

THE HIPAA PRIVACY RULE AND RESEARCH

Abstract: *This article (abstracted from SoCRA's workshop for Investigators and Key Research Staff, December, 2002) provides an overview of the HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule, focusing on its impact on research and researchers. The Privacy Rule protects the privacy of individually identifiable health information by establishing conditions for its use and disclosure by a health plan, health care clearinghouse, and certain health care providers. It requires researchers to obtain written permission—authorization—from individuals before their “protected health information” (PHI) can be used and disclosed. There are some exceptions to the authorization requirement for research. Covered entities, those who must comply with the privacy rule, must also account for disclosures of PHI when decisions are made without an authorization. This article provides basic information about certain provisions of the Privacy Rule in the context of health research. It should not be construed as a formal training session that would meet the Rule's training requirements nor should it be construed to give advice to covered entities. **Those who must comply with the Privacy Rule are encouraged to seek legal counsel to determine how the Privacy Rule could apply to specific research projects.***

The HIPAA Privacy Rule is a new federal law that protects the privacy of individually identifiable health information by establishing conditions for its use and disclosure by a health plan, health care clearinghouse, and certain health care providers. The Privacy Rule was first issued in December 2000 and was issued modified on August 14, 2002. April 14, 2003 is the main compliance date (small health plans have an additional year.)

Table 1 outlines several new concepts that the Privacy Rule

introduces. It does not replace or modify the Common Rule or U.S. Food and Drug Administration (FDA) regulations. The Privacy Rule is supposed to work with these other regulations to increase human subject protections. It exceeds the privacy protections of the Common Rule and FDA regulations by: applying to all research within a covered entity regardless of funding; using a broader definition of “identifiable information” than the Common Rule; requiring authorization for use and disclosure of certain types of health information; and applying to decedents' information.

Many institutions are grappling with whether to be a covered entity or a hybrid entity, in which case the institution is broken up into different parts and only certain parts are covered entities. It may cover a researcher who is employed by a covered entity.

The Privacy Rule protects one type of health information, which it calls PHI. PHI is health information plus an identifier held or maintained by a covered entity. PHI can be transmitted or maintained in any form (e.g., blood pressure, name on a chart, in a database). PHI includes decedents' information. It does not include de-identified health information or biological tissue alone. Research repositories would generally be protected if they contain PHI.

The Privacy Rule defines 18 identifiers:

- 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:

How the Privacy Rule will affect research depends on who you are, where you work, and the type of information you use, collect, or release. If your state law is more stringent or offers greater protection, it supersedes the Privacy Rule.

The Privacy Rule defines covered entities to include health care providers who transmit PHI electronically for any covered HIPAA transaction, e.g., a physician who electronically bills for services, health plans, and health care clearinghouses. A covered entity can be a person or an institution.

TABLE 1
New Concepts Introduced by the Privacy Rule

- An individual's written authorization is required for PHI use or disclosure unless waived or otherwise excepted
- Authorization waivers can be granted by IRBs or privacy boards
- Decedents' information is protected, but authorization is not required
- Accounting and reporting of disclosures are required

- (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
- (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

- 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
- E-mail address
- Social Security numbers
- Medical records and prescription numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- VIN and serial numbers, license plate numbers
- Device identifiers, serial numbers
- Web URLs
- IP address numbers
- Biometric identifiers (fingerprints)
- Full face, comparable photo images
- Unique identifying numbers, unless otherwise permitted for re-clarification

These identifiers must be removed from health information in order for that information to be de-identified. These identifiers apply to the individual and his/her relatives, household members, and employer. Medical charts and case report forms may contain PHI, and therefore, be protected by the privacy rule.

Authorization

In general, the Privacy Rule requires an individual to give written permission—authorization—before a covered entity can use and disclose PHI. However, there are instances where the Privacy Rule permits research activities to continue without individual authorization under limited circumstances.

The authorization form is very important. The goal is to describe the uses and disclosures of the information so the individual is not surprised when the health information goes, for example, to FDA or the sponsor. Table 2 provides an overview of authorizations for research.

