



## **PROTECTING A PARTICIPANT'S PRIVACY INTERESTS AND THE CONFIDENTIALITY AND SECURITY OF THE RESEARCH DATA**

10/08/2008

### **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. The latter 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. The increase in computerized medical records and electronic transfer of information by e-mail, fax and the Internet has increased concern that the confidentiality of health information could be compromised. 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.

With the implementation of the Privacy Rule, research involving humans as research participants must be conducted according to three sets of regulations.

- 1) Investigators doing research involving a product regulated by the Food and Drug Administration (FDA) are required to meet all relevant FDA regulations. Such research ordinarily involves the use of a drug, device or biological product, whether the regulated product has received FDA approval for marketing or remains an investigational product. Regulations describing the need to protect the research subject's privacy are set forth in 21 CFR 56.111(a)(7). This citation also notes the need for ensuring the confidentiality of the subject's data, as do regulations set forth in 21 CFR 50.25(a)(5).
- 2) If the investigator receives U.S. federal funds to support his/her research, or if the investigator is a faculty or staff member of an academic institution that has made a commitment to the U.S. Department of Health and Human Services (DHHS) to follow all federal regulations governing research involving humans subjects, the investigator is required to comply with regulations set forth in 45 CFR 46, including subparts A-D. Subpart A, titled "Basic HHS Policy for Protection of Human Research Subjects", is referred to as the Common Rule. Regulations describing the need to protect the research subject's privacy are set forth in 45 CFR 46.111(a)(7). This citation also notes the need for ensuring the confidentiality of the subject's data, as do regulations set forth in 45 CFR 46.101(b)(3), 46.116(a)(5) and 46.117(c)(1).
- 3) Investigators in institutions that meet the definition of a covered entity must also comply with the Privacy Rule. The regulations described above are unchanged by the Privacy Rule. While they provide for protection of the research subject's privacy and for the confidentiality of his/her research data, such protections are enhanced by the Privacy Rule (45 CFR 160 & 164). It adds a layer of privacy protections for subjects by defining

the ways in which a person's individually identifiable health information may be used in research.

## **What New Considerations Does the Privacy Rule Add to Research?**

### **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)). Health information in this context includes biological specimens if they can be individually identified.

### **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)). The subject must authorize specifically what research information may be shared and who will receive the information, must acknowledge the expiration of the authorization and have the right to revoke the authorization, and must be informed that further disclosure by recipients of the information may not be covered by the federal privacy rules. In keeping with DUHS IRB policy, this authorization is to be incorporated into the informed consent document.

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)).

A sample consent and authorization form, which includes HIPAA language, is available on the IRB web site and the e-IRB web site.

### **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. In the research setting, DUHS has declared that only the IRB may exercise this authority.

### **Review Preparatory to Research:**

The Privacy Rule makes clear that some action to satisfy the Rule is required by the investigator if he/she wants to use PHI for research purposes. This action may be as simple as notifying the

DUHS IRB of the research plan, or as complex as obtaining IRB approval for waiving authorization to use PHI for research. If an investigator wishes to review PHI in order to determine the feasibility of a research project, he/she may do so by notifying the IRB of a planned "Review Preparatory to Research" (45 CFR 164.512(i)(1)(ii)). By this notification the investigator declares that he/she will use the PHI solely as needed to prepare a research protocol or for similar purposes preparatory to research, that the PHI will not be reused or re-disclosed for another purpose or leave the investigator's institution (covered entity), and that the PHI is necessary in order to develop the protocol. Note that a Review Preparatory to Research may be used by an investigator, prior to IRB approval, in order to review the PHI of potential research subjects; however, the investigator may not contact potential subjects to ask for their participation in the research without first obtaining IRB approval of the research. Likewise, the investigator may wish to record PHI or other identifiable private information obtained from a Review Preparatory to Research; however, the investigator may not do so without first obtaining IRB approval of the research and either consent of the research subject or IRB-approved waiver of consent, as described at:

<http://privacyruleandresearch.nih.gov/>

When notifying the IRB of plans for a review preparatory to research, complete the interactive RPR form found on the forms page of the IRB web site.

