
HIPAA and Human Subjects Research

Content Authors

- ▶ **Anita Cava, J.D**
 - ▶ **Reid Cushman, Ph.D.**
 - ▶ **Kenneth Goodman, Ph.D.**
- University of Miami Ethics Programs

This new module on the changes in the privacy rules and regulations consists of 8 sections, and will take you between 10 and 15 minutes to complete. You will then be directed to take a short quiz.

Introduction and Background

The Health Insurance Portability and Accountability Act (HIPAA) was a milestone in the federal effort to facilitate the transfer of health care data. HIPAA, passed by Congress in 1996, also mandates regulations protecting the confidentiality of health information, and in this way supplements the patchwork of state protections. Issued by the U.S. Department of Health and Human Services (HHS) in 2000 and revised in August of 2002, the HIPAA Final Privacy Rule protects oral, written and electronic Protected Health Information (PHI). PHI is any information that "relates to the past, present or future physical or mental health or condition of an individual." The regulations went into effect April 14, 2003, for most organizations.



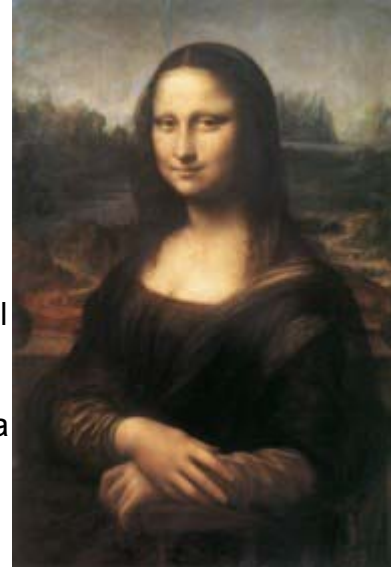
This CITI module provides an introduction to the HIPAA Privacy Rule. The HIPAA Privacy Rule also requires your institution to provide additional education ([workforce training](#)) about your institution's privacy policies and procedures.

What is protected health information (PHI) under HIPAA?

Protected health information is defined under HIPAA as *individually identifiable* health information. *Identifiable* refers to data explicitly linked to a particular individual as well with data that could enable individual identification.

Identifiers include obvious ones like name and Social Security number. Others are:

- ▶ All geographic subdivisions smaller than a state, including street address, city, county, precinct, Zip Code, and their equivalent geocodes.
- ▶ 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.
- ▶ Voice and fax telephone numbers.
- ▶ Electronic mail addresses.
- ▶ Medical record numbers, health plan beneficiary numbers, or other health plan account numbers.
- ▶ Certificate/license numbers.
- ▶ Vehicle identifiers and serial numbers, including license plate numbers.
- ▶ Device identifiers and serial numbers.
- ▶ Internet Protocol (IP) address numbers and Universal Resource Locators (URLs).
- ▶ Biometric identifiers, including finger and voice prints.
- ▶ Full face photographic images and any comparable images.
- ▶ Any other unique identifying number, characteristic, or code.



Information is considered de-identified if all of the above have been removed,

and there is no reasonable basis to believe that the remaining information could be used to identify a person.

As an alternative to using fully de-identified information, HIPAA makes provisions for a limited data set from which direct identifiers (like name and address) have been removed, but not indirect ones (such as age). Limited data sets require data use agreements between the parties from which and to which information is provided.



Authorization for disclosures of protected health information

Under HIPAA, the general rule is that researchers must have valid **authorization** for all uses and disclosures of PHI in connection with research.

- ▶ "Protected health information (PHI)" means individually identifiable health information transmitted or maintained in any form or medium.
- ▶ "Use" means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of such information *within the entity that maintains such information*.
- ▶ "Disclosure" means the releases, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. A valid research authorization must be in writing, must be signed by an individual, and must contain certain elements.

A valid authorization must include specific elements:

- ▶ A description of the PHI being used.
- ▶ A statement of the purpose of the use of PHI.
- ▶ A list of those who can use the PHI.
- ▶ A list of those who can receive the PHI, including the possibility of re-disclosure.
- ▶ A statement that once PHI is disclosed by the recipient it may no longer be protected by the Privacy Rule.
- ▶ Information about the expiration of the authorization.
- ▶ Information about the right to revoke the authorization.



If an actual expiration date is not provided, then a note pointing this out is required. A statement explaining an expiration event such as the end of the research project is also acceptable.

The authorization must either explain how to revoke the authorization or refer to the covered entity's privacy notice, if that is applicable. A revocation must be in writing and can be made at any time. If a research study has already relied on information

disclosed before the authorization was revoked, that information may still be used. Once the authorization is revoked, no further disclosure of PHI is allowed under that authorization.

The covered entity – that is, "health plans, health providers and health clearinghouses" or "any entity in the health sector that uses health information in the regular course of business" – may require the authorization as a condition of providing research-related treatment. Authorizations for research disclosures may be combined with other documents, such as a consent form.

Each covered entity that discloses PHI determines the required format for its HIPAA authorization. Organizations/individuals that receive PHI from a covered entity do not determine the adequacy or format of the authorization for the disclosing covered entity.

