The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: Impacts on Research Involving Protected Health Information

Overview
Effective April 14, 2003, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 CFR 160 and 164) requires covered health care entities1 to obtain written authorization from individuals in order to use or disclose their protected health information for research purposes.

As research involving protected health information qualifies as human subjects research, such research conducted by UNH agents must be reviewed and approved by the UNH Institutional Review Board (IRB) prior to commencing. In addition, UNH researchers who plan to obtain protected health information from covered health care entities should check with those covered health care entities as early as possible to find out any requirements for review by their own IRBs.

In order for researchers to access and use protected health information maintained by covered health care entities, in most situations researchers will have to either obtain written authorization from each subject for use or disclosure of his/her protected health information or approval of a waiver of authorization from the appropriate IRB(s). In other specified research activities involving use or disclosure of protected health information, researchers do not have to obtain written authorization but have to fulfill other requirements. The authorization requirement is in addition to human subject protections regulations2 requiring informed consent to participate in a research study.

This document outlines the responsibilities and requirements of covered health care entities and IRBs when reviewing authorizations, requests for waiver of authorization, and other research activities involving the use or disclosure of protected health information. Researchers may find this information useful when preparing IRB applications and research protocols involving the use of protected health information maintained by covered health care entities.

Definitions
Disclose is defined as “the release, transfer, provision of access to, or divulging in any other manner information outside the entity holding the information” (§164.501).

Health information is defined as “any information, whether oral or recorded in any form or medium, that: (1) 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 (2) 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” (§160.103).

Individually identifiable3 health information is defined as “information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care

---

1 45 CFR § 160.103 defines a covered entity as “(1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.”

2 45 CFR § 46.116

3 The Privacy Rule considers the following as identifiers:
   - Names;
provider, health plan, employer, or health care clearinghouse; and (2) 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 (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual” (§160.103).

_Protected health information_ is defined as “individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) transmitted by electronic media; (ii) Maintained in any medium described in the definition of _electronic media_ at §162.103 of this subchapter; or (iii) transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable information in: (i) Education records covered by the Family Educational Rights and Privacy Act as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer” (§164.501).

_Research_ is defined as “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge” (§164.501).

Use is defined as “with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information” (§164.501).

**Use or Disclosure of Protected Health Information for Research Purposes**

A covered health care entity is permitted to use or disclose protected health information for research purposes with written authorization from individuals, or, in limited circumstances, without written authorization.

**A. Use/Disclosure with Individual Authorization**

The Privacy Rule permits covered health care entities to use or disclose protected health information for research purposes when an individual authorizes the use or disclosure of information about him or herself in writing. Authorizations are required to be study-specific. In order to be valid, an authorization needs to include the following information:

- 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: (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;
- 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; and,
- Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section (§164.514(b)(2)(i)).
- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion [§164.508(c)(1)(i)], e.g., “laboratory results” or “height, weight, and diagnosis” rather than “all health information necessary for study purposes.”

- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure [§164.508(c)(1)(ii)], i.e., the names of the hospital, physician, physical therapist, or health care provider who maintain the desired information.

- The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure [§164.508(c)(1)(iii)], i.e., the name of the researcher and any study personnel who will have access to the information.

- A description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of purpose [§164.508(c)(1)(iv)].

- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository [§164.508(c)(1)(v)].

- Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative’s authority to act for the individual must also be provided [§164.508(c)(1)(vi)].

In addition to the above information, the authorization must contain the following “required” statements:

- Notice of the individual’s right to revoke the authorization in writing and the exceptions to the right to revoke. This can be accomplished either by describing the right to revoke and the exceptions in the authorization or by referring to the covered entity’s Notice of Privacy Practices [§164.508(c)(2)(i)]. (Each covered health care entity has to develop a Notice of Privacy Practices and make it available to individuals.)

A covered entity may continue to use and disclose protected health information that was obtained before an authorization was revoked in order to maintain integrity of the study (American Council on Education [ACE], 2002). A covered entity may not disclose protected health information obtained after the effective date of a revoked authorization. Only information gather by the covered entity before the effective date of a revocation may be disclosed. When an individual revokes his/her authorization, the researcher may continue to use the information previously received as long as it complies with the original authorization (ACE, 2002).

