HIPAA Research and Privacy Board Policy

Introduction

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") was written to allow for insurance portability but also as a Privacy Rule to protect the privacy and security of a person's identifiable health information. The purpose of this policy is to provide researchers with the information they will need to comply with the Privacy Rule associated with HIPAA.

The HIPAA Privacy Rule establishes the conditions under which Protected Health Information (PHI) may be used or disclosed by covered entities for research purposes. CWRU is a hybrid entity and as such, must abide by the HIPAA Rules for the use and disclosure of PHI under its jurisdiction (see 45 CRR 160 and 164) for related purposes. CWRU and its affiliated hospitals empower their IRBs to act as Privacy Boards on behalf of each Covered Entity.

Definitions

Authorization is permission to gain access to PHI. Authorization may be obtained by signing a separate document or incorporating authorization language into a consent form.

HIPAA (Health Insurance Portability and Accountability Act) – HIPAA regulates the transfer and collection of PHI between and within covered entities defined as:
(a) health care plans;
(b) health care clearinghouse, and
(c) health care providers who electronically transmit any health information.
The Health Insurance Portability and Accountability Act (HIPAA) went into effect on April 14, 2003 to insure the portability of insurance coverage as employees moved from job to job, increase accountability and decrease fraud and abuse in healthcare; and improve the efficiency of the health care payment process, while at the same time protecting a patient's privacy.

Covered Entity: HIPAA applies to "Covered Entities," defined by the Privacy Rule as a healthcare provider that conducts certain transactions in electronic form, a healthcare clearinghouse, a health plan, or a business associate (person or organization) performing a function on behalf of the Covered Entity for which access to protected health information is needed.

Hybrid Entity: CWRU is permitted to designate itself as a "hybrid entity," which allows it to apply the Privacy Rule only to those parts of CWRU that, if standing alone, would be a Covered Entity. As a hybrid entity, CWRU must designate its "healthcare components," which includes departments that provide support for healthcare components. Healthcare components at CWRU are:

- CWRU School of Dental Medicine

- CWRU School of Dental Medicine Faculty Practice
- CWRU Student Self-Insured Health Plan & Optional Dependent Medical Plan
- CWRU Employee Health Plan
- Prion Disease Pathology Surveillance Center

Privacy Rule establishes the minimum federal standards for safeguarding the privacy of individually identifiable health information (also referred to as protected health information (PHI)). The Department of Health and Human Services (DHHS) issued the Privacy Rule in order to implement the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which required compliance as of April 14, 2003 (see 45 CFR part 160 and subparts A and E of part 164). The Privacy Rule includes the standards for an individual's privacy rights, to enable them to understand and control how their health information is used. Within DHHS, the Office for Civil Rights (OCR) is authorized to implement and enforce the Privacy Rule.

Protected Health Information (PHI) is individually identifiable health information, including demographic and genetic data that is collected from an individual, and:

1. is created or received by a health care provider, health care entity, health plan, public health authority, employer, life insurer, school/university, or health care clearing house; AND
2. relates to past, present or future physical or mental health or condition of the individual; or the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; AND
3. identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual; AND
4. is transmitted or maintained in any form or medium, whether electronic, paper or oral (see 45 CFR 160.103).

Research Privacy Board is a review body which acts upon the HIPAA Privacy Rule's authorization requirements for use or disclosure of PHI for a specific research protocol. The Research Privacy Board's authority is limited to approval of privacy language; approval of requests for a waiver or alteration of the Privacy Rule's authorization requirements; approval for the use of PHI from deceased individuals; and review of HIPAA compliance allegations. CWRU and its affiliated hospitals empower their IRBs to act as Privacy Boards on behalf of each Covered Entity.

Research, as defined in the Privacy Rule, is a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge (45 CFR 164.501).

Policy

Any research study involving collection or use of PHI must comply with HIPAA. It is the responsibility of the investigator to comply with HIPAA Authorization/Privacy Rule

requirements, and the policies relating to use of PHI in research as outlined by the CWRU HIPAA Policies.

The HIPAA equivalent of consent for use or disclosure of a person's PHI. Required elements for an authorization form include:

a. Specific description of what PHI will be used or disclosed
b. Who may use or disclose PHI
c. Who may receive the PHI
d. Purpose of the use or disclosure
e. Statement of how long the use or disclosure will continue. "No expiration date" is allowed for research purposes.
f. Right to revoke authorization.
g. Notice that the information may be disclosed to others not subject to the Privacy Rule.
h. Right to refuse to sign authorization
i. The subject must sign the form and receive a signed copy for the authorization to be valid.

