Health Services Research and the HIPAA Privacy Rule

Overview

Health services researchers conduct studies designed to improve the quality of health care, reduce its cost, improve patient safety, decrease medical errors, and broaden access to essential services. The evidence-based information produced by these researchers helps health care decision-makers make more informed decisions and improve the quality of health care services. Studies in health services research are often accomplished by analyzing large databases of health care information collected or maintained by health care providers, institutions, payers, and government agencies. With the implementation of the Federal Privacy Rule, health services researchers and database custodians have sought information about the Rule and how it may affect the use and disclosure of data for health services research.

As of April 14, 2003, the Privacy Rule requires many health care providers and health insurers to obtain additional documentation from researchers before disclosing personal health information for research and to scrutinize researchers' requests for access to health information more closely. Although the Privacy Rule introduces new rules for the use and disclosure of health information by covered entities, researchers can help to enable their continued access to health data by understanding the Privacy Rule and assisting health care entities covered by the Privacy Rule in meeting its requirements.

This factsheet discusses the Privacy Rule and how it permits certain health care providers, health plans, and other entities covered by the Privacy Rule to use and disclose personal health information for health services research. Additional information about the Privacy Rule can be found in related publications, including:

- *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*
- *Clinical Research and the HIPAA Privacy Rule*
- *Research Repositories, Databases, and the HIPAA Privacy Rule*
- *Institutional Review Boards and the HIPAA Privacy Rule*
- *Privacy Boards and the HIPAA Privacy Rule*

Introduction to the Privacy Rule

In response to a congressional mandate in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the U.S. Department of Health and Human Services (HHS) issued the regulations *Standards for Privacy of Individually Identifiable Health Information*. For most covered entities, compliance with these regulations, known as the Privacy Rule, was required as of April 14, 2003.

The Privacy Rule is a response to public concern over potential abuses of the privacy of health information. The Privacy Rule establishes a category of health information, referred to as "protected health information" (PHI), which may be used or disclosed to others only in certain circumstances or under certain conditions. PHI is a subset of what is termed "individually identifiable health information." With certain exceptions, the Privacy Rule applies to individually identifiable health information created or maintained by a covered entity. Covered entities include health plans, health care clearinghouses, and health care providers that transmit health information electronically in connection with certain defined HIPAA transactions, such as claims or eligibility inquiries.

Researchers are not themselves covered entities, unless they are also health care providers and engage in any of the covered electronic transactions. If, however, researchers are employees or other workforce members of a covered entity (e.g., a covered hospital or health plan), they may have to comply with that entity's Privacy Rule policies and procedures. Researchers who are not themselves covered entities, or who are not workforce members of covered entities, may be indirectly affected by the Privacy Rule if covered entities supply their data.

In addition to the Privacy Rule, other regulations may apply as well. For instance, individual records held by covered entities that are also alcohol and substance abuse treatment providers are protected by the Federal Confidentiality of Alcohol and Substance Abuse Patient Records Regulation (see 42 CFR part 2). Also, the HHS and the U.S. Food and Drug Administration (FDA) Protection of Human Subjects Regulations (45 CFR part 46 and 21 CFR

parts 50 and 56, respectively) may apply to health services research. In addition, if health-related research involves electronic PHI, covered entities must also consider the requirements of the HIPAA Security Rule (45 CFR part 160 and Part 164, subparts A and C). Compliance with the Security Rule is required no later than April 20, 2005, for all HIPAA-covered entities, except for small health plans, which have an extra year to comply.

Use and Disclosure of PHI for Research

The Privacy Rule permits covered entities to use or disclose PHI for research purposes either with an individual's specific written permission, termed an "Authorization," or without it, if certain conditions are met. A covered entity is permitted to use or disclose PHI for research purposes if it:

- Obtains the individual's Authorization for the research use or disclosure of PHI as specified under section 164.508 of the Privacy Rule,
- Obtains satisfactory documentation of an Institutional Review Board (IRB) or Privacy Board's waiver of the Authorization requirement that satisfies section 164.512(i) of the Privacy Rule,
- Obtains satisfactory documentation of an IRB or Privacy Board's alteration of the Authorization requirement as well as the altered Authorization from the individual,
- Uses or discloses PHI for reviews preparatory to research with representations from the researcher that satisfy section 164.512(i)(1)(ii) of the Privacy Rule,
- Uses or discloses PHI for research solely on decedents' PHI with representations from the researcher that satisfy section 164.512(i)(1)(iii) of the Privacy Rule,
- Provides a limited data set and enters into a data use agreement with the recipient as specified under section 164.514(e) of the Privacy Rule,
- Uses or discloses information that is de-identified in accordance with the standards set by the Privacy Rule at section 164.514(a)-(c) (in which case, the health information is no longer PHI), or
- Uses or discloses PHI based on a permission that predates the applicable compliance date of the Privacy Rule (generally, April 14, 2003), i.e., an express legal permission to use or disclose the information for the research, an informed consent of the individual to participate in the research, or a waiver by an IRB of informed consent to participate in the research. See the Privacy Rule at section 164.532(c).

Overview of the Impact of the Privacy Rule on Health Services Research

Health services research differs from other types of research in several ways. For example, in contrast to a clinical trial where the researcher may have the opportunity to ask each subject for his or her Authorization to use or disclose his or her PHI, health services researchers often work with large, population-level databases containing thousands or even millions of records. As a result, health services researchers frequently do not interact with the individual subjects of their research. In such circumstances, contacting data subjects to ask for their Authorization prior to a health services research study may not be practicable or even possible.

Another difference is that databases used in health services research may be compiled by entities such as hospitals, insurers, private organizations, and government agencies. Such database custodians have likely adopted their own policies to protect personal privacy while permitting the use of data for legitimate research. The Privacy Rule imposes national requirements that covered entities must meet before granting researchers access to the PHI in their databases.

Health services researchers should understand that the Privacy Rule *distinguishes between a research study and a study that a covered entity may undertake as part of its health care operations to understand and improve its own service (i.e., a quality improvement study or assessment related to covered functions).* The Privacy Rule defines research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." This definition is adapted from the definition of "research" found in the HHS Protection of Human Subjects Regulations at 45 CFR part 46. The Privacy Rule distinguishes between research and studies for quality assessment and improvement purposes based on whether the *primary* purpose of

the study in question is to obtain generalizable knowledge. If the primary purpose of such a study is to obtain generalizable knowledge, then the activity cannot be considered to be a health care operations activity. Rather, it meets the definition of "research," and any use or disclosure of PHI for such study must be made in accordance with the Privacy Rule's provisions on the use and disclosure of PHI for research. If, however, a covered entity is conducting a quality improvement or assessment study—-the primary purpose of which is not to develop or contribute to generalizable knowledge—then the study is considered to be a health care operation, and the covered entity may use or disclose PHI for the study as part of its health care operations under the Privacy Rule.