- The covered entity’s inability to make treatment, payment, enrollment, or eligibility for benefits conditional upon signing the authorization. One exception is where research involves treatment. If a participant elects to participate in a study involving research-related treatment and refuses to sign an authorization, the researcher does not have to enroll the individual in the study [§164.508(c)(2)(iii)].

- The potential for information disclosed under the authorization to be re-disclosed by the recipient and not protected by the Privacy Rule. The covered entity is not responsible for what researchers do with the protected health information after receiving it from the covered entity [§164.508(c)(2)(iii)].

In addition to the required elements and statements, the Privacy Rule states that:

- An authorization must be written in plain language
A copy of the signed authorization must be provided to the individual who is permitting the use or disclose of his/her protected health information.

**Authorizations and Informed Consent**

Human subjects protections regulatory requirements for informed consent and Privacy Rule requirements for written authorization are different. Informed consent, as required by the Common Rule\(^4\), is a consent to participate in the research study as a whole whereas the Privacy Rule’s authorization is for the use or disclosure of protected health information for research purposes. IRBs do not have to approve authorization forms per se. However, IRBs review authorization as information provided to subjects in the study and for consistency with the research protocol.

Although there are important differences between the Common Rule’s requirements for informed consent and the Privacy Rule’s requirements for authorization, the elements are compatible. Thus researchers have a couple of options when they are required to obtain authorization from subjects for the use or disclosure of protected health information in a research study:

- **Use separate consent and authorization documents.** (See UNH IRB document, Authorizations for Use or Disclosure of Protected Health Information for Research available at [http://unh.edu.research/files/docs/RIS/hipaa_sample_auth_language.rtf](http://unh.edu.research/files/docs/RIS/hipaa_sample_auth_language.rtf))

- **Use a consent form that includes the required authorization language.** For a consent form to also function as a valid authorization for use or disclosure of protected health information, the information outlined above (Use/Disclosure with Individual Authorization) must be included. (See UNH IRB document, Sample Authorization Language for Consent Forms for Use or Disclosure of Protected Health Information available at [http://unh.edu.research/files/docs/RIS/hipaa_sample_consent_form_auth_language.rtf](http://unh.edu.research/files/docs/RIS/hipaa_sample_consent_form_auth_language.rtf))

**B. Use/Disclosure without Individual Authorization**

There are four situations where a covered health care entity may use or disclose protected health information for research purposes without obtaining written authorizations from individuals:

1. IRB waivers
2. Reviews preparatory to research
3. Research on a decedent’s information
4. Limited data sets

Although all UNH research involving protected health information requires UNH IRB review, only the first situation involves specific action and findings by the IRB. The regulations governing the other situations are enforced by administrative units in the covered health care entity although the UNH IRB also has to approve the research.

1. **Documented Approval of Waiver by IRB**

   A covered health care entity may use or disclose an individual’s protected health information for research purposes without obtaining a written authorization if it obtains documentation that an IRB has waived the written authorization requirement or has approved a modified authorization [§164.512(i)(1)(i)]. This might be used, for example, to conduct records research when researchers are unable to use de-identified information and the research could not practicably be conducted if individuals’ authorization were required.

   If a researcher requests a waiver of written authorization by subjects, the IRB has to make the following findings in order to approve the waiver request.

---

\(^4\) 45 CFR 46
• A determination that the alteration or waiver of authorization, in whole or in part, satisfies the following criteria:

  a. The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:

     (i) An adequate plan to protect the identifiers from improper use and disclosure;

     (ii) An adequate plan to destroy identifiers at the earliest opportunity consistent with conduct of the research unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

     (iii) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research which the use or disclosure of protected health information would be permitted by the Privacy Rule.

  b. The research could not practicably be conducted without the waiver or alteration; and

  c. The research could not practicably be conducted without access to and use of the protected health information [§164.512(i)(2)(ii)].

In addition to the above, documentation of IRB approval of an alteration or waiver of authorization provided to the covered health care entity must include all of the following:

• Identification of the IRB and the date on which the alteration or waiver of authorization was approved [§164.512(i)(2)(i)];

• A brief description of the protected health information for which use or access has been determined to be necessary by the IRB pursuant to paragraph §164.512(i)(2)(ii)(C) [§164.512(i)(2)(iii)].

