

HIPAA PRIVACY REGULATIONS AND MEDICAL RESEARCH: UT GSM IRB GUIDANCE AND PROCEDURES

INTRODUCTION

Recognizing that the rapid evolution of electronic information systems pose dangers to the privacy of personal health information, Congress addressed the issue of establishing national standards for the use and disclosure of individually identifiable health information in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Certain sections of the Act authorized the Secretary of Health and Human Services (HHS) to promulgate standards for the privacy of individually identifiable health information. HHS issued these privacy regulations entitled, “Standards for Privacy of Individually Identifiable Health Information”, 45 CFR Parts 160 and 164. The regulations are commonly referred to as the “Privacy Rule” and are administered by the HHS Office of Civil Rights.

The regulations apply to individually identifiable health information [called “protected health information” (PHI) in the text of the regulation] that is used and disclosed by health care providers and facilities. The regulations impose three basic requirements on health care providers and facilities (called “covered entities” in the text of the regulations) that hold or maintain PHI: (1) covered entities must obtain the agreement of patients to use or disclose their PHI unless specified exceptions are applicable; (2) persons must be notified by covered entities of their rights under the privacy regulations; and (3) use and disclosure of PHI by covered entities must generally be restricted to the minimum necessary to accomplish the intended purpose. Finally, the

regulations implement four basic rights of persons with respect to their PHI: (1) to agree to the use and disclosure of PHI; (2) to inspect and copy their records; (3) to amend their records; and (4) to obtain certain limited audits of the disclosures of their records that have been made by covered entities.

The Privacy Rule also establishes the conditions under which PHI may be used or disclosed in medical research. The following discussion has two objectives. The first is to provide UT GSM investigators, study coordinators and other research personnel with a comprehensive overview of the requirements of the Privacy Rule as they pertain to the conduct of medical research. The second is to provide a synopsis of IRB policies and procedures as revised to implement the requirements of the Privacy Rule in the research context.

RESEARCH USE OF PHI WITH AUTHORIZATION

The Privacy Rule delineates two basic types of written agreements that are utilized to secure the permission of persons for the use and disclosure of PHI. The first type is a general, written **consent** by individuals for the use and disclosure of their PHI for treatment, payment and health care operations in the non-research setting. This written consent provides a one-time, blanket permission for a covered entity to utilize PHI for various purposes related to the provision of clinical care. The second type of written agreement involves **authorization** for the use of PHI for specific purposes other than treatment, payment or health care operations. Specific written authorization is required for the use and disclosure of PHI in research studies. Under the regulations, this authorization may be incorporated into consent forms for clinical research or may be

secured via a separate authorization form. The UT GSM IRB is adopting the option of including the authorization in the consent form for research studies.

The Privacy Rule specifies the basic elements of information that must be provided in writing to prospective subjects in securing authorization for the research use of their PHI. These items of information are covered in the confidentiality section of the [Consent Template](http://gsm.utmck.edu/irb/forms.htm) located at <http://gsm.utmck.edu/irb/forms.htm>. This template, appropriately adapted for individual studies, must be inserted into the confidentiality section of research consent forms. According to the regulations, the following elements must be included in the written authorization and presented in “plain language”:

- (1) A description of the information to be used or disclosed that identifies the information “in a specific and meaningful fashion”;
- (2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
- (3) The name or other specific identification of the person(s), or class of persons, to whom the covered entity is permitted to make the requested use or disclosure;
- (4) A description of each purpose for the requested use or disclosure;
- (5) An expiration date or an expiration event that relates to the purpose of the use or disclosure; the expiration date may be specified as “end of the research study”, or as “none” in the event that the PHI will be used for an indefinite period as part of a research database or repository;

- (6) A description of the individual's right to revoke the authorization in writing, including limitations on this right, and an explanation of how the individual may revoke the authorization. In explaining limitations on the right to revoke the authorization, investigators must indicate that the Privacy Rule permits the continued research use and disclosure of PHI obtained from the subject prior to the time when the authorization is revoked;
- (7) An explanation that the investigator may condition research participation on the provision of the authorization and that subjects who revoke the authorization may be withdrawn from the study;
- (8) The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer protected by the Privacy Rule; and
- (9) When the research includes treatment, a statement that the subject's access to PHI will be temporarily suspended as long as the research is in progress, but will be reinstated upon completion of the research; this ground for the denial of access does not apply to research in which treatment is not provided.