The authorization document is comprised of core elements and required statements. Core elements include: description of PHI to be used or disclosed, person(s) authorized to make and receive the requested use or disclosure, purpose for the use or disclosure, and expiration date or event (e.g., “end of the research study” or “none”). Required statements include: the right to

revoke authorization plus exceptions and the process for revoking authorization; ability/inability to condition treatment, payment, or enrollment/eligibility for benefits on authorization; and PHI may no longer be protected by the Privacy Rule once it is disclosed by the covered entity. An individual’s access to his/her PHI may also be during a clinical trial if this restriction is part of the authorization document. The individual must sign and date the form before the PHI can be used and disclosed.

If research is conducted with patient permission, under the Common Rule and FDA regulations, a researcher needs IRB review of the research and the informed consent document. Under the Privacy Rule, a researcher needs individual authorization. The IRB is only required to see the authorization form when the elements of the authorization are combined with the informed consent document.

Research Use and Disclosure of PHI without Authorization

Some research uses and disclosures do not require research participants to give their authorization (Table 3). De-identified PHI means that the 18 elements have been removed and there is no actual knowledge that the subject could be identified. Alternatively, PHI could be statistically de-identified where a statistician certifies that there is a “very small” risk that the information could be used to identify the individual.

**TABLE 2
Authorizations for Research**

- Must be for a specific research study—blanket authorization is not permitted
- Do not need review/approval by an IRB or privacy board
- Must be different from but may be combined with informed consent
- Must contain core elements and required statements in the rule
- Do not have to expire
- Cover creation and maintenance of a research repository or database

**TABLE 3
Research Use and Disclosure of PHI Without Authorization**

- De-identified PHI
- Limited data set with data use agreement
- IRB or privacy board waiver of the authorization requirement
- Activity preparatory to research
- Research on decedents’ information
- Research qualified for the transition provisions
- Disclosure to a public health authority or as required by law

The Privacy Rule permits limited types of indirect identifiers to be released with health information (referred to as a limited data set). Limited data sets exclude the following direct identifiers: names, postal address information, telephone and fax numbers, e-mail addresses, Social Security numbers, medical records and prescription numbers, health plan beneficiary numbers, account numbers, certification/license numbers, VIN and serial numbers, license plate numbers, device identifiers, serial numbers, Web URLs, IP address numbers, biometric identifiers (fingerprints), and full face, comparable photo images. The recipient must sign a data use agreement with the covered entity, which describes the permitted uses and disclosures, identifies who can use and disclose the PHI, and sets requirements for the recipient (e.g., use or disclose information for the specified purposes only). The waiver or alteration of the authorization requirement is used in instances where the research could not practically be conducted if authorization were required. Researchers can obtain documentation that an IRB or privacy board has determined that each of the waiver criteria was satisfied:

- The use or disclosure involves no more than minimal risk because of an adequate plan/assurance: to protect PHI from improper use or disclosure, to destroy identifiers at the earliest opportunity, or that PHI will not be inappropriately reused or disclosed
- The research could not practically be conducted without the waiver or alteration
- The research could not practically be conducted without access to and use of PHI.

IRBs or Privacy Boards will see requests to waive or alter authorization requirements. Such a waiver must be signed and dated by the IRB's chair or their designee.

The Privacy Rule permits covered entities to conduct some activities that are preparatory to research to continue without authorization. To do so, covered entities must obtain some sort of representation from the researchers that the PHI is to be used solely to prepare a protocol or for a similar purpose, PHI will not be removed from the covered entity, and PHI is necessary for research. Authorization is not needed for research recruitment or disclosure to prepare a protocol or a similar activity if no PHI will be removed from the covered entity, when the patient's direct treatment provider discusses possible participation with a patient, and pursuant to a waiver of the authorization requirement. For example, researchers who are part of a covered entity can look through that covered entity's database to see if there is an adequate patient population for a study and to contact the individuals in the database. A direct treatment provider can discuss participation in a trial with his/her patient, but he/she cannot discuss that patient's participation in research with another physician who is not a part of that covered entity.

In conducting research on a decedent's information, the covered entity must receive from the researcher representations that the use or disclosure is solely for research, PHI is necessary for research, and the individual is a decedent (and provide documentation upon the covered entity's request).

Research qualifies for the transition provisions ("grand fathered") if, before the compliance date (usually April 14, 2003), a covered entity obtained either a participant's informed consent or a waiver of informed consent, or express legal permission to use or disclose PHI for research. "Grand fathered" research is conducted as usual. Covered entities that recruit patients for studies after the compliance date

(usually April 14, 2003) will need authorization, unless the activity is otherwise permitted by the Privacy Rule.