Unlike the Privacy Rule, a quality improvement or assessment study involving human subjects may be considered research under the HHS Protection of Human Subjects Regulations if the study was designed to contribute to generalizable knowledge regardless of whether that is its primary purpose. Thus, a covered entity conducting a health care operations study under the Privacy Rule (i.e., where creating generalizable knowledge is not the primary purpose of the study) still may be conducting "research" under the HHS Protection of Human Subjects Regulations. Thus, the covered entity may have to comply with the HHS Protection of Human Subjects Regulations, even though any uses or disclosures in question could be made without complying with the Privacy Rule's requirements that apply to uses and disclosures for research. The HHS Protection of Human Subjects Regulations apply to all research involving human subjects that is conducted or supported by any component of HHS, or under an applicable assurance, unless the research involves one or more of the categories of exempt research described under the HHS regulations at 45 CFR 46.101(b). The HHS Protection of Human Subjects Regulations require, among other things, an IRB to review research involving human subjects. The HHS Protection of Human Subjects Regulations at 45 CFR 46.102(f) define a "human subject," in part, as a living individual about whom an investigator conducting research obtains "identifiable private information...*Private information* must be individually identifiable (i.e., the identity of the subject is or may be *readily ascertained* [emphasis added] by the investigator or associated with the information)."

Health services researchers may have had less contact with the process of IRB review than biomedical researchers. Because of the type of data used, health services research often is not considered research involving human subjects and may be exempt from the HHS Protection of Human Subjects Regulations. For example, the HHS Protection of Human Subjects Regulations would not apply if the research involved the collection or study of only existing records, and the research information was recorded by the investigator(s) in such a manner that (an) individual subject(s) could not be identified either directly or through identifiers linked to the subject(s). However, such data may be PHI under the Privacy Rule. Under the Privacy Rule, health information is individually identifiable if it identifies the individual or if there is a reasonable basis to believe the information could be used to identify the individual. Such information may include certain data elements, such as dates of service and ZIP Codes, that may not be considered to be identifiable private information under the HHS Protection of Human Subjects Regulations.

It is important to recognize that the Privacy Rule permits covered entities, such as certain hospitals, clinics, and other health care providers, to continue gathering information on their patients for treatment, payment, and health care operations purposes and to put this information into their own databases for these purposes without Authorization. Covered entities also are permitted to disclose PHI without Authorization to government-authorized public health authorities for disease surveillance, disease prevention, and other public health purposes, such as reporting disease and injury, in accordance with the Privacy Rule. In addition, the Privacy Rule permits other disclosures when required by law, for example, for State-mandated reporting to cancer registries. Thus, many databases that are now used for health services research will continue to be maintained and updated and will remain available to researchers, although, in some cases, under new terms.

How Covered Entities May Use and Disclose Data for Health Services Research Without Authorization From Data Subjects

Although covered entities may use or disclose PHI for research purposes on obtaining the Authorization of each data subject as indicated above, obtaining Authorization may not be practicable in certain health services research situations. This section explains in greater detail the conditions under which a covered entity may use or disclose PHI for research under the Privacy Rule without obtaining an Authorization from each data subject.

De-Identified Data Sets

The Privacy Rule permits covered entities to use and disclose data that have been de-identified without obtaining an Authorization and without further restrictions on use or disclosure because de-identified data are not PHI and, therefore, are not subject to the Privacy Rule. A covered entity may de-identify PHI in one of two ways. The first way, the "safe-harbor" method, requires the removal of every one of 18 identifiers enumerated at section 164.514(b)(2) of the Privacy Rule.[1] Data that are stripped of these 18 identifiers are regarded as de-identified, unless the covered entity has actual knowledge that it would be possible to use the remaining information alone or in combination with other information to identify the subject.

The second way to de-identify PHI is to have a qualified statistician[2] determine, using generally accepted statistical and scientific principles and methods, that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by the anticipated recipient to identify the subject of the information. The qualified statistician must document the methods and results of the analysis that justify such a determination.

It is important to note that the Privacy Rule permits a covered entity to assign to, and retain with, the de-identified health information a code or other means of record re-identification, if the following conditions are met. First, the re-identification code may not be derived from or related to information about the individual or otherwise be capable of being translated to identify the individual. For example, an encrypted individual identifier (e.g., an encrypted Social Security number) would make otherwise de-identified health information identifiable. An encrypted individual identifier does not meet the conditions for use as a re-identification code for de-identified health information because it is derived from individually identifiable information. Second, the covered entity may not use or disclose the code for any other purpose or disclose the mechanism for re-identification.

Limited Data Sets

In some cases, de-identified data may lack critical information needed for health services research (e.g., nine-digit ZIP Codes or dates of treatment). When such indirect identifiers are needed for the research, a covered entity may provide the data to a researcher as a limited data set. No Authorization or waiver or alteration of Authorization by an IRB or Privacy Board is required for a covered entity to use or disclose a limited data set.

Limited data sets are data sets stripped of certain direct identifiers that are specified in the Privacy Rule. Limited data sets may be used or disclosed only for public health, research, or health care operations purposes. Because limited data sets contain certain identifiers, they are *not* de-identified information under the Privacy Rule. Importantly, unlike de-identified data, PHI in limited data sets may include the following: Addresses other than street name or street address or post office boxes, all elements of dates (such as admission and discharge dates), and unique codes or identifiers not listed as direct identifiers at section 164.514(e).[3]

Before disclosing a limited data set to a researcher, a covered entity must enter into a data use agreement with the researcher. Among other requirements set forth in section 164.514(e)(4) of the Privacy Rule, the data use agreement must identify who will receive the limited data set, establish how the data may be used and disclosed by the recipient, and provide assurances that the data will be protected. If the covered entity learns that the researcher has violated this agreement, the entity must take reasonable steps to end or repair the violation and, if such steps are unsuccessful, stop disclosing PHI to the researcher and report the problem to the HHS Office for Civil Rights. Additional information on limited data sets and data use agreements can be found in the booklet *Protecting Personal Health Information in Research:Understanding the HIPAA Privacy Rule.*

Waiver or Alteration of the Authorization Requirement by an IRB or Privacy Board

For some types of research, de-identified information or a limited data set may not be sufficient for the research purposes. It also may be impracticable for researchers to obtain written Authorization from research participants, for example, for some research conducted on existing databases or repositories where no contact information is available. To address these situations, the Privacy Rule contains criteria for waiving or altering the Authorization requirement by an IRB or another review body, called a Privacy Board. The Privacy Rule permits a covered entity to use or disclose PHI for research purposes without Authorization (or with an altered Authorization) if the covered entity receives proper documentation that an IRB or Privacy Board has granted a waiver (or an alteration) of the Authorization requirement for the research use or disclosure of PHI.

