What is HIPAA?

The ***Health Insurance Portability and Accountability Act of 1996 (HIPAA)*** contains provisions to protect the confidentiality and security of personally-identifiable information that arises in the course of providing health care. The intention of HIPAA is to protect patients from inappropriate disclosures of ***Protected Health Information (PHI)*** that can cause harm to a person's insurability, employability, etc. In order to understand how HIPAA affects research, there are a few important terms that are defined by the law.

A ***covered entity*** is the organization that has to comply with HIPAA. The University of California is a Hybrid Covered Entity because, in addition to providing health care at its medical facilities, it also has other organizational activities such as education and research.

Note: UC Merced is not a covered entity, therefore, data generated by UC Merced researchers is not covered under HIPAA unless the data is generated in collaboration with a covered entity. HIPAA compliance is also applicable when a UC Merced researcher receives data from a covered entity to be used for research purposes.

The HIPAA Privacy Rule governs ***PHI*** which is defined as information that can be linked to a particular person (ie., is person-identifiable) that arises in the course of providing a health care service.

When PHI is communicated inside of a covered entity, this is called a ***use*** of the information. When PHI is communicated to another person or organization that is not part of the covered entity, this is called a ***disclosure***. HIPAA allows both use and disclosure of PHI for research purposes, but such uses and disclosures have to follow HIPAA guidance and have to be part of a research plan that is reviewed and approved by an Institutional Review Board (IRB).

There are 18 PHI identifiers as follows:

Name	Address (all geographic subdivisions smaller than state, including street address, city, county, ZIP code)	All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death and exact age if over 89)
Telephone numbers	FAX number	E-mail address
Social Security number	Medical record number	Health plan beneficiary number
Account number	Certificate/license number	Any vehicle or other device serial number
Device identifiers or serial numbers	Web URL	Internet Protocol (IP) address numbers
Finger or voice prints	Photographic images	Any other characteristic that could uniquely identify the individual

Definitions

Authorization: Under HIPAA, the granting of rights to access PHI. Authorization is required by HIPAA for disclosures or uses other than for Treatment Payment Operations (TPO), which are covered in the Notice of Privacy Practices. Treatment cannot be conditioned on granting of an authorization. An authorization is a specific, detailed document requesting patient-subject permission for the use of covered PHI.

Covered Entity: A covered entity is a health plan, a health care clearinghouse, or a health care provider transmitting health information, and is, therefore, subject to the HIPAA regulations.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of PHI outside the entity holding the information. Disclosure of PHI requires a specific authorization under HIPAA except if disclosure is related to the provision of TPO (Treatment Payment Operations) of the entity responsible for the PHI or under a limited set of other circumstances, such as public health purposes.

Health Information: Any information, whether oral or recorded in any form or medium, that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually Identifiable Health Information is any information created, used, or received by a researcher (from a covered entity) that relates to:

- The past, present, or future physical or mental health or condition of an individual,
- The provision of health care to an individual, or
- The past, present, or future payment for the provision of health care to an individual with respect to which there is a reasonable basis to believe the information can be used to identify the individual. The collection of individually-identifiable health information for research constitutes human subjects research.

Minimum Necessary Standard: The least information reasonably necessary to accomplish the intended purpose of the use, disclosure, or request of PHI.

Research Health Information (RHI) is defined as data used in research that would be personally identifiable but not considered PHI and is therefore not subject to the HIPAA Privacy and security Rules. The key distinction between RHI and PHI is that PHI is associated with or derived from a healthcare service event, i.e. the provision of care or payment for care. RHI is covered by other state and federal laws for privacy and confidentiality of research health information.

Protected Health Information (PHI) is defined as any individually identifiable health information collected or created as a consequence of the provision of health care by a covered entity, in any form, including verbal communications. PHI is information that can be linked to a particular person and that is created, used, or disclosed in the course of providing a health care service (i.e., diagnosis or treatment).

What Does the Privacy Rule Have To Do With Research?

The Privacy Rule is a nickname for DHHS' regulation, "Standards for Privacy of Individually Identifiable Health Information", applicable to entities covered by HIPAA. HIPAA affects only that

research which uses, creates, or discloses PHI. Researchers have legitimate needs to use, access, and disclose PHI to carry out a wide range of health research studies. The Privacy Rule protects PHI while providing ways for researchers to access and use PHI when necessary to conduct research. In general, there are two types of human research that would involve PHI:

- Studies involving review of existing medical records as a source of research information. Retrospective studies, such as chart reviews, often do this. Sometimes prospective studies do it also, for example, when they contact a participant's physician to obtain or verify some aspect of the participant's health history.
- Studies that create new medical information because a health care service is being performed as part of the research, such as testing of a new way of diagnosing a health condition or a new drug or device for treating a health condition. Virtually all sponsored clinical trials that submit data to the U.S. Food and Drug Administration (FDA) will involve PHI.

What is the IRB's Role?

The IRB acts as a Privacy Board (required by HIPAA) to review the use/disclosure of PHI and to determine whether the subjects should sign an "Authorization" (an addendum to the consent to participate in research) or if a Waiver of Authorization (roughly analogous to a Waiver of Consent under the Common Rule) may be granted.

Note: UC Merced is not a covered entity, therefore, data generated by UC Merced researchers is not covered under HIPAA unless the data is generated in collaboration with a covered entity. HIPAA compliance is also applicable when a UC Merced researcher receives data from a covered entity to be used for research purposes.