The HIPAA authorization can be a separate document from the consent form, or the required elements can be incorporated into the consent form. Authorization should be obtained in each of the following two circumstances:

a. When requesting permission from a patient to have their name, address and phone number or other health information released to an investigator for recruitment into a research study; or
b. When enrolling a subject into a specific research study to request permission to collect their PHI as related to the research study. This second circumstance occurs simultaneously with the consent process.

Waiver of Authorization: Waiver of Authorization can be obtained if the following three criteria have been met:

1. The research is no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
   a. an adequate plan to protect the identifiers from improper use and disclosure
   b. an adequate plan to destroy the identifiers at the earliest opportunity
   c. adequate written assurances that the PHI will not be reused or disclosed to any other person or entity.
2. The research cannot practicably be carried out without a waiver; and
3. The research cannot be done without this specific PHI.

When applying for a waiver of authorization, the investigator must complete the "Waiver of HIPAA Authorization" form. Uses and disclosures of PHI pursuant to the waiver must be limited to the minimum necessary to achieve the research purpose. This means that if you use a waiver to collect PHI, you must only collect the bare minimum of information from patient records that are necessary to answer the research question.

Examples of when a waiver may be utilized:
Example 1. A researcher would like to conduct a retrospective chart review at Treatment Center X. Waiver of consent is appropriate because it is impractical to attempt to contact the many patients that a retrospective chart review entails, and the chart review is considered to be minimal risk. [NOTE: If only de-identified data are recorded, then it is not considered to be PHI, and no waiver of authorization is required.]
Example 2. A researcher has a list of patients who were involved in his previous study and would like to re-contact these patients to participate in a follow-up study. The investigator would apply for a waiver of authorization to pull medical records to find the patients' current phone numbers. The investigator will still need to use an authorization form when enrolling the subjects, but in order to obtain this PHI before contacting the patients, a waiver is required.

De-Identified Data: Health information is considered de-identified when it does not identify an individual and the health care entity has no reasonable basis to believe that the information can be used to identify an individual.
Research involving de-identified data will not be required to adhere to HIPAA regulations requiring authorization.
De-identified data includes **none** of these 18 identifying links:

1. name
2. address including city, county, precinct, zip code
3. all elements of dates (except year) for dates directly linked to an individual (birth date, admission date, discharge date, date of death) [For all subjects over 89 years, all elements of dates including year that are indicative of their age cannot be used; however, age can be aggregated into a 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/license number
12. vehicle identifiers
13. device identifiers
14. Web Universal Resource Locators/Identifiers
15. Internet Protocol address numbers
16. Biometric identifiers including finger or voice prints
17. Full face photographs and comparable images
18. Any other unique identifying number, characteristic, or code

Limited Data Set. Limited Data Sets include research that falls under HIPAA regulations but does not require researchers to obtain authorization or waiver of authorization. Researchers can collect data that retains the following types of identifiers:

a. Admission, discharge and service dates
b. Birth date
c. Date of death
d. Age (including over age 89)
e. Geographic information (except street addresses) such as city, state, and five-digit zip code

Researchers using a limited data set will be able to use the data only for research purposes but may not use the limited data set to contact subjects.

Recruitment of Subjects. No researcher may contact potential subjects with whom the researcher does not have a clinical relationship, without authorization. If a researcher wishes to recruit subjects into a study, then the researcher must request that a health care provider who does have a clinical relationship with these subjects obtain authorization from the subjects to release information to the researcher. Alternatively, the care-providing physician can give the patient the contact information about the study.

The HIPAA rule does not apply at research sites outside of the United States where individually identifiable information may be collected. Once the individually identifiable information is transferred to a HIPAA-covered facility then any individually-identifiable health information becomes PHI by virtue of its being held by a facility covered by HIPAA. Once data is transferred to a HIPAA covered component, all HIPAA regulations apply.

All investigators conducting research outside the United States must comply with HIPAA requirements for all studies unless the investigator requests a waiver of HIPAA based on criteria outline in 45 CFR 164.512. This includes when the investigator conducting research outside the United States sends PHI back to the United States in any form.