The Privacy Rule establishes criteria to be used by an IRB or Privacy Board in approving a waiver or alteration of the Authorization requirement. For a covered entity to use or disclose PHI under a waiver or alteration of the Authorization requirement, it must obtain documentation of, among other things, the IRB's or Privacy Board's determination that the following criteria have been met:

- The use or disclosure involves no more than a minimal risk to the privacy of individuals based on at least the presence of (1) an adequate plan presented to the IRB or Privacy Board to protect PHI identifiers from improper use and disclosure; (2) an adequate plan to destroy those identifiers at the earliest opportunity, consistent with the research, absent a health or research justification for retaining the identifiers or if retention is otherwise required by law; and (3) adequate written assurances that the PHI will not be reused or disclosed to any other person or entity except (a) as required by law, (b) for authorized oversight of the research study, or (c) for other research for which the use or disclosure of the PHI is permitted by the Privacy Rule;
- The research could not practicably be conducted without the requested waiver or alteration; *and*,
- The research could not practicably be conducted without access to and use of the PHI.

Additional information about the waivers and alterations of Authorization can be found in the publications *Institutional Review Boards and the HIPAA Privacy Rule* and *Privacy Boards and the HIPAA Privacy Rule.*

Research Involving Decedents' PHI

A covered entity may provide access to decedents' records for research purposes if the covered entity receives from the researcher (1) representations that the decedents' PHI is necessary for the research and is being sought solely for research on decedents (not, e.g., for research on living relatives of decedents) and (2) on request of the covered entity, documentation of the deaths of the study subjects.

No Authorization or waiver or alteration of Authorization by an IRB or Privacy Board is needed for use or disclosure of decedents' PHI for research, if these conditions are met.

Reviews Preparatory to Research

Covered entities may permit researchers to review PHI in medical records or elsewhere to prepare a research protocol or for similar preparatory to research purposes. This review allows the researcher to determine, for example, whether a sufficient number or type of records exist to conduct the research. Importantly, the covered entity may not permit the researcher to remove any PHI from the covered entity.

To permit the researcher to conduct a review preparatory to research, the covered entity must receive from the researcher representations that:

- The use or disclosure is sought solely to review PHI as necessary to prepare the research protocol or other similar preparatory purposes,
- No PHI will be removed from the covered entity during the review, and
- The PHI that the researcher seeks to use or access is necessary for the research purposes.

Additional information on activities preparatory to research can be found in the publications *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule, Institutional Review Boards and the HIPAA Privacy Rule,* and *Clinical Research and the HIPAA Privacy Rule.*

Research Permissions "Grandfathered" by the Transition Provisions of the Privacy Rule

The Privacy Rule contains a transition provision that, under certain conditions, allows covered entities to continue to use or disclose PHI for research without an Authorization or waiver or alteration of the Authorization requirement. For many such uses and disclosures of PHI in connection with research, a covered entity may rely on any one of the following that was obtained prior to the applicable compliance date (usually, April 14, 2003):

- An Authorization or other express legal permission from an individual to use or disclose PHI for the research,
- The informed consent of the individual to participate in the research, or
- A waiver by an IRB of informed consent in accordance with applicable laws and regulations governing informed consent, unless informed consent is sought after the compliance date.

Other Privacy Rule Requirements When PHI Is Used or Disclosed for Research

Minimum Necessary Standard

When using or disclosing PHI for research without an Authorization, a covered entity must make reasonable efforts to limit the PHI used or disclosed to the minimum necessary amount to accomplish the research purpose. However, when disclosing PHI to a researcher who has provided proper documentation or representations as required under Section 164.512(i) of the Privacy Rule (i.e., documentation of an IRB or Privacy Board waiver or alteration of Authorization or representations and documentation as required for reviews preparatory to research or for research on decedents' PHI) a covered entity may reasonably rely on the researcher's request consistent with such documentation and representations as the minimum necessary amount of PHI for the research. See section 164.514(d)(3)(iii)(D) of the Privacy Rule.

Right to an Accounting of Disclosures

The Privacy Rule grants individuals new rights, including the right to receive an accounting of research disclosures made by a covered entity without the individual's Authorization (e.g., under a waiver of Authorization), except for disclosures of a limited data set. The individual has a right to such an accounting of disclosures made by a covered entity in the 6 years prior to the date on which the accounting is requested, not including the period prior to the compliance date of the Privacy Rule. For such disclosures, in general, individuals who request an accounting must be told which PHI was disclosed, to whom it was disclosed, and the date and purpose of the disclosure. Covered entities must provide the address of the recipient, if known.

For certain research disclosures made by a covered entity, two other options exist to facilitate providing an accounting. When multiple disclosures of PHI are made to the same person or entity for a single purpose, the accounting for such disclosures may consist of the information described above for the first disclosure, plus the number or frequency of disclosures, and the date of the last disclosure during the time period covered by the request.

In addition, if during the period covered by the accounting the covered entity has disclosed the records of 50 or more individuals for a particular research purpose, the covered entity may provide to the requester a more general accounting, with the following information:

- The name and description of the protocols for which their PHI may have been disclosed,
- A brief description of the type of PHI disclosed,
- The date or period of time of the disclosures, including the date of the last such disclosure during the accounting period,
- The contact information of the researcher and the research sponsor, and
- A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or research activity.

Section 164.528(b)(4)(ii) of the Privacy Rule requires that, on request, the covered entity must help the individual contact the sponsor and researcher when it is reasonably likely that the individual's PHI was disclosed for a particular protocol. Additional information on accounting for disclosures can be found in the booklet *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*.

Commonly Asked Questions and Answers About the Privacy Rule and Health Services Research

Q: I am a health services researcher employed by a university that has designated itself as a "hybrid entity" for purposes of the Privacy Rule. The university's hospital and medical school are within the "health care component" of the hybrid entity, but my epidemiology department is not. Am I subject to the Privacy Rule requirements that apply to the health care component of the university?

A: No. The Privacy Rule permits a covered entity that performs both covered and noncovered functions as part of its business operations to elect to be a hybrid entity. A covered function is any function, the performance of which makes the entity a health plan, health care provider, or health care clearinghouse. To become a hybrid entity, the covered entity must designate and include in its health care component(s) all components that would meet the definition of a covered entity if that component were a separate legal entity. In addition, a covered entity may include in its health care component any component that functions as a noncovered health care provider or that performs activities that would make the component a business associate of the entity if it were legally separate. However, the hybrid entity is not permitted to include in its health care component other types of components that do not perform the covered functions of the covered entity. For example, a university that has designated its hospital and medical school as the health care component may not also include a component that performs records research that is not used to support the covered functions of the health care component. Within the hybrid entity, most of the Privacy Rule requirements apply only to the health care component(s), although the hybrid entity retains certain oversight, compliance, and enforcement obligations. See section 164.105 of the Privacy Rule for more information.

