

Investigator Guidance Series

University of Utah Institutional Review Board

HIPAA PRIVACY RULE & AUTHORIZATION

Definitions

The Privacy Rule was issued by the U.S. Department of Health and Human Services (DHHS) and was designed to implement the requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The Privacy Rule is a set of national standards for the protection of certain health information. The Privacy Rule applies directly to “covered entities” and is designed to protect individuals’ health information.

Description

To protect patient privacy, “covered entities” (all health plans, health care “clearinghouses,” and health care providers) must obtain specific, written authorization from a patient to use or disclose PHI. Patients must also be notified about their right to restrict the use and disclosure of such information. Covered entities must make reasonable efforts to limit the health information disclosed to the minimum necessary to accomplish the intended purposes.

Options for Conducting HIPAA-Compliant Research

1. Obtain HIPAA authorization from individuals to use their protected health information (PHI)
2. Use a de-identified Data Set that contains no PHI
3. Use a Limited Data Set with an effective Data Use Agreement in place as applicable
4. Obtain an IRB Waiver of (HIPAA) Authorization

Local Institutional Review Boards (IRB) have the authority to make determinations about whether the proposed procedures of research under their domain meet Privacy Rule requirements.

The 18 PHI Identifiers

1. Names
2. Geographic subdivisions smaller than a state if it contains less than 20,000 people (the initial three digits of the zip code are allowed). This includes street address, city, county, precinct, and zip code (or equivalent geocodes).
 - o The initial three digits of a zip code may be included if, according to the currently publicly available data from the Bureau of Census the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to “000”
3. Dates
 - o 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 (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. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate or license numbers
12. Vehicle identifiers, serial numbers, and license plate numbers
13. Device identifiers and serial numbers
14. Internet Universal Resource Locators (URLs)
15. Computer Internet Protocol (IP) addresses

Please contact the IRB Office at (801) 581-3655 or irb@hsc.utah.edu for additional guidance.

Investigator Guidance Series

University of Utah Institutional Review Board

16. Biometric identifiers
17. Full-face photographs and comparable images
18. Any other unique identifying number, characteristic, or code, except as permitted for re-identification of the de-identified data

In order for a record (or research data set) to be considered de-identified, each of the above identifiers must be removed. This is applicable to identifiers of the individual, or of relatives, employers, or household members of the individual.

OPTION 1: Obtain HIPAA Authorization from Individuals to use their PHI

The IRB consent document template includes a section titled "Authorization for Use of Your Protected Health Information." This section includes all of the required elements to obtain authorization from participants, and is required for most studies where health information is included in the research and a full consent document is utilized as a part of the consent process.

OPTION 2: Use a De-identified Data Set That Contains No PHI

There are no restrictions on the use of disclosure or de-identified health information. There are two ways to de-identify information:

1. a formal determination by a qualified statistician (i.e. "Statistical Analysis" De-Identification); or
2. the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is only adequate if the covered entity has no knowledge that the remaining information could be used to identify the individual (i.e. "Safe Harbor" De-Identification).

OPTION 3: Use a Limited Data Set with a Data Use Agreement

HIPAA's Privacy Rule makes provisions for a "**limited data set**," authorized only for public health, research, and health care operations purposes (45 CFR § 164.514(e)(3)(i)).

A limited data set must have all **direct identifiers removed**, including:

- name and social security number;
- street address, e-mail address, telephone and fax numbers;
- certificate/license numbers;
- vehicle identifiers and serial numbers;
- URLs and IP addresses;
- full face photos and any other comparable images;
- medical record numbers, health plan beneficiary numbers, and other account numbers;
- device identifiers and serial numbers; and
- biometric identifiers, including finger and voice prints.

A limited data set **may include** the following (potentially identifying) information:

- admission, discharge, and service dates;
- dates of birth and, if applicable, death;
- age (including age 90 or over); and
- five-digit zip code or any other geographic subdivision, such as state, county, city, precinct and their equivalent geocodes (except street address).

What is the Difference Between a "De-Identified" and a "Limited" Data Set?

A De-Identified Data Set excludes the 18 PHI Identifiers. A covered entity may de-identify PHI so that

Please contact the IRB Office at (801) 581-3655 or irb@hsc.utah.edu for additional guidance.

Investigator Guidance Series

University of Utah Institutional Review Board

such information may be used and disclosed freely, without being subject to the Privacy Rule. However, a de-identified data set may contain a linking code that could allow the covered entity to re-identify the data later.

A Limited Data Set also excludes the 18 PHI Identifiers, but does not have to be fully de-identified. A Limited Data Set may include dates (birth, death, admission, discharge, age), and limited geographic information (zip code, state, county, city, precinct and their equivalent geocodes except street address). With a Data Use Agreement, a Limited Data Set may be used or disclosed for research purposes if it is stripped of most identifiers.

De-Identified Data Verses Limited Data Set

The following chart describes the information that must be *eliminated* from a database, registry, or any other data set for the data set to be considered “De-identified” or a “Limited Data Set”. Appropriately De-identified Data Sets are not regulated by HIPAA. Limited Data Sets may be used or disclosed for research, public health, and other limited purposes, but only by those who sign a DUA. Note that for each data element listed below, the information must be eliminated with respect to the patient *and* to any of the patient’s relatives, employers, or household members.

Even if HIPAA does not regulate the use of a dataset or permits its use or disclosure for research, federal regulations and University policies governing human subjects research may still apply.