Several other features of authorizations must also be noted. First, the authorization must be signed and dated by the subject or the subject's personal representative. Second, if the signature is secured from the subject's personal representative, then a description of the representative's authority to act on the individual's behalf must also be provided. This latter provision requires that, for studies in which personal representatives may be providing consent or permission for some

subjects, a new line must be inserted in the signature section of the research consent form for describing the relationship of the representative to the subject. Third, a copy of the signed authorization form must be provided to the subject or the subject's personal representative. When the authorization is included in the consent form for the research study, a copy of the consent form must be provided to the subject or the subject's personal representative. Finally, signed authorization forms or consent forms including the authorization must be retained for at least six years.

RESEARCH USE OF PHI WITHOUT AUTHORIZATION

The Privacy Rule permits the use of PHI in medical research without subject authorization under several conditions. These conditions include review of PHI preparatory to research, research involving subjects who are decedents, research involving the use of limited data sets, and research in which a waiver or alteration of authorization is granted by the IRB. Requests to use PHI for research purposes without subject authorization must be submitted to the IRB using Form 8 located at: <http://gsm.utmck.edu/irb/forms.htm> "Request for the Research Use and Disclosure of Protected Health Information (PHI) Without Subject Authorization".

Reviews of PHI Preparatory to Research

Investigators may review PHI without authorization in the preparation of a research study, e.g., to assist in the formulation of a study hypothesis. In order to use PHI under this provision of the regulations, the researcher must provide assurances to the covered entity holding the PHI that:

- (1) The use or disclosure of PHI is sought solely for the purpose of preparing a research protocol or for similar purposes preparatory to research;
- (2) No PHI is to be removed from the covered entity by the researcher in the course of the review; and
- (3) The PHI for which use or access is sought is necessary for research purposes.

HHS has made clear that this exception to the authorization requirement precludes the electronic transfer of PHI from a covered entity to a researcher's office. In addition, reviews preparatory to research must not involve making copies of PHI or making notes that include PHI. However, medical records of interest to investigators in preparing a study may be flagged for future reference.

Research Involving Subjects Who Are Decedents

Investigators may proceed without authorization when using PHI that is derived entirely from decedents. Qualification under this provision of the Privacy Rule requires that the researcher provide to the covered entity:

- (1) Assurance that the use or disclosure is sought solely for research on the PHI of decedents;
- (2) Documentation, at the request of the covered entity, of the death of such individuals; and
- (3) Assurance that use of the PHI is necessary for the research purposes.

Research Involving the Use of Limited Data Sets

[Please note that UHS does not enter into Limited Data Set Use Agreements and predicate all use of patient medical records on IRB review and approval]

The regulations permit covered entities to use or disclose PHI for research purposes without subject authorization if:

- 1) The use or disclosure involves *only* a “limited data set” and
- 2) The covered entity enters into a data use agreement with the investigator.

A “limited data set” is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- (1) Names;
- (2) Postal address information, other than town or city, state and zip code;
- (3) Telephone numbers;
- (4) Fax numbers;
- (5) Electronic mail addresses;
- (6) Social security numbers;
- (7) Medical record numbers;
- (8) Health plan beneficiary numbers;
- (9) Account numbers;
- (10) Certificate/license numbers;
- (11) Vehicle identifiers and serial numbers, including license plate numbers;
- (12) Device identifiers and serial numbers;
- (13) Web universal resource locaters (URLs);
- (14) Internet protocol (IP) address numbers;
- (15) Biometric identifiers, including finger and voice prints; and
- (16) Full face photographic images and any comparable images.

A limited data set may, however, include other indirect identifiers, especially dates of birth, treatment, discharge, or death.