Remember, however, that a health care component must comply with the Privacy Rule when using or disclosing PHI, including when sharing PHI with a non-health care component of a hybrid entity. Thus, for a health care component of a covered entity to disclose PHI to a researcher in a non-health care component of the entity, the disclosure of PHI must be permitted either by the individual's Authorization or by one of the Privacy Rule's exceptions to the Authorization requirement, such as a waiver of Authorization granted by an IRB or Privacy Board. In addition, since the Privacy Rule treats the sharing of PHI from the health care component to any non-health care component as a disclosure, a health care component's sharing of PHI with another component of the hybrid entity for research purposes may, in certain cases, be subject to the Privacy Rule's accounting requirements. See section 164.528 of the Privacy Rule.

Q: I am conducting a large research study in which I will obtain data from multiple covered entities. Must each covered entity disclosing data to me for my research receive documentation that its own IRB or Privacy Board has granted my project a waiver of Authorization?

A: No. The Privacy Rule permits covered entities reasonably to rely upon a researcher's documentation that a waiver was properly granted by a single IRB or Privacy Board, even if the IRB or Privacy Board is not affiliated with the covered entity. Under the Privacy Rule, one IRB or Privacy Board's documentation of waiver of Authorization suffices.

Q: I work for a covered entity and conduct observational studies on patients' reactions to various emergency room triaging. The nature of the study requires that individuals not know they are being observed. Under the HHS Protection of Human Subjects Regulations, the IRB is allowed to waive the informed consent requirement when certain criteria are met. Must I also receive documentation of an IRB waiver of the Authorization requirement under the Privacy Rule for observational studies?

A: It depends on whether the study is research, as defined by the Privacy Rule. The Privacy Rule distinguishes between research and studies for quality assessment and improvement purposes based on whether the *primary* purpose of the

study in question is to obtain generalizable knowledge. The Privacy Rule defines research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." If the primary purpose of such a study is to obtain generalizable knowledge, then the activity does not meet the definition of a "health care operation" and, instead, meets the definition of "research," and any use or disclosure of PHI for such study must be made in accordance with the Privacy Rule's provisions for the use and disclosure of PHI for research. For example, an IRB or a Privacy Board may waive or alter the Authorization requirement, as long as certain criteria at section 164.512(i)(2)(ii) are met (i.e., the use or disclosure of PHI involves no more than minimal risk to the privacy of individuals and the research could not practicably be conducted without the requested waiver or alteration or without access to and use of the PHI).

If, however, a covered entity is conducting a quality improvement or assessment study, the primary purpose of which is not to develop or contribute to generalizable knowledge, then the study is considered to be a health care operation, and the covered entity may use or disclose PHI for the study as part of its health care operations under the Privacy Rule. The Privacy Rule does not require documentation of an IRB or Privacy Board waiver or alteration of Authorization for uses and disclosures of PHI for health care operations activities. Nor does the Privacy Rule require the individual's Authorization for uses and disclosures of PHI for health care operations activities.

Q: Under what circumstances may a Privacy Board or an IRB use an expedited review procedure to review requests for a waiver or alteration of the Authorization requirement?

A: A Privacy Board is permitted to use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the PHI for which use or disclosure is sought. Thus, a Privacy Board may use an expedited review procedure for any request that meets the waiver criterion at section 164.512(i)(2)(ii)(A) of the Privacy Rule, which requires that the use or disclosure of PHI involves no more than minimal risk to the privacy of individuals, based on, at least, the presence of (1) an adequate plan presented to the Privacy Board to protect PHI identifiers from improper use and disclosure; (2) an adequate plan to destroy those identifiers at the earliest opportunity, consistent with the research, absent a health or research justification for retaining the identifiers or if retention is otherwise required by law; and (3) adequate written assurances that the PHI will not be reused or disclosed to any other person or entity except (a) as required by law, (b) for authorized oversight of the research study, or (c) for other research for which the use or disclosure of PHI is permitted by the Privacy Rule. For example, a Privacy Board may use an expedited review procedure to approve a request that meets all required criteria at section 164.512(i)(2)(ii), as well as disapprove a request that may meet the minimal risk criterion but not one or both of the other required criteria. If, however, a Privacy Board using an expedited review procedure determines that a request involves more than minimal risk to the privacy of individuals, the request must then be reviewed by the Privacy Board's normal review procedures. Where the Privacy Board is permitted, and elects, to use an expedited review procedure, the review and approval of the alteration or waiver of Authorization may be carried out by one or more members of the Privacy Board, as designated by the Privacy Board chair.

Under the Privacy Rule, an IRB that reviews research using the HHS or FDA Protection of Human Subjects Regulations must follow the procedures for normal and expedited IRB review set forth in these regulations when it reviews a request to waive or alter the Privacy Rule Authorization requirement. See 164.512(i)(2)(iv)(A). For IRBs, HHS and FDA have established categories of research that may be reviewed by an IRB through an expedited review procedure for compliance with their respective Protection of Human Subjects Regulations (see 63 *Federal Register* 60364, November 9, 1998, and 63 *Federal Register* 60353, November 9, 1998). Thus, expedited review of a request for a waiver or an alteration of the Authorization requirement is permitted under the Privacy Rule where the research activity is on the HHS or FDA list of approved categories and involves no more than minimal

risk to the research subjects. In addition, 45 CFR 46.110 and 21 CFR 56.110 permit an IRB to use an expedited review procedure to review minor changes in previously approved research. Under the HHS and FDA regulations, a modification to a previously approved research protocol, which only involves the addition of an Authorization for the use or disclosure of PHI to the IRB-approved informed consent, may be reviewed by the IRB through an expedited review procedure, since this type of modification may be considered to be no more than a minor change to research. If expedited review procedures using the HHS or FDA Protection of Human Subjects Regulations are appropriate for acting on the request to waive or alter the Authorization under the Privacy Rule, the review may be carried out by the IRB chair or by one or more experienced reviewers designated by the chair from among the IRB members.

A member with a conflicting interest may not participate in an expedited review. If, under the HHS or FDA regulations, the head of the Federal department or agency (or his or her designee) regulating the research has restricted, suspended, terminated, or chosen not to authorize an institution or IRB to use expedited review procedures, under the Privacy Rule, any waiver or alteration granted on an expedited basis would not be valid.

