THE PRIVACY RULE ("HIPAA") IN RESEARCH

11/20/2023

I. OVERVIEW

The U.S. Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996 to protect health insurance coverage as a worker changes employment; to reduce fraud; and to establish national standards for electronic healthcare transactions. Also reflected in HIPAA is a concern for the privacy of a person and the confidentiality of their health information.

Federal privacy regulations implemented as a result of HIPAA (45 CFR 160 & 164, referred to as the "Privacy Rule") apply to "covered entities", which are defined as health plans, health care clearinghouses or health care providers who transmit any health information electronically. Individual investigators must comply with the regulations if they are also health care providers who electronically transmit health information or if they are employees or members of a covered entity.

II. DEFINITIONS

1. **Covered Entity –** A health plan; a health care clearinghouse; or a health care provider who transmits any health information in electronic form in connection with a transaction covered under the Privacy Rule
2. **Health Information –** Any information, including genetic information, whether oral or recorded in any form or medium, that:
   - **a.** 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
   - **b.** 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.
3. **Individually Identifiable Health Information –** This is a subset of health information, including demographic information collected from an individual, and that:
   - **a.** Is created or received by a health care provider, health plan, employer, or health care clearinghouse, AND
   - **b.** 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, AND
   - **c.** That identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual
4. **Person –** A natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private
5. **Protected Health Information –** Individually identifiable health information

that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium.

Protected health information excludes individually identifiable health information:

a. In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
b. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv)
c. In employment records held by a covered entity in its role as employer
d. Regarding a person who has been deceased for more than 50 years

III. PROTECTED HEALTH INFORMATION

The Privacy Rule designates individually identifiable health information transmitted or maintained by a covered entity in any form (electronic, written or oral) as "protected health information" (PHI), and establishes the conditions under which investigators may access and use this information in the conduct of research. PHI is any information that relates to the past, present or future physical or mental health or condition of an individual who can be identified by any of eighteen identifiers. These identifiers are:

- Names
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the 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.

    According to the August 2002 Final Modifications to the Privacy Rule and utilizing the 2000 Census data, there are 17 restricted three-digit ZIP codes that correspond to populations of 20,000 or fewer persons and must be changed to 000 to be de-identified: 036, 059, 063, 102, 203, 556, 692, 790, 821, 823, 830, 831, 878, 879, 884, 890, and 893

- 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
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers

- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

Per guidance from the federal government, a patient's or subject's initials are included in the category of any other unique identifying number, characteristic or code.

IV. AUTHORIZATION

Except as otherwise permitted, the Privacy Rule requires that a research subject "authorize" the use or disclosure of their PHI in order to be utilized in research. This authorization is distinct from the subject's consent to participate in research, which is required under the Common Rule and FDA regulations. Just as a valid consent under Common Rule and FDA regulations must meet certain requirements, a valid authorization must contain certain core elements (45 CFR 164.508(c)).

In accordance with DUHS practice, this authorization is typically incorporated into the consent form. A sample consent and authorization form, which includes HIPAA language, is available on the DUHS IRB website.

A subject may revoke this authorization at any time. However, the investigator and the institution may continue to use and disclose PHI that was obtained before the subject revoked authorization to the extent that the investigator or institution has acted in reliance on the authorization. This includes, for example, the use or disclosure of PHI in order to maintain the integrity of the research (45 CFR 164.508(b)(5)(i)).

While consent may be given verbally under the Common Rule and FDA regulations for minimal risk research activities, authorization under the Privacy Rule must be in writing (signed and dated). Therefore, if a verbal (or other non-written) consent process will be used in research and if that research involves PHI, a waiver request of all elements of HIPAA authorization should be submitted for IRB review and approval.

V. REVIEW PREPARATORY TO RESEARCH

If an investigator wishes to review PHI to determine the feasibility of a research project, they may do so by submitting a Review Preparatory to Research (RPR) (45 CFR 164.512(i)(1)(ii)) form, which is an interactive form completed on the IRB web site: https://irb.duhs.duke.edu/forms/review-preparatory-research-rpr-form. When completing the RPR form, the investigator confirms each of the following:

1. Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research
2. No protected health information is to be removed from the covered entity by

the researcher in the course of the review

3. The protected health information for which use or access is sought is necessary for the research purposes.

VI. DECEDENT RESEARCH

The Common Rule defines a human research subject as a living individual. The Privacy Rule recognizes that the privacy of both living and deceased humans must be protected. If an investigator wishes to conduct a research project using PHI of one or more deceased individuals, prior IRB review may be required.

In making this request, the investigator confirms each of the following:

1. Representation that the use or disclosure sought is solely for research on the protected health information of decedents
2. Documentation, at the request of the covered entity, of the death of such individuals
3. Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes

VII. LIMITED DATA SETS

A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- Names
- Postal address information, other than town or city, State, and zip code
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images

A covered entity may use or disclose a limited data set only for the purposes of research, public health, or health care operations.

A covered entity may use protected health information to create a limited data set, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

A covered entity may use or disclose a limited data set only if the covered entity

obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of the Privacy Rule, that the limited data set recipient will only use or disclose the protected health information for limited purposes.

If a limited data set is received by or disclosed by DUHS, then a data use agreement is required. Such an agreement must establish the proposed uses and disclosures of the data and who is permitted to have access to the data, and must ensure that no other use will be made of the data, no attempt will be made to identify or contact individuals whose data are included in the limited data set, and that appropriate safeguards are in place to protect the data from unauthorized use. Contact the Office of Research Contracts (ORC) to obtain the appropriate agreement.

VIII. DATABASES AND REPOSITORIES

Creation and/or use of research databases or repositories are subject to the Privacy Rule when the data and/or specimens stored therein contain PHI. The creation and/or use of such databases or repositories require either written authorization from participants or a Waiver of Authorization by the IRB.

Each use or disclosure of PHI from a database or repository for research purposes is considered a separate research activity. As such, each use or disclosure requires written authorization from participants or a Waiver of Authorization by the IRB.

Requesting authorization from a research participant for the use or disclosure of their data and/or specimens for current or future **specified** research is permitted if that future research is required to meet the objectives of the protocol under review and is described in the protocol.

Research-related treatment cannot be conditioned on participation in future unspecified research. This includes the collection and storage of data and/or specimens for future unspecified research.

The DUHS IRB will not approve a research protocol that requires the use or disclosure of data and/or specimens for a future unspecified research activity not clearly needed to meet the present protocol's objectives (answer the study questions). However, the storage of data and specimens for future research could occur through a separate protocol and consent/authorization form (if samples are stored in a Duke-controlled facility) or as an optional activity in the present protocol (if samples are stored outside of Duke oversight and control). Subjects must be asked for separate consent and authorization to opt-in to the future unspecified activity. An opt-out alone is not sufficient.

IX. PRIVACY BOARD

The Privacy Rule permits for either a duly constituted IRB or for a Privacy Board as described at 45 CFR 164.512(i)(1)(i)(B) to implement the Rule as it relates to alterations of authorization or waivers of authorization. The Duke University Health System (DUHS) utilizes the IRB for these purposes.

Previous Version Date(s): 10/8/2008, 2/26/2016, 4/18/2021