Data Element	De-Identified Data Set ¹	Limited Data Set
Names	Remove	Remove
Address, city and other geographic information smaller than state. <i>3-digit zip code may be included in a de-identified data set for an area where more than 20,000 people live; use “000” if fewer than 20,000 people live there.</i>	Remove	Remove postal address information other than city, town, state or zip code.
All elements of dates (except year); plus age and any date (including year) if age is over 89. <i>Examples: date of birth, date of death, date of admission, date of discharge, date of service.</i>	Remove	May be included.
Telephone, fax numbers; e-mail addresses, web URL addresses, IP addresses.	Remove	Remove
Social security number, medical record number, health plan beneficiary number, any account number, certificate or license number.	Remove	Remove
Vehicle identifiers and serial numbers, including license plate numbers.	Remove	Remove
Device identifiers and serial numbers.	Remove	Remove
Biometric identifiers (e.g., fingerprints; voice prints). <i>DNA is not considered a biometric identifier for purposes of HIPAA.</i>	Remove	Remove
Full-face photographs and any comparable images.	Remove	Remove
Any other unique identifying number, characteristic or code.	Remove ²	May be included.

A **Data Use Agreement (DUA)** is an agreement required by the Privacy Rule between a covered entity and a person or entity that receives a limited data set. The DUA must state that the recipient will use or disclose the information in the limited data set only for specific limited purposes.

Covered entities must condition the disclosure of the limited data set on execution of a DUA, which

¹ Even if all of the information listed in this column is removed, if the researcher knows that any remaining information in the data set could be used to re-identify a patient (e.g., a diagnosis code where the disease is very rare), then the data set is not considered de-identified.

² If links must be maintained in the data set for potential later re-identification, they must be completely unrelated to any of the above elements. For example, a patient’s initials or a scrambled social security number are not permitted in a de-identified data set. A subject code that reflects the order in which subjects were enrolled into a trial would be permitted.

Please contact the IRB Office at (801) 581-3655 or irb@hsc.utah.edu for additional guidance.

Investigator Guidance Series

University of Utah Institutional Review Board

- establishes the permitted uses and disclosures of such information by the recipient, consistent with the purposes of research, public health, or health care operations;
- limits who can use or receive the data; and
- requires the recipient to agree not to re-identify the data or contact the individuals.

In addition, the DUA must contain adequate assurances that the recipient will use appropriate physical, technical and administrative safeguards to prevent use or disclosure of the limited data set other than as permitted by HIPAA and the data use agreement, or as required by law.

These assurances are similar to the requirements for business associate contracts. As with such agreements, the recipient is required to report to the covered entity any improper uses or disclosures of which it becomes aware.

Alternatively, if a covered entity becomes aware of a violation of the data use agreement, it must take reasonable steps to remedy the problem or, if unsuccessful, discontinue disclosure of PHI to the recipient and report the problem to DHHS.

The minimum necessary standard governs covered entities' disclosures, and recipients' uses, of limited data sets. The covered entity may place reasonable reliance that a requested disclosure is indeed the minimum necessary for the stated purposes, or make its own determination that a lesser amount of information would be sufficient.

When a Data Use Agreement (DUA) is Required for a Limited Data Set (LtdDS)

If a researcher is using a LtdDS created by a person or entity outside of the University of Utah's Covered Entity and you have received a DUA from that person or entity, then please refer to that form for a list of elements that must be present in the agreement. Forward the agreement to the IRB for signature as necessary.

If you are disclosing a LtdDS to a person or entity outside of the University of Utah Covered Entity, please obtain that entity's or institution's signature on the U of U standard Data Use Agreement and forward the agreement to the IRB for signature.

In order for a DUA to be valid, it must be signed by the appropriate institutional officials. Use of a LtdDS without a valid Data Use Agreement in place is a violation of the Privacy Rule. Whether you are using a University of Utah standard Data Use Agreement, or a Data Use Agreement you received from a person or entity outside of the U of U, you must forward the agreement to the IRB for approval and signature by a U of U designated institutional official. Once the Data Use Agreement is signed by all parties, you may begin using the LtdDS.

OPTION 4: Obtain an IRB Waiver of (HIPAA) Authorization

Investigators may request a Waiver of Authorization in the ERICA application by selecting "Waiver of Authorization" in Section 4.1a of the New Study Application. The application will automatically generate the Waiver of Authorization page after the Section has been checked.

If you choose to pursue a Waiver of Authorization, you must:

- 1) list the identifying information you plan to collect or keep a link to,
- 2) explain why the PHI to be used/disclosed is the minimum necessary to accomplish the research objectives,
- 3) explain why the research could not practicably be conducted without the waiver,
- 4) describe your plan to protect the identifiers,
- 5) describe how/when the identifiers will be destroyed, or justify their retention, and
- 6) describe the measures you will take to ensure the PHI will not be reused or disclosed to unauthorized persons or entities.

Please contact the IRB Office at (801) 581-3655 or irb@hsc.utah.edu for additional guidance.

Investigator Guidance Series

University of Utah Institutional Review Board

References & Links

*Data Use Agreement
Form*

[http://www.research.utah.edu/irb/forms/hipaa/word/Data_Use_Agreement\(Research\)-Uo%20U-Sep08.doc](http://www.research.utah.edu/irb/forms/hipaa/word/Data_Use_Agreement(Research)-Uo%20U-Sep08.doc)

*HIPAA Standards for
De-Identification and
Re-Identification of PHI*

http://intranet.uuhsc.utah.edu/policy/index.cfm?fuseaction=cPolicies.policy&fileId=2106&fileVersionId=2&policiesAsOfDate=10/21/2008&sess_id

*IRB HIPAA Forms
Templates (Consent
Documents, Data Use
Agreements, etc.)*

<http://www.research.utah.edu/irb/forms/hipaa/index.html>

Please contact the IRB Office at (801) 581-3655 or irb@hsc.utah.edu for additional guidance.