Q: My employer, a covered entity, began collecting and analyzing PHI for a quality improvement study as part of its health care operations, but the study evolved into a research project. What do we need to do to be in compliance with the Privacy Rule?

A: If a covered entity determines that a quality study has become a research activity (i.e., the primary purpose of the study is now to develop or contribute to generalizable knowledge), the covered entity must be able to establish that, at the time the study was initiated, the covered entity was not required to comply with the Privacy Rule's conditions for uses and disclosures for research. If the covered entity needs to use or disclose PHI for research (e.g., to collect further data in order to conduct the research), the covered entity must then comply with the Privacy Rule's research requirements by obtaining, for example, the individual's Authorization or an IRB or Privacy Board waiver of Authorization, before doing so.

Q: A covered hospital hired a researcher as a business associate to conduct a quality assessment study using PHI, and the researcher has made some findings that he or she would like to publish for his or her own purposes in a scientific or professional journal. Is this permissible under the Privacy Rule?

A: Generally not. The business associate agreement between the covered entity and the researcher generally may not authorize the researcher to use or disclose PHI created or received in the researcher's capacity as a business associate for the researcher's own purposes. The business associate agreement also must require that the PHI be returned to the covered entity or destroyed at termination of the contract, if feasible. However, a covered entity may provide the researcher with de-identified information that he or she may use for the purposes of preparing the publication or with PHI with individuals' Authorizations for such purpose. In addition, the business associate agreement between the covered entity and the researcher may authorize the researcher to de-identify PHI or to obtain Authorizations from individuals on behalf of the covered entity for publication, even if the researcher is ultimately the intended recipient of the information.

Q: Is a covered entity that conducts a quality study as part of its health care operations permitted by the Privacy Rule to publish the results?

A: A covered entity may publish the results of a health care operation's quality study if the health information is de-identified, prior to publication, in accordance with the Privacy Rule's de-identification standard. Alternatively, if the health information remains individually identifiable, the covered entity may obtain the individual's Authorization to publish the PHI. See sections 164.508 and 164.514 of the Privacy Rule for the requirements related to Authorizations and de-identification.

Q: Is a limited data set that has been de-identified according to the Privacy Rule still PHI or covered by the Privacy Rule?

A: No. Although information in a limited data set is PHI, if it is subsequently de-identified according to the Privacy Rule at section 164.514(a)-(c), it is not PHI, and therefore, its use and disclosure are not regulated by the Privacy Rule.

Q: Does the Privacy Rule require that the covered entity and the intended recipient of a limited data set sign the data use agreement?

A: Yes, unless a legally binding document can be created absent a signature under applicable State law.

Q: May a data use agreement identify specific entities, rather than persons, that are permitted to use or receive the limited data set?

A: Yes. A data use agreement between a covered entity and the intended recipient of a limited data set need not identify specific person(s) as the recipient(s). Rather, a data use agreement may identify a specific entity as the intended recipient, such as a particular laboratory, hospital department, or business, as long as the data use agreement is legally binding on both parties.

Q: Does the Privacy Rule require data use agreements to have an expiration date?

A: No. Data use agreements need not specify an expiration date.

Q: May a limited data set include a unique code or identifier not listed at section 164.514(e)(2) of the Privacy Rule?

A: A limited data set may include unique codes or identifiers not listed as direct identifiers at section 164.514(e)(2) of the Privacy Rule, provided the code or identifier does not replicate part of a listed direct identifier. For example, a limited data set may not include the last four digits of a Social Security number or an individual's initials since these identifiers are elements of, or replicate part of, a direct identifier. However, the limited data set may include a code that is derived from the individual's direct identifier as long as it does not replicate any part of the direct identifier. In any event, before a covered entity may use or disclose a limited data set, the recipient of the information must be restricted by a data use agreement from re-identifying the information or contacting the subjects of the information. See section 164.514(e)(4)(ii) for additional content requirements of the data use agreement.

Q: Does the Privacy Rule permit a covered entity to de-identify health information or create a limited data set without Authorization, waiver of the Authorization requirement from an IRB or Privacy Board, or representations for reviews preparatory to research?

A: Yes. In the Privacy Rule, such use is permissible because creating de-identified health information or a limited data set is a health care operation of the covered entity and, thus, does not require an individual's Authorization, a waiver of the Authorization requirement, or the representations associated with reviews preparatory to research. The Privacy Rule also does not require an IRB or Privacy Board to review or approve a data use agreement established for the use or disclosure of a limited data set.

If a business associate is hired by a covered entity to de-identify health information or to create a limited data set, such activity must be conducted in accordance with the business associate requirements at sections 164.502(e) and 164.504(e) of the Privacy Rule. These provisions require that the covered entity and the business associate enter into an agreement that, among other things, limits the business associate's use and disclosure of the PHI to the purposes specified in the agreement and requires the business associate to safeguard the information.

Q: May a covered entity that performs research create de-identified health information to be used to prepare a grant application for research as part of its health care operations, or is this activity a review preparatory to research?

A: Creating de-identified health information from PHI is a health care operation. Thus, to de-identify PHI, a covered entity that performs

research need not have representations as required for a review preparatory to research, and the covered entity's subsequent use or disclosure of the de-identified information is not subject to the Privacy Rule. A covered entity is also permitted to hire a business associate to de-identify PHI.

Q: May a covered entity hire a researcher as a business associate to de-identify health information when the researcher is the intended recipient of the de-identified data?

A: Yes. A covered entity may hire the intended recipient of the de-identified data as a business associate for purposes of creating the de-identified data. That is, a covered entity may provide a business associate that is also the de-identified data recipient with PHI, including identifiers, so that the business associate can de-identify the data for the covered entity. However, the data recipient, as a business associate, must agree in its business associate agreement to return or destroy the identifiers once the de-identified data set has been created.

Q: May a covered entity that has hired a researcher as its business associate for the purposes of de-identifying data permit the researcher to assign to the de-identified data a re-identification code, if the researcher is also the intended recipient of the de-identified data?

A: Yes, provided the researcher is able to return or destroy all identifiers once the de-identified data set has been created, as required by her or his business associate contract. This would include the researcher's providing to the covered entity the mechanism for re-identification (the code key) and retaining no copy or other method of re-identification. In cases where the researcher has a standard method for assigning a re-identification code that necessarily remains with the researcher even after the other identifiers have been returned or destroyed, the information is not considered de-identified if the researcher assigns such a re-identification code.

Q: Is a covered entity's patient list that includes only names and addresses considered to be PHI if there is no other health or payment information attached?

A: Yes, because the names are in a context that indicates that the individuals named were patients of the covered entity. See the Privacy Rule's definition of "individually identifiable health information" at section 160.103, which explicitly includes demographic information collected from an individual.

