ILLINOIS

Office for the Protection of Research Subjects

Research Guidance Document

HIPAA PRIVACY RULE & AUTHORIZATION

Definitions

Breach. The term 'breach' means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

Disclosure. With regards to Protected Health Information (PHI), a *disclosure* means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information (45 CFR 46 160.103).

HIPAA Privacy Rule. 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, and describes the ways in which covered entities can use or disclose PHI, including for research purposes. The Privacy Rule applies directly to "covered entities" and is designed to protect individuals' health information.

Protected Health Information (PHI). Individually identifiable health information. Information about the past, present, or future physical or mental health of an individual that identifies or could be used to identify the individual and is created or received by a Covered Entity. (45 CFR 160.301, 164.501; information about the provision of health care and payment for health care is included; some educational and employment records are excluded.)

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. Obtain an Alteration of Authorization
3. Use a de-identified Data Set that contains no PHI
4. Use a Limited Data Set with an effective Data Use Agreement in place, as applicable
5. Obtain an IRB Waiver of (HIPAA) Authorization
6. Preparatory to Research, and Research on Decedents' Information

Local Institutional Review Boards (IRB) have the authority to make determinations about whether the proposed procedures of research under their purview 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).
    - 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
    - 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
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: Obtain an Alteration of Authorization

Research that would have a waiver of documentation of consent under the Common Rule can be addressed under HIPAA as an *alteration* to the authorization. One of the core elements of a valid authorization under HIPAA is *the signature of the individual* (45 CFR 164.508(c)(vi)). If granted by the IRB, the Alteration of Authorization allows the researcher to omit one of the core elements of a valid authorization; in this case, the signature of the participant. This will allow the researcher to use a Consent Cover Letter (CCL) to obtain authorization instead of a full consent document, provided the research qualifies to use the CCL and can justify the alteration by satisfying all of the criteria outlined in 45 CFR 164.512.

OPTION 3: Use a De-identified Data Set That Contains No PHI

A De-Identified Data Set excludes the 18 PHI Identifiers. De-identified health information, as described in the Privacy Rule, is not PHI, and thus is not protected by the Privacy Rule. There are no restrictions on the use or disclosure of 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; The person certifying statistical de-identification must document the methods used as well as the result of the analysis that justifies the determination); 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 4: 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)). Because limited data sets may contain identifiable information, they are still PHI.

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 Limited Data Set excludes the 16 of 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.
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 subject to the Privacy Rule. Limited Data Sets may be used or disclosed for research, public health, and other limited purposes, but only by those who sign a Data Use Agreement (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 and 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. *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.*	Remove	Remove postal address information other than city, town, state or zip code.

[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.

All elements of dates (except year); plus age and any date (including year) if age is over 89. *Examples: date of birth, date of death, date of admission, date of discharge, date of service.*	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). *DNA is not considered a biometric identifier for purposes of HIPAA.*	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 the covered entity and the intended recipient of a limited data set. It establishes the ways in which the information in the limited data set may be used and how it will be protected. The DUA is the means by which covered entities obtain satisfactory assurances that the recipient of the limited data set will use or disclose the PHI in the data set only for specified purposes. ***Even if the person requesting a limited data set from a covered entity is an employee or otherwise a member of the covered entity's workforce, a written data use agreement meeting the Privacy Rule's requirements must be in place between the covered entity and the limited data set recipient.*

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) establishes the permitted uses and disclosures of such information by the recipient, consistent with the purposes of research, public health, or health care operations;
2) limits who can use or receive the data; and
3) 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 require the recipient 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.

Ensuring the Data Use Agreement (DUA) for a Limited Data Set (LtdDS) is Valid
If a researcher is using a LtdDS created by a person or entity outside of the Covered Entity and you have received a Data Use Agreement (DUA) from that person or entity, then please contact the Sponsored Programs Administration (SPA). SPA will forward the DUA to OPRS for signature.

[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.

If you are disclosing a LtdDS to a person or entity outside of the University of Illinois Urbana-Champaign, please contact the Office of Technology Management (OTM) to request a Data Use Agreement. OTM will forward the agreement to OPRS 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. Once the Data Use Agreement is signed by all parties, you may begin using the LtdDS.

OPTION 5: Obtain an IRB Waiver of (HIPAA) Authorization

Investigators may request a Waiver of Authorization in the IRB application by selecting "Waiver or Alteration of Authorization" on the **HIPAA and the Covered Entity** page in 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.

OPTION 6: Preparatory to Research, and Research on Decedents' Information

Section 164.512 of the Privacy Rule also establishes specific PHI uses and disclosures that a covered entity is permitted to make for research without an Authorization, a waiver or an alteration of Authorization, or a data use agreement. These limited activities are the use or disclosure of PHI preparatory to research and the use or disclosure of PHI pertaining to decedents for research.

For activities involved in **preparing for research**, covered entities may use or 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 a researcher 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 in the course of review, and
(3) the PHI for which use or access is requested is necessary for the research.

Researchers should note that any preparatory research activities involving human subjects research as defined by the HHS Protection of Human Subjects Regulations, which are not otherwise exempt, must be reviewed and approved by an IRB and must satisfy the informed consent requirements of HHS regulations.

To use or disclose **PHI of the deceased for research**, covered entities are not required to obtain Authorizations from the personal representative or next of kin, a waiver or an alteration of the Authorization, or a data use agreement. However, the covered entity must obtain from the researcher who is seeking access to decedents' PHI

(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, at the request of the covered entity, of the death of the individuals whose PHI is sought by the researchers.

References & Links

Guidance regarding Methods for De-Identification of PHI	*https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html*
NIH HIPAA Privacy Rule Information for Researchers	*http://privacyruleandresearch.nih.gov/pr_08.asp*