A covered entity may use or disclose a limited data set without subject authorization for research purposes only if it completes a data use agreement with the researcher who is the recipient of the data. This agreement must include several elements. First, it must specify that the investigator may use or disclose the limited data set only for research purposes. Second, the agreement must establish who is permitted to receive and use the limited data set. Third, the agreement must specify that the recipient investigator will: (1) not use or further disclose the information other than as permitted by the data use agreement or by law; (2) use appropriate safeguards to prevent use or disclosure of the information except for the purposes described in the data use agreement; (3) report to the covered entity any use or disclosure of the information not addressed by the data use agreement if the investigator becomes aware of such use or disclosure; (4) ensure that any agents, including a subcontractor, to whom he or she provides the limited data set agrees to the same restrictions and conditions that apply to the recipient investigator with respect to the information; and (5) not attempt to identify or contact the subjects whose PHI is used.

IRB Waiver of Authorization for Research Use of PHI

The Privacy Rule permits investigators to use PHI in research under an alteration or waiver of the authorization requirements when they obtain approval from an IRB or a “privacy board”. Investigators are required to secure the waiver or alteration of authorization from only one IRB or privacy board, even if they will seek PHI from more than one covered entity maintaining such information. In addition, the committee utilized by the investigator is not required to be the IRB or the privacy board of the covered entity that maintains the PHI. However, covered entities providing PHI are permitted to request

that their own IRB or privacy board approve requests for waiver or alteration of authorization prior to allowing use or disclosure of PHI to investigators. Because the UT GSM IRB will be used as the mechanism for reviewing requests from UT investigators for waiver or alteration of authorization, the privacy board mechanism will not be discussed here further.

The criteria for determining whether investigators qualify for a waiver or alteration of authorization are specified in the Privacy Rule. The investigator must provide information about the research study that enables the IRB to determine that three conditions are satisfied:

(1) There must be no more than minimal risk to the privacy of individual subjects based on the presence of the following elements: (a) an adequate plan to protect the identifiers from improper use and disclosure; (b) an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining identifiers or such retention is otherwise required by law; and (c) an adequate written assurance that the PHI will not be reused or disclosed to any other person or entity, except as required by law, or for authorized oversight of the research study, or for other research for which the use or disclosure is permitted without authorization;

(2) It must not be practicable to conduct the research without the waiver or alteration of the authorization requirement; and

(3) It must not be practicable to conduct the research without access to and use of the PHI for which the waiver or alteration of the authorization requirement is sought.

Once the IRB has approved the waiver or alteration of authorization, the investigator must provide the covered entity maintaining the PHI with documentation from the IRB that establishes its approval. This approval letter from the IRB must include the following elements. First, it must identify the IRB and provide the date on which the waiver or alteration of authorization was approved. Second, it must include a statement that the IRB has determined that the waiver or alteration satisfies the criteria described above. Third, the approval letter must provide a brief description of the PHI for which use or access has been determined to be necessary by the IRB. Fourth, the letter must describe whether the request for waiver or alteration of the authorization requirements was reviewed under full board or expedited review procedures. Finally, the approval letter must be signed by the chair of the IRB or his/her designee.

Waiver of authorization may be sought for three specific research uses of PHI:

1. to identify potential research subjects through review of their PHI;
2. to contact potential subjects in order to determine their interest in research participation;
3. to receive or collect PHI during the conduct of research studies.

Identification of Potential Subjects

Although investigators can use PHI in activities that are preparatory to research without authorization and without a waiver (as described above, under “Reviews of PHI Preparatory to Research”), such use must not involve either removing records from facilities or copying PHI from these records. If investigators need to copy or remove information from medical records in order to identify potential subjects, then they must secure a waiver of authorization to examine these medical records if they are not staff

members of the institution or are not direct care providers for the individuals whose records will be reviewed. However, if investigators are staff members of the institution holding the records or are direct care providers for the individuals whose records will be reviewed, then a waiver of authorization is not required.

Recruitment of Potential Subjects

Once potential research subjects have been identified, they must be contacted in accord with the provisions of the regulations. Personnel from the institution holding the records may use PHI to make the initial contact, without prior authorization from potential subjects, to determine their interest in participating in a research study. Similarly, direct care providers may communicate with their current or past patients about research opportunities without prior authorization of these patients. However, an investigator may not use the PHI maintained by another provider or facility in order to make the initial contact with individuals about participation in a research study, unless those individuals have given prior authorization for such a contact or the IRB has provided a waiver of authorization to the investigator.