Q: My health services research study at a covered entity involves obtaining information about patients' behaviors. If the only information I collect pertains to behaviors that could affect an individual's health–not diagnosis or other medical information–is this information PHI if it is identifiable?

A: Yes. In general, information about health behaviors is PHI if it:

(1) is held by a covered entity,

(2) identifies the individual or if there is a reasonable basis to believe the information could identify the individual, and

(3) 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 health care.

Although it may not reveal a diagnosis or identify a medical condition, the information would be PHI as long as it relates to a past, present, or future physical or mental health condition of an individual and the other above criteria are met.

Q: A covered entity wants to conduct several studies to assess why some individuals do not sign the acknowledgment of receipt of the Notice of Privacy Practices, why some do not sign Authorization forms, and why others revoke their Authorizations. Is this permissible under the Privacy Rule?

A: Such studies may be considered a health care operation of a covered entity or research, depending on whether the primary purpose of the study is to develop or contribute to generalizable knowledge. If the primary purpose of such a study is to produce generalizable knowledge, then the activity does not meet the

definition of "health care operations," but is, instead, "research," and any use or disclosure of PHI for such a study must be made in accordance with the Privacy Rule's research provisions on the use and disclosure of PHI for research (e.g., with an IRB or Privacy Board waiver or alteration of the Authorization requirement). If, however, a covered entity is conducting a quality improvement or assessment study, the primary purpose of which is not to develop or contribute to generalizable knowledge, then the study is considered to be a health care operation, and the covered entity may use or disclose PHI for the study as part of its health care operations under the Privacy Rule.

Q: My employer, a covered entity, is contemplating disclosing PHI for a research study under an IRB's waiver of the Authorization requirement. However, our Notice of Privacy Practices does not include a statement about "research." Would we need to revise our Notice of Privacy Practices to include research uses and disclosures that are permitted without Authorization?

A: Yes. Any use or disclosure of PHI made by a covered entity must be consistent with its Notice of Privacy Practices, where the Privacy Rule requires the covered entity to have one. Among other things, the Notice must describe the uses and disclosures that the covered entity is permitted to make without an Authorization. Therefore, a covered entity is not permitted to use or disclose PHI for research activities without an Authorization if the covered entity's Notice does not so inform individuals.

Q: A researcher requests data that include a code derived from the last four digits of the Social Security number. This code is necessary to link individual records from different data sources (but is not used by the covered entity to re-identify the individual). The data contain none of the other identifiers listed at section 164.514(b)(2) of the Privacy Rule. Are the data considered to be de-identified under the Privacy Rule?

A: Generally not. Under the "safe-harbor" de-identification standard of the Privacy Rule, a de-identified data set may not contain unique identifying codes, except for codes that are not derived from, or do not relate to, information about the individual and that cannot be translated so as to identify the individual. A code derived from part of a Social Security number, medical record number, or other identifier would not meet this test. However, the Privacy Rule does permit, as an alternative to the "safe-harbor" method, covered entities to de-identify health information using a statistical method. The statistical method requires that a qualified statistician or scientist, applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, determine that the risk is very small that the remaining information could be used, alone or in combination with other reasonably available information, to identify an individual. In some cases, this statistical method may require the removal of fewer identifiers or allow certain identifiers to remain with the information as long as the risk of re-identification remains very small. See section 164.514(a)-(c) of the Privacy Rule for additional information about de-identification.

Q: May information de-identified under the Privacy Rule's "safe-harbor" method contain a data element that identifies a time period of less than a year (e.g., the fourth quarter of a specific year)?

A: No. The Privacy Rule's "safe-harbor" method for de-identifying health information requires removal of, among other elements, all elements of dates directly related to an individual, except for year. Thus, a data element such as the fourth quarter of a specified year must be removed if a covered entity intends to de-identify data using the "safe-harbor" method. However, fewer identifiers may need to be removed under the Privacy Rule's alternative method for de-identification, where a qualified statistician, applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, determines that the risk of re-identification is very small. Thus, it may be possible for certain elements of dates to be considered de-identified where this second method allows it. See section 164.514(b)(1) of the Privacy Rule.

As an alternative to de-identified data, the Privacy Rule would permit a covered entity to use or disclose information about dates in the form of a limited data set.

Q: May a limited data set contain ages over 89 years?

A: Yes. A limited data set may contain all ages, including those over 89, and all elements of dates indicative of such age.

Q: Must a covered entity account for disclosures of PHI contained in a limited data set?

A: No. The accounting requirement does not apply to disclosures of a limited data set. See section 164.528(a)(1)(viii) of the Privacy Rule.

Q: My medical research center is a covered entity. Does the Privacy Rule apply when we obtain a limited data set, or other PHI, from another source?

A: Yes. A covered entity is required to protect the PHI it receives as well as the PHI it creates. Moreover, when a covered entity receives a limited data set from another covered entity, the limited data set can be used and disclosed only within the bounds of the data use agreement.

Q: May an IRB or Privacy Board waive the Authorization requirement so that a covered entity may obtain Authorization for research orally?

A: Yes. A covered entity is permitted to use or disclose PHI for research based on proper documentation from an IRB or Privacy Board that waives the Authorization requirement so that verbal permission can be obtained.

Q: Does the minimum necessary standard apply to research permissions that qualify for the transition provisions of the Privacy Rule (e.g., an informed consent document that was obtained prior to April 14, 2003)?

A: Yes. Since a "grandfathered" permission does not meet the requirements of section 164.508 of the Privacy Rule for Authorizations, the minimum necessary standard applies. Thus, covered entities are required to make reasonable efforts to limit uses and disclosures of PHI pursuant to permissions for research "grandfathered" by the Privacy Rule to the minimum amount necessary to accomplish the research purpose.

Q: Would the transition provisions apply if a covered entity obtained informed consent from study participants before the Privacy Rule compliance date but did not begin the research until after the compliance date?

A: Yes. Under the transition provisions of the Privacy Rule at section 164.532(c), a covered entity is permitted to use or disclose PHI pursuant to one of the listed permissions obtained prior to the compliance date, even if the research study did not begin until after the compliance date.

Q: Is a noncovered entity required to enter into a data use agreement before sending what would qualify under the Privacy Rule as a limited data set to the covered entity?

A: No. Such information is not considered PHI because it does not originate from a covered entity, and thus, it is not considered to be a limited data set under the Privacy Rule. However, the information will be considered PHI when in the hands of the recipient covered entity and, thus, may be used and disclosed only by the recipient in accordance with the Privacy Rule.

Q: Must disclosures of a limited data set for research be research-study specific?

A: No.