#### **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 do a research project using PHI of deceased individuals, he/she may do so without concern for Common Rule considerations. But since Privacy Rule considerations must also be met, first the IRB must be notified in order for the investigator to attest that the use of PHI is solely for research using the PHI of decedents, and that the PHI sought is necessary in order to perform the research. 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, use the Decedent Research Notification form found on the forms page of the IRB web site.

#### **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:

<http://privacyruleandresearch.nih.gov/>

Similarly, each use or disclosure of PHI from a database or repository for research purposes is considered a separate research activity. The Privacy Rule does not permit authorization to be given for unspecified future research. Thus the authorization to include PHI in a database and/or specimen repository must specify the research purpose for which the use or disclosure will occur (in this case, the storage in the research database or specimen repository). As with any authorization, this one may either be combined with an IRB approved consent for research or obtained as a separate document, although DUHS IRB policy requires investigators to integrate the authorization contents into the consent document.

Furthermore, research-related treatment cannot be conditioned on participation in future unspecified research, such as the collection and storage of data/samples for future vague research. Requesting authorization from a research subject for the use or disclosure of his/her

data/specimens for future unspecified research is precluded. Requesting authorization from a research subject for the use or disclosure of his/her data/specimens for current or future **specified** research is permitted. In an effort to draw a bright line in the continuum between current or future specified research and future unspecified research, the DUHS IRB has the following policy:

**The DUHS IRB will not approve a research protocol that requires the use or disclosure of data/specimens for a future research activity not clearly needed to meet the present protocol's objectives (answer the study questions). However, the banking of data and specimens for future research could occur through a separate protocol or as an optional activity in the present protocol.**

Banking within DUHS of data/specimens for future research related to the subject's disease, or to any human disease, but not clearly related to the purpose of this research protocol, would be permitted only if the banking request were a separate request that complies with the DUHS policy on data/sample repositories, found at the policies page of the IRB web site.

As noted below, all future research uses and disclosures of PHI from a database or specimen repository require IRB approval. The IRB may require re-consent/authorization if the intended purpose of the future research is outside the original intent of the database/repository. Or, alternatively, the IRB may waive consent and authorization if the requirements for waiver of each are met. Anonymization and de-identification of the data or release as a limited data set with a data use agreement (discussed below) are alternative considerations that may be useful in certain circumstances.

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, see the policy titled "Use of Existing Data or Specimens in Retrospective Research" 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, see the policy on Research Databases and Specimen Repositories on the policies page of the IRB web site.

When planning the use of data/samples for research purposes in such a way that the research may not be subject to the Common Rule and yet in compliance with the Privacy Rule, see the policy on "IRB Determination of Research Not Involving Human Subjects for Research Using Coded Specimens or Coded Identifiable Private Information", available on the policies page of the IRB web site.

**Limited Data Set with a Data Use Agreement:**

The Privacy Rule also introduces a strategy for presenting PHI, such as PHI in a database with or without an associated sample repository, as a limited data set with a data use agreement, thereby fulfilling Privacy Rule requirements (45 CFR 164.514(e)). The PHI can be presented as a limited data set by removing all direct personal identifiers, and removing postal address information except for town or city, State and ZIP code (nine digit ZIP+4 code is permitted). Event dates, the subject's age (without restriction) and an identifying code derived from the subject's PHI (such as subject initials) may be included in the limited data set. Therefore data in a limited data set are not de-identified data.

A data use agreement must be in place to ensure that the limited data set recipient will only use or disclose the protected health information for limited purposes. 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.

Forms for requesting IRB approval of a limited data set with a data use agreement may be found in Attachments 2 and 3 of the policy titled "IRB Determination of Research Not Involving Human Subjects for Research Using Coded Specimens or Coded Identifiable Private Information", available on the policies page of the IRB web site. The DUHS Data Use Agreement extends the HIPAA privacy rule by requiring an "honest broker" restricting the re-linking field to that used in a HIPAA de-identified data set.