Waivers of authorization

The Privacy Rule allows exceptions to the authorization requirement.

The first two exceptions do not require IRB/Privacy Board waivers, but rather a representation made to the covered entity, presumably via the privacy officer. However, state law or institutional policy may differ and in fact require IRB review of these two types of research. More stringent state law pre-empts HIPAA.

1. Activities preparatory to research.

An investigator may tell the covered entity that the activity is solely **preparatory to research**, for instance for the purpose of designing a protocol; that the information requested is the minimum necessary to do the activity; and that no PHI will be removed from the covered entity's premises.



2. Use of PHI from decedents.

Under this circumstance, an investigator tells the covered entity that the research involves only the protected health information of deceased persons, that the data are essential (minimum necessary), and that it is not practical to obtain an authorization.

3. Research activities under a waiver of authorization.

- ▶ A request from an investigator to conduct research without an authorization requires the IRB or a Privacy Board to grant a waiver. In order to do so, all the following factors must be documented:
 - The use or disclosure involves no more than a minimal risk to the individuals, based on the following items:
 - A plan to protect identifiers from improper use and disclosure.
 - A plan to destroy the identifiers as soon as possible, unless there is a health or research justification for keeping them or the law requires that identifying information be kept; *and*
 - A written assurance that the protected health information will not be reused or disclosed to any other person or entity except as required by other laws.
 - The research could not realistically be performed without the alteration or waiver and
 - The research could not be conducted without access to and use of the protected health information.

To approve a waiver of authorization, an IRB/ Privacy Board must be composed of members with the background and competence to review the project, with at least one person not affiliated with the project, institution, or related to anyone affiliated with the project. The IRB / Privacy Board must take steps to assure that participating members do not have a conflict of interest.

A waiver of authorization is not the same as a waiver of informed consent. The approach taken by the HIPAA Privacy Rule is similar to that required by the Common Rule, which has long governed federally funded research. The Common Rule requires that express consent be obtained prior to engaging in research involving human subjects, but provides that a waiver may be granted by an IRB if certain conditions are met, including that there is "no more than minimal risk of harm to subjects" and "the research could not practicably be

carried out without the waiver" (45CFR46.116).

"Minimum Necessary" Standard

HIPAA has established that the use and disclosure of PHI in situations other than medical treatment must be kept to the minimum necessary to meet the need of the research project. In keeping with this approach, PHI collected during research under an IRB or Privacy Board waiver can



only be used or disclosed to the extent that it is the minimum necessary. However, research done with patient authorization is *not* subject to the minimum necessary standard for use and disclosure of PHI. What counts as "minimum necessary" will require judgments. Investigators unsure of whether a particular use meets this criterion should contact their IRB or Privacy Board – which, of course, should have in place some mechanism or policy for responding to such inquiries.

Note that here, too, state law or institutional policy may differ from the HIPAA standard and should be considered in making this determination. If it is stricter or more stringent, a state statute or institutional policy will pre-empt HIPAA.



The Privacy Rule provides a compromise between identifiable PHI and fully de-identified PHI.

Under HIPAA, a limited data set is one in which identifiers other than city, state, Zip Code and dates (of service, birth or death) have been removed. This allows researchers

to conduct studies requiring dates or localities without requesting a waiver of authorization. In contrast, "de-identified" data under the HIPAA rule eliminates the inclusion of locations smaller than states, a zip code identifier smaller than the first 3 digits of the zip code, all dates except for years, and ages over 89.

HIPAA allows a researcher who wishes to use a limited data set to enter into an appropriate "data use agreement" with a covered entity; providing the limited data set without an authorization or a waiver of authorization from an IRB or Privacy Board.

The agreement must list the permitted use and disclosures of the PHI being used and require that the researcher will:

- Use appropriate safeguards for the information;
- Not use or further disclose the information other than as agreed or as required by law;
- Report any uses/disclosures that were not permitted;
- Ensure that anyone who has access to the data also agrees to these restrictions; and
- Not identify the information or contact the individuals.

Disclosure Accounting Requirements

The HIPAA Privacy Rule allows patients to request an accounting of disclosures of their PHI for research. Research based upon a waiver is subject to HIPAA's disclosure accounting requirement, whereas authorization-based research is not. Routine disclosures required to federal agencies such as the FDA are subject to the accounting requirement. Research involving "decedents" and "reviews preparatory to research" also require accounting by the covered entity. This disclosure accounting requirement can be met by providing individuals with a list of all protocols for which their PHI may have been disclosed pursuant to a waiver or other HIPAA allowable exceptions to use of PHI such as reviews preparatory to research and research on decedents. The information provided would also include the researcher's name and contact information.



A researcher using de-identified data, where the information cannot be traced to a particular individual, or protected health information disclosed by a covered entity in a limited data set under an appropriate data use contract, is exempt from the disclosure accounting requirements.

As a practical and administrative matter, institutions should have established mechanisms, policies, and procedures for annotating records to show that information contained in them has been disclosed for research.

Revised 9-03-06