Q: I am a researcher who works in the health care component of a hospital and obtained the appropriate documentation of an IRB waiver to disclose PHI for my research study. To conduct this study, I need to share with research collaborators certain PHI covered by the waiver, including dates of service, ZIP Codes, and medical record numbers. Must I account for the research disclosures of this information, and if so, how can I do so when the names or identities associated with the PHI are unknown to me?

A: The Privacy Rule requires covered entities to account for certain disclosures of PHI, including those made pursuant to an IRB waiver of Authorization, regardless of whether the disclosure includes the name or otherwise directly identifies the individual. However, the Privacy Rule affords covered entities significant latitude in designing compliance methods for the accounting requirement. For example, disclosures of PHI need not be noted in each individual's file. Rather, a covered entity may, if convenient, keep track of disclosures of PHI using the medical record number. When an individual requests an accounting, the individual's medical record number may be used to determine whether any disclosures have been made of his or her PHI.

In addition, where the PHI of 50 or more individuals has been disclosed for a particular research purpose pursuant to documentation of an IRB waiver or alteration of Authorization, the covered entity may provide a more simplified accounting to individuals that lists, among other things, the name of the protocol(s) for which the individuals' information may have been disclosed. See section 164.528(b)(4) of the Privacy Rule.

Q: May a researcher access PHI through a remote access connection as a review preparatory to research?

A: Under certain, specified conditions and reasonable and appropriate security safeguards, yes. However, covered entities must comply with the relevant standards in both the Privacy Rule and Security Rule (upon its compliance date) before access to PHI through a remote access connection for preparatory research purposes is permitted to occur.

Under the Privacy Rule, covered entities are permitted to use or disclose PHI for reviews preparatory to research if the researcher provides representations that satisfy section 164.512(i)(1)(ii). The required representations must, among other things, provide that no PHI will be removed from the covered entity by the researcher in the course of the review. Remote access connectivity (i.e., out-of-office computer access achieved through secure connections with access permissions and authentication) involves a transmission of electronic PHI, which is not necessarily a removal of PHI under the Privacy Rule. However, although the access to PHI through a remote access connection is not itself a removal of PHI, the printing, copying, saving, or electronically faxing of such PHI would be considered to be a removal of PHI from a covered entity.

The Privacy Rule permits a covered entity to rely on representations from persons requesting PHI if such reliance is reasonable under the circumstances. In the case of a request by a researcher to access PHI remotely, this means that, among other things, the risk of removal, as described above, should be assessed in order to determine whether it is reasonable to rely on the researcher's representation that the PHI will not be removed from the covered entity. The covered entity should determine whether its reliance is reasonable based on the circumstances of the particular case.

For example, a covered entity may conclude that it can reasonably rely on representations from researchers who are its employees or contractors because their activity is manageable through the covered entity's employment and related policies establishing sanctions for the misuse of PHI. On the other hand, where the researcher has no connection to the covered entity, the covered entity may conclude that it cannot reasonably rely on the researcher's representations that PHI will not be removed from the covered entity, unless the researcher's activity is managed in some other way.

Covered entities that permit their workforce or other researchers to access PHI via a remote access connection must also comply with (on and after the compliance date) the Security

Rule's requirements for appropriate safeguards to protect the organization's electronic PHI. Specifically, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to protect the integrity of, and guard against the unauthorized access to, electronic PHI. The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect electronic PHI as it is transmitted, select a solution, and document the decision.

Q: May a researcher, who is a workforce member of an affiliated covered entity (ACE), take away PHI from another covered entity within the ACE under a review preparatory to research?

A: Yes. Affiliated covered entities are legally separate covered entities that designate themselves as a single covered entity, for purposes of the Privacy Rule. A covered entity is permitted to use or disclose PHI for a review preparatory to research as long as the PHI is not removed from the covered entity and other required representations are obtained. Thus, PHI can be reviewed for such purposes throughout the various members of the affiliated covered entity as long as PHI does not leave the premises of the affiliated covered entity and the required representations are obtained from the researcher. However, in order for a covered entity within the ACE to use or disclose PHI for a research study, it must obtain the individual's Authorization, obtain documentation of a waiver from an IRB or Privacy Board, or meet other conditions for the research use or disclosure under the Privacy Rule.

Q: How is a limited data set different from a designated record set?

A: A limited data set refers to PHI that excludes 16 categories of direct identifiers and that may be used or disclosed for purposes of research, public health, or health care operations as long as the covered entity enters into a data use agreement with the recipient of the information. A limited data set can be used or disclosed without obtaining either an individual's Authorization or a waiver or an alteration of Authorization. A covered entity may use and disclose a limited data set for research activities conducted by itself, another covered entity, or a researcher. Because limited data sets may contain identifiable information, they are still PHI.

A designated record set is "a group of records maintained by or for a covered entity that is (1) The medical records and billing records about individuals maintained by or for a covered health care provider; (2) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) Used, in whole or in part, by or for the covered entity to make decisions about individuals." A record is any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity. The Privacy Rule generally gives individuals the right to see and get a copy of their PHI in (a) designated record set(s). Research records maintained by a covered entity may be part of a designated record set if, for example, they also are medical records or if they are not medical records but are otherwise used to make decisions about individuals.

Q: If a researcher, who is a workforce member of a covered provider (not a hybrid entity), obtains through a waiver of Authorization a copy of individually identifiable medical and billing records from that covered provider for health services research, do individuals have a right to access this copy of their PHI?

A: Generally, individuals have the right to access their PHI within designated record sets. A designated record set is defined to include medical records or billing records about individuals maintained by or for a covered health care provider. (A record, in this regard, means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.) Research records maintained by a covered entity constitute a designated record set if, for example, it is a medical or billing record about the individual that is maintained by or for the covered health care provider or is a record that is used, in

whole or in part, by the covered health care provider to make decisions about the individual. However, the Privacy Rule does not require that an individual be provided access to every copy or duplicate of PHI in a designated record set that may be maintained by the covered entity. Rather, a covered entity meets the Privacy Rule's requirements by providing the individual access to only one copy of the PHI. Thus, in cases where a covered entity has copies of medical and billing records in both its treatment and research records, the covered entity need only provide access to one set, when such access is requested by the individual.

Q: I am a noncovered researcher who received an individual's written revocation of an Authorization that had permitted several covered hospitals to provide PHI to me. Does the Privacy Rule require me to stop using the PHI for my research?

A: No. However, when an individual revokes an Authorization, the covered entity may not provide further data about the individual, and thus, such information could not be provided if the researcher asks for it. Also, a valid Authorization must inform the individual how the Authorization may be effectively revoked, and depending on the revocation process described in the Authorization, the researcher may have undertaken additional obligations to ensure that the individual's revocation is effectuated (i.e., the researcher may be under contractual or ethical obligations that prohibit her or him from requesting or receiving the individual's data after receiving the revocation).