### **Other Interactions Between the Privacy Rule and the Common Rule**

As described above (Review Preparatory to Research), DHHS has provided guidance that it considers research to be occurring if the investigator records PHI or other identifiable private information during the search for potential subjects (during the ascertainment/recruitment process). The investigator must therefore first obtain IRB approval of the research, and then obtain either consent and authorization of the subjects or IRB approval of a waiver of consent and authorization.

Waiver of consent under the Common Rule (45 CFR 46.116(d)) requires that the IRB find that:

- a) The research involves no more than minimal risk.
- b) The waiver does not adversely affect the rights and welfare of the subject.
- c) The research could not be practicably carried out without the waiver.
- d) Whenever appropriate, the subjects will be informed of any pertinent information.

When requesting waiver of consent, use the form found on the forms page of the IRB web site.

In order for the IRB also to alter or waive authorization, the Privacy Rule (45 CFR 164.512(i)(2)(ii)) requires that the IRB find that:

- a) Disclosure of the PHI involves no more than minimal risk.
- b) The waiver will not adversely affect the privacy rights or welfare of the subject.
- c) The research could not practicably be carried out without the waiver.
- d) The research could not practicably be carried out without access to the PHI.
- e) The privacy risks are reasonable in relation to the information to be gained.
- f) There is an adequate plan to protect the identifiers from improper use and disclosure.
- g) There is an adequate plan to destroy the identifiers at the earliest opportunity.
- h) There is written assurance that the PHI will not be further disclosed, with a few exceptions specified in 45 CFR 164.512(i)(2)(ii)(A)(3).

When requesting waiver or alteration of authorization, use the form found on the forms page of the IRB web site.

When requesting both waiver of consent and waiver of authorization, use the form found on the forms page of the IRB web site.

## What New Considerations Does the Security Rule Add to Research?

The maintenance of adequate security for the research data is an implied activity under the Common Rule confidentiality requirement (45 CFR 46.111(a)(7)). Confidentiality and privacy cannot be maintained without associated security; this security is explicitly required under the Privacy Rule (45 CFR 164, Subpart C).

At the Duke Health Enterprise (DHE), including, but not limited to, Duke University Hospital, Durham Regional Hospital, Duke Health Raleigh Hospital, and the Duke University Schools of Medicine and Nursing, all systems containing PHI must operate under a Security Design Plan. These Security Design Plans exceed the minimum requirements of HIPAA. Recognizing the variety of systems and work organizations at Duke, the DHE Information Security Officer specified that these organizations could design their own plans as long as the plans met the DHE Information Security Standards. Any system containing human subjects research information that is subject to a Security Design Plan meets the security requirements of the DUHS IRB by specifying the plan to which they adhere (the name of the plan supporting the investigator's activities can be obtained from the local network administrator or departmental IT manager).

Because the scope of the DUHS IRB extends beyond the DHE, the following additional ways of satisfying the security needs of this policy are available:

If another HIPAA compliant security plan exists, cite it. This might be appropriate, for example, for a PI who is a physician admitting to Durham Regional Hospital who is not faculty of the Duke University School of Medicine.

Describe the security approach used for the project, including:

- 1) Have a Security Management Process
  - Information access management
  - Physical Security (e.g., office locked when not in use)
  - Logical security (e.g., users have individual IDs and passwords for networked computers)
- 2) Security Awareness and Training
  - Protection from malicious software (e.g., up to date, and regularly updated, virus protection software)
  - Password management (e.g., how often passwords need to be changed, and policies for strong passwords)
- 3) Security Incident Procedures. A security incident is a serious protocol violation reportable to the IRB. A process to identify, document, and report is required.
- 4) Contingency Plan
  - Backups. Regular backups must be made.
  - Disaster Recovery Plan. (This may be as simple as storage of backups in another building.)
- 5) Encryption. If appropriate, please describe.

These requirements are a subset of the requirements for HIPAA security. Many of the other security requirements, such as workforce clearance and termination procedures, are incorporated as other responsibilities of a project.