Use of Protected Health Information in the Conduct of Research Studies

After subjects are identified and recruited, the study itself will involve the disclosure to investigators of PHI maintained by covered entities and/or the creation of PHI pertaining to the performance and results of study procedures. Investigators may obtain a waiver or alteration of prior authorization by subjects if the research use of their PHI meets the conditions described above for approval by the IRB. This option will normally be relevant only to studies in which waiver or alteration of informed consent for research participation is also being sought. The most common use of the waiver option

will relate to retrospective studies of PHI associated with existing medical records and specimens.

USE OF DE-IDENTIFIED DATA IN MEDICAL RESEARCH

Health information that provides no reasonable basis for identifying individuals is not PHI according to the regulatory definition. It may be used in medical research without subject authorization or an IRB waiver. The Privacy Rule refers to such health information as “de-identified data”.

The regulations provide two mechanisms for determining that PHI has been transformed into “de-identified data”. First, health information may be considered to be “de-identified” if a person, who possesses appropriate knowledge and experience in using accepted statistical and scientific principles and methods for rendering information not individually identifiable, determines that the risk is very small that the information could be used by the recipient, alone or in combination with other information, to identify individual subjects. When this mechanism is used for determining that PHI has been de-identified, the individual providing the assessment must document the methods and results of the analysis that justify his/her determination that the health information is properly de-identified. Second, health information can be considered de-identified provided that the following identifiers of the individual or of relatives, employers or household members of the individual are removed:

- (1) Names;
- (2) All geographic subdivisions smaller than a state, including street address, city, county, precinct, and their equivalent geocodes, except for the initial

three digits of a zip code if the geographic unit represented by these three initial digits contains more than 20,000 people;

- (3) 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 indicative of age over 89, except that such ages and elements may be aggregated into a single category of age 90 or older;
- (4) Telephone numbers;
- (5) Fax numbers;
- (6) Electronic mail addresses;
- (7) Social security numbers;
- (8) Medical record numbers;
- (9) Health plan beneficiary numbers;
- (10) Account numbers;
- (11) Certificate/license numbers;
- (12) Vehicle identifiers and serial numbers, including license plate numbers;
- (13) Device identifiers and serial numbers;
- (14) Web universal resource locators (URLs);
- (15) Internet protocol (IP) address numbers;
- (16) Biometric identifiers, including finger and voice prints;
- (17) Full face photographic images and any comparable images; and
- (18) Any other unique identifying number, characteristic, or code.

Covered entities may assign code numbers to individual records to allow de-identified information to be re-identified, provided that the code is not derived from information about the individuals and the covered entity does not disclose the mechanism for re-identification.

PROCEDURES FOR COMPLIANCE

For all studies the application must specify in the section on confidentiality either that the research use and disclosure of PHI will be undertaken with authorization, or that the research use or disclosure satisfies one of the conditions under which subject authorization is not required under the privacy regulations.

For studies in which subject authorization for the use and disclosure of PHI is required, the confidentiality section of the subject consent form must include the required authorization disclosure. The required disclosure is provided in the consent form template. **The authorization language in the consent form must conform precisely to the template provided in the consent form template.**

For studies in which the use or disclosure of PHI may satisfy one of the conditions under which subject authorization is not required under the privacy regulations, the investigator must submit UT GSM IRB Form 8, “Application for Waiver of HIPAA Authorization”. The investigator will receive a separate approval letter for the use and disclosure of PHI without subject authorization. This approval letter can be presented to the entity maintaining the PHI, if separate from the investigator, to establish that the IRB has reviewed the proposed use and disclosure of PHI without subject authorization and has determined that it satisfies the regulatory requirements. If the PHI

is maintained by the investigator, the letter should simply be retained as confirmation that the regulatory requirements have been satisfied for using or disclosing PHI in research without subject authorization.

Acknowledgement:

This document was adapted from ‘HIPAA Privacy Regulations and Medical Research: UT GSM IRB Guidance and Procedures’ prepared by: Terrence F. Ackerman, Ph.D., Chairman Institutional Review Board UT Health Science Center, Memphis, Professor and Chairman Department of Human Values and Ethics

The original may be seen in it’s entirety at:

http://www.utmem.edu/research/IRB/docs/GUIDANCE_PROCEDURES_MAIN_INFO.doc