Q: If an individual revokes his or her Authorization after PHI is stored in a covered entity's database for a particular research study, is the covered entity permitted to retain and use that individual's PHI for data analysis?

A: Yes, if the use or disclosure of such PHI is necessary to protect the integrity of the research (i.e., to make sure the research study is still reliable, for example). In general, a research subject has the right to revoke, in writing, his or her Authorization at any time, and the revocation is effective when the covered entity receives it in writing; but an individual may not revoke the Authorization to the extent that the covered entity has already acted in reliance on the Authorization. For example, a covered entity is not required to retrieve information that it disclosed under a valid Authorization before receiving the revocation. Likewise, for research uses and disclosures, the reliance exception would permit the continued use and disclosure of PHI already obtained pursuant to the Authorization to the extent necessary to protect the integrity of the research, for example, to account for the individual's withdrawal from the study. However, the reliance exception would not permit a covered entity to continue disclosing additional PHI to a researcher or to use for its own research purposes information not already gathered at the time an individual withdraws his or her Authorization.

Q: Is a covered entity permitted, after the Privacy Rule compliance date, to waive or alter the Authorization requirement for the use or disclosure of psychotherapy notes?

A: No. An IRB or Privacy Board may not grant a waiver or alteration of Authorization for the use or disclosure of psychotherapy notes. The Privacy Rule provides individuals with special protections for psychotherapy notes, which are notes recorded by a mental health provider that document or analyze counseling session conversations and that are maintained separately from the medical record. Unless the covered provider obtained, prior to the compliance date of the Privacy Rule, the individual's informed consent or other express legal permission for the research or an IRB waiver of informed consent for the research, a covered entity may not use or disclose these notes for research without the individual's written Authorization.

Q: I know that the Privacy Rule permits a covered entity to disclose decedents' PHI for research without Authorization or waiver, if the covered entity obtains certain representations from the researcher. May the covered entity also disclose the PHI of minor decedents to researchers, without obtaining Authorization from the person with authority to act on behalf of the decedent?

A: Yes. If the covered entity obtains the representations required by section 164.512(i)(1)(iii) from the researcher, the

Privacy Rule permits a covered entity to use or disclose a decedent's PHI for research without Authorization from an executor, administrator, or other person having authority to act on behalf of the deceased individual or the individual's estate, even if the decedent is a minor. In addition to the required representations, the covered entity also may request that the researcher produce documentation of the death of each subject whose PHI is sought for the research.

Q: May an Authorization identify a third-party recipient's future use or disclosure of individually identifiable health information?

A: Yes. A valid Authorization may identify more than one purpose of the disclosure. For example, a research Authorization may state, "As part of this study, we may share your hospital discharge records with the sponsor of this study, the State hospital association, which may conduct a followup hospital discharge outcome study." It should be noted, however, that the Authorization need not describe the third party's uses and disclosures of PHI.

Q: May a covered entity rely on an Authorization signed by parent on behalf of a minor child, even after the child has reached the age of majority? Similarly, would the Privacy Rule's transition provisions "grandfather" an informed consent signed by a minor's parent even if the child reached the age of majority before the Privacy Rule compliance date?

A: Yes. A valid Authorization signed by a parent, as the personal representative of a minor child at the time the Authorization is signed, remains valid until it expires or is revoked, even if such time extends beyond the child's age of majority. If the Authorization expires on the date the minor reaches the age of majority, the covered entity would be required to obtain a new Authorization form signed by the individual in order to further use or disclose PHI covered by the expired Authorization.

In addition, the Privacy Rule's transition provisions at section 164.532(c) "grandfather" permissions for research (e.g., an informed consent) obtained prior to compliance with the Privacy Rule (usually, April 14, 2003). Therefore, even if the child has reached the age of majority, the Privacy Rule "grandfathers" a parent's consent on behalf of his or her minor child for research so that the consent remains valid until it expires or is withdrawn.

Q: May a covered entity contract with a researcher as a business associate to avoid complying with the research requirements under the Privacy Rule with respect to disclosures to the researcher?

A: No. A covered entity may hire a researcher as a business associate to perform certain functions on its behalf, such as to create a limited data set or to create de-identified data. The business associate agreement must require, among other things, that the researcher return or destroy the PHI at termination of the contract, if feasible, and also must limit the uses and disclosures the researcher may make with the PHI. See sections 164.502(e) and 164.504(e) of the Privacy Rule. A covered entity may not use the business associate provisions to avoid having to comply with the conditions for research disclosures. Where a covered entity wishes to disclose PHI to a researcher for a research purpose, it must first obtain the individual's Authorization, obtain a waiver or alteration of Authorization from an IRB or Privacy Board, enter into a data use agreement if disclosing only a limited data set, or meet other conditions, as appropriate. This is true regardless of whether the covered entity and the researcher have entered into another contract or agreement.

Q: What is "data aggregation" under the Privacy Rule, and does it apply to combining multiple data sets for research?

A: The Privacy Rule allows a covered entity to disclose PHI to a business associate, subject to the terms of a business associate agreement, for the purpose of data aggregation. Data aggregation, for purposes of the Privacy Rule, occurs when a business associate of one covered entity combines the PHI it receives from that covered entity with other PHI from another covered entity (with whom it also has a business associate relationship) in order to permit the creation of data for analyses that relate to the health care operations of the respective covered entities. Covered entities are permitted to

contract with business associates to undertake quality assurance and comparative analyses that involve the PHI of more than one contracting covered entity. For example, a State hospital association could act as a business associate of its member hospitals and could combine data provided to it to assist the hospitals in evaluating their relative performance in areas such as quality, efficiency, and other patient care issues. However, the business associate contracts of each of the hospitals would have to permit the activity, and the PHI of one hospital could not be disclosed to another hospital unless the disclosure is otherwise permitted by the Rule (e.g., as de-identified information or a limited data set). A covered entity may hire a health services researcher as a business associate to perform such data aggregation services.

Although covered entities may participate in certain research activities that involve combining multiple sets of data for research (e.g., for a meta-analysis), such an activity is not considered data aggregation, as defined by the Privacy Rule, unless the activity is undertaken by a business associate in support of a covered entity's health care operations. Multiple covered entities may disclose PHI to a researcher for the researcher to combine the multiple sets of data for research without business associate agreements, because a research activity is not a business associate function or activity (e.g., a health care operation of a covered entity). However, each covered entity's disclosure of PHI to a researcher for research purposes must be permitted by the Privacy Rule (e.g., with an Authorization, waiver of the Authorization requirement, or as a limited data set).

Q: Is a covered entity permitted, as part of its health care operations activities