THE PRIVACY RULE ("HIPAA") IN RESEARCH

02/26/2016

Introduction

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 his/her health information. "Health information" is defined as information about one's physical or mental health or condition, or one's health care, or one's payment for health care. 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.

Protected Health Information

The Privacy Rule defines 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 specific identifiers (name, geographic location smaller than a State or the first three digits of a ZIP code, dates except year, telephone number, fax number, e-mail address, social security number, medical record number, health plan beneficiary numbers, account numbers, certificate or license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, URLs, Internet protocol (IP) address numbers, biometric identifiers, full face photographs, any other unique identifying number, characteristic or code (45 CFR 164.514(b)(2)(i)). 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.

Authorization

Except as otherwise permitted, the Privacy Rule requires that a research subject "authorize" the use or disclosure of his/her PHI to be utilized in the 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 keeping with DUHS IRB policy, this authorization is to be incorporated into the consent form. A sample consent and authorization form, which includes HIPAA language, is available on the DUHS IRB and e-IRB web sites.

The subject's right to revoke authorization is limited. 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, such as

to use or disclose 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. Waiver forms can be found on the DUHS IRB and e-IRB web sites.

Privacy Board

The Privacy Rule (45 CFR 164.512(i)(1)(i)(B)) describes a new board, constituted in a manner similar to an IRB, that has authority to implement the Rule as it relates to alteration of authorization or waiver of authorization. For the Duke University Health System (DUHS), the DUHS IRB is also the Privacy Board.

Review Preparatory to Research

If an investigator wishes to review PHI to determine the feasibility of a research project, s/he may do so by notifying the IRB of a planned Review Preparatory to Research (RPR) (45 CFR 164.512(i)(1)(ii)). By this notification the investigator declares that s/he will use the PHI solely to prepare a research protocol or for similar purposes preparatory to conducting research, that the PHI will not be recorded or disclosed, and that the PHI is necessary to develop the protocol. IRB notification may occur by completion of the interactive RPR form found on the DUHS IRB web site or within the eIRB submission form as part of a specific research protocol.

Decedent Research

The Common Rule defines a human research subject as a living individual. The Privacy Rule recognizes both living and deceased humans as individuals whose privacy must be protected. If an investigator wishes to conduct research project using PHI of one or more deceased individuals, prior IRB review is required. The IRB may request documentation of death (45 CFR 164.512(i)(1)(iii)). When notifying the IRB of plans to use or disclose decedent PHI for research, the Decedent Research Notification form found on the DUHS IRB web site should be completed and include within the eIRB submission for a specific research protocol.

Databases and Repositories

The Privacy Rule recognizes the creation of a research database or a specimen repository to be a research activity if the data/specimens stored contain PHI and requires either written authorization or an IRB approved waiver: http://privacyruleandresearch.nih.gov/

Each use or disclosure of PHI from a database or repository for research purposes is considered a separate research activity and also requires written authorization or an IRB-approved waiver.

Research-related treatment cannot be conditioned on participation in future unspecified research, such as the collection and storage of data/samples for future unspecified research, (45 CFR 164.508).

Requesting authorization from a research subject for the use or disclosure of his/her data/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.

The DUHS IRB will not approve a research protocol that requires the use or disclosure of data/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.

When developing a database or sample repository for the retention of identifiable private information, including PHI, that are existing at the time of IRB submission (already collected/stored in the past or "retrospectively"), see the policy titled *"Research Databases, Biospecimen Repositories, and Contact Lists"* on the policies page of the IRB web site.

When developing a database or sample repository for the retention of identifiable private information, including PHI, that will be collected in the future (prospectively), see the policy on "Research Databases, Biospecimen Repositories, and Contact Lists" on the policies page of the IRB web site.

Research using coded samples already collected may not be subject to the Common Rule but may still be subject to the Privacy Rule or FDA regulations and a submission to the e-IRB is required.

Limited Data Set with a Data Use Agreement

Health information labeled only with one or more of the following is considered a "limited data set" and is still considered PHI: town or city, state, ZIP code (up to nine digit ZIP+4 code), dates, the subject's age (without restriction), and/or an identifying code derived from the subject's PHI (such as subject initials). If a limited data set is received by or disclosed by DUHS, a data use agreement is required.

This 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 appropriate safeguards are in place to protect the data from unauthorized use. Contact the Office of Corporate Research Collaborations (OCRC) to obtain the appropriate agreements.

Previous Version Dates: 10/08/2008