Use and disclosure without authorization are permitted if required by law, or if for public health activities, for example, adverse event reporting to the sponsor, FDA, and the National Institutes of Health (NIH). A covered entity may disclose PHI related to an adverse event to NIH if required to do so by NIH regulations. Even if not required to do so, the researcher may disclose adverse events to NIH as a public health authority.

The Privacy Rule generally entitles individuals to access their health records, receive an accounting of disclosures, and revoke an authorization. Access to research records means that individuals have a right to view and copy their health records maintained by covered entities or a designated record set. For research records, patients have the right to access records that involve treatment (e.g., some clinical trials) or are used to "make decisions about individuals," if they are held by a covered entity. This right can be temporarily restricted during a clinical trial (e.g., if it could un-blind the trial) if the individual agreed to this restriction in the authorization form.

Accounting for Disclosures

When disclosure of PHI is made without an individual's authorization, the covered entity must keep a record that the information left the institution. This requirement includes disclosures for reviews preparatory to research, research using decedents' PHI, research under a waiver of authorization, disclosures to public health authorities or sponsors, and most disclosures mandated by law.

There are three types of accounting for disclosures: general accounting, multiple disclosures to the same person for the same purpose, and research accounting for PHI of 50 or more individuals. General accounting covers the types of items that must be in the disclosure: date, recipient, recipient address if known, and the purpose of the disclosure. If a covered entity makes multiple disclosures to the same person for the same purpose, the covered entity needs to record the date, recipient, recipient address if known, the purpose of the disclosure, frequency, periodicity or number of disclosures, and date of last disclosure. If the covered entity discloses PHI on 50 or more individuals, the covered entity does not need to account individually for them. The covered entity needs to disclose the name of the protocol; description of the protocol or research activity and PHI disclosed; date or period of time during which disclosure occurred or may have occurred, and last date of disclosure; name, address, and phone number of the sponsor and the recipient; and a statement that the PHI may or may not have been disclosed for a particular protocol or research activity. Accounting is not needed for disclosures of PHI in limited data sets with a data use agreement, PHI made with an authorization (or informed consent that meets the transition provisions requirements), PHI to the

individual, disclosures made before April 14, 2003, and disclosures of de-identified health information.

Accounting for disclosures is sometimes necessary for research conducted without authorization. Accounting is needed when discussing PHI with a colleague outside the covered entity, with a waiver of authorization, with decedents' information, preparatory to research, and for public health activities (e.g., adverse event reporting).

On and after the compliance date, individuals will have the right to revoke their authorization. Covered entities may, however, continue to use or disclose PHI that was obtained before a revocation if "necessary to maintain the integrity of the research study." For example, the researcher can continue using PHI to account for a subject's withdrawal from the study.

The covered entity must keep the following types of documentation related to research: authorization form, data use agreement, written revocation, statistical certification of de-identification, waiver of authorization, access to the designated record set, and accounting for disclosures made after the compliance date. The covered entity must keep these documents for six

years from the date of creation or from the date when last in effect, whichever is later.

Institutions must make decisions about how they will handle the Privacy Rule. Researchers should ask questions to prompt this decision-making and clarify how the Privacy Rule will affect them (Table 4).

**TABLE 4
What Researchers Can Do Now
About the Privacy Rule**

1. Ask if you or your institution is subject to the Privacy Rule (a covered entity)
2. Ask who is your institution's privacy official
3. Ask how your institution will train its researchers about the rule
4. Determine if you partner with a researcher or an institution subject to the Privacy Rule
5. List projects that involve the collection, use, or disclosure of PHI
6. Send questions to the Office for Civil Rights (ocprivacy@oc.dhhs.gov)
7. Help NIH help you. What informational materials would be most helpful to you (e.g., Web site, brochures, FAQs)?

NIH Privacy Contacts

Office of Science Policy

Lora Kutkat: 301-594-2464, kutkatl@od.nih.gov

Betsy Dean: 301-594-7743, deanb@od.nih.gov

Dr. Lana Skirboll: 301-496-2122,

skirboll@od.nih.gov

Office of Extramural Research

Dr. Della Hann: 301-402-2725, hannd@od.nih.gov

The full OCR/HIPAA Privacy Regulation Text, October 2002, "Standards for Privacy of Individually Identifiable Health Information, as amended," may be found at <http://www.hhs.gov/ocr/combinedregtext.pdf>