization”?**

Authorization Required Statements (Privacy Rule, 45 C.F.R. § 164.508(c)(2)):

1. The individual's right to revoke his/her Authorization in writing and the exceptions to the right to revoke and a description of how the individual may revoke Authorization.
2. Notice of the covered entity's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the Authorization, including research-related treatment, and, if applicable, consequences of refusing to sign the Authorization.
3. The potential for the PHI to be re-disclosed by the recipient and no longer protected by the Privacy Rule. This statement does not require an analysis of risk for re-disclosure but may be a general statement that the Privacy Rule may no longer protect health information.
4. **When does a researcher need to “account for disclosures”?**

HIPAA allows for individuals to request an account of certain “disclosures” made by a covered entity. In the context of research, any disclosure made pursuant to a waiver of HIPAA authorization would need to be accounted for. A “disclosure” is when a covered entity is providing or communicating PHI outside of its workforce (NOTE: UVM employees and faculty who have been credentialed are considered members of the UVM Medical Center workforce as well as faculty and students who are listed as personnel on an IRB protocol and acting under supervision of a UVM Medical Center PI). If a researcher from another institution (UVM, for example) will receive UVM Medical Center PHI, that person’s accessing or viewing of the PHI will generally be a disclosure – this can be for purposes of recruitment or conducting research. Contact the UVM Medical Center Privacy Office with questions.

1. **What are the required statements in a HIPAA “Alteration”?**

Any of the requirements of a written HIPAA Authorization (See above or 45 CFR 164.508) can be altered or waived by the IRB if the research meets the criteria for waiver or alteration. The most frequent “alteration” is for verbal HIPAA Authorization when the IRB has also waived the requirement for written consent under 45 CFR 46.117(c)(2). Demonstrating that the "research could not practicably be conducted without the waiver or alteration" is the main obstacle to approving an alteration. If the subject is physically present, it is usually practicable to obtain written HIPAA Authorization. If the documentation of consent has been waived by the IRB and verbal consent will be obtained, verbal HIPAA Authorization should also be obtained.

1. **What is the difference between a “Partial Waiver of Authorization” and an “Alteration”?**

A Partial Waiver of Authorization is when HIPAA authorization to use and disclose PHI is waived for just part of the research. For example, a Partial Waiver may be appropriate to allow a researcher to obtain PHI as necessary to recruit potential research subjects. Once a subject is recruited, he or she would be asked to sign a HIPAA Authorization for purposes of the research study. An Alteration would be used where a study team is requesting that one of the required Authorization elements (a patient signature, for example) be removed.

1. **When is data considered “De-identified”?**

Data is considered to be “de-identified” when **all 18 HIPAA identifiers** (see table below) **have been removed** and the researcher has no actual knowledge that the remaining information could be used in combination with other publicly available information to identify a particular patient. Please note that Dates of Service and MRNs are considered identifiers.

|  |  |
| --- | --- |
| (A) Names | |
| (B) 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 the 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 | |
| (C) All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, 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 | |
| (D) Telephone numbers | (L) Vehicle identifiers and serial numbers, including license plate numbers |
| (E) Fax numbers | (M) Device identifiers and serial numbers |
| (F) Email addresses | (N) Web Universal Resource Locators (URLs) |
| (G) Social security numbers | (O) Internet Protocol (IP) addresses |
| (H) Medical record numbers | (P) Biometric identifiers, including finger and voice prints |
| (I) Health plan beneficiary numbers | (Q) Full-face photographs and any comparable images |
| (J) Account numbers | (R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section [Paragraph (c) is presented below in the section “Re-identification”]; and |