• A statement that the alteration or waiver of authorization has been reviewed and approved under either expedited review procedures or at a convened meeting of the IRB [§164.512(i)(2)(iv)].

• The signature of the chair or other member, as designated by the Chair, of the IRB [§164.512(i)(2)(v)].

When submitting a research protocol that involves a request for waiver of individual authorization for the use or disclosure of protected health information to the IRB for review, the researcher should make sure that s/he clearly addresses the criteria (a-c) in the first bullet above.

2. Reviews Preparatory to Research
   A covered health care entity may use protected health information or disclose it to a researcher without obtaining written authorization if it obtains representations from the researcher that:

   • The use or disclosure of the protected health information is solely to prepare a research protocol or for similar purposes preparatory to research;

   • The researcher will not remove any protected health information from the covered entity; and
• Protected health information for which access is sought is necessary for the research [§164.512(i)(1)(ii)].

This provision might be used, for example, to design a research study or to assess the feasibility of conducting a study. This exception does not allow for the electronic transfer of protected health information from a covered health care entity to a researcher's office (ACE, 2002).

3. Research on Protected Health Information of Decedents
A covered health care entity may use protected health information or disclose it to a researcher without obtaining a written authorization if it obtains representations from the researcher that:

• The use or disclosure being sought is solely for research on the protected health information of decedents;
• The protected health information being sought is necessary for the research; and,
• At the request of the covered entity, documentation of the death of the individuals about whom information is being sought [§164.512(i)(1)(iii)].

4. Limited Data Sets with a Data Use Agreement
A covered health care entity may use or disclose protected health information without obtaining a written authorization if it enters into a data use agreement with the limited data set recipient. Pursuant to this agreement, the covered health care entity may disclose the limited data set to the researcher for research, public health, or health care operations [§164.514(e)(1)].

In order to qualify as a limited data set, the following direct identifiers of the individual or of relatives, employers, or household members of the individual must be excluded:

• Names;
• Postal address (other than town/city, state and zip code);
• Telephone and fax numbers;
• Email addresses;
• URLs and IP addresses;
• Social security numbers;
• Medical record and health plan beneficiary numbers;
• Account numbers;
• Certificate/license numbers;
• Vehicle identification and serial numbers;
• Device identifiers and serial numbers;
• Biometric identifiers including finger and voice prints; and
• Full face photographic images [§164.514(e)(2)].

The data use agreement that a researcher enters into must:

• Establish the permitted uses and disclosures of the limited data set by the recipient, consistent with the purposes of the research, and which may not include any use or disclosure that would violate the Privacy Rule if done by the covered entity;
• Establish who is permitted to use or receive the limited data set; and
• Require the recipient to agree to the following:
  * Not to use or disclose the information other than as permitted by the data use agreement or as otherwise required by law;
  * Use appropriate safeguards to prevent the use or disclosure of the information other
than as provided for in the data use agreement;

- Report to the covered entity any use or disclosure of the information not provided for by the data use agreement of which the recipient becomes aware;
- Ensure that any agents, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the recipient with respect to the limited data set; and
- Not to identify the information or contact the individual [§164.514(e)(4)].

When submitting a research protocol to the IRB for review that involves a limited data set, the researcher should make sure that s/he includes the data use agreement.

**Transition Provisions**

Under the Privacy Rule, a covered health care entity may use and disclose protected health information created or received for research, either before or after April 14, 2003, if it obtained any one of the following prior to the compliance date:

- An authorization or other express legal permission from an individual to use or disclose protected health information for the research;
- The informed consent of the individual to participate in the research; or
- A waiver of informed consent by an IRB in accordance with the Common Rule or an exception under FDA’s human subject protection regulations.

If a waiver of informed consent was obtained prior to April 14, 2003, but informed consent is subsequently sought after the compliance date, the covered health care entity must obtain the individual’s authorization as required at §164.508.

The Privacy Rule allows covered health care entities to rely on such express legal permission, informed consent, or IRB-approved waiver of informed consent, created or received before April 14, 2003, to use and disclose protected health information for specific research studies, as well as for future unspecified research that may be included in such permission.

Researchers will have to get written authorization from any subjects recruited into a study on or after April 14, 2003 in order for a covered health care entity to disclose protected health information about the individual, unless the researcher obtains an IRB approval of waiver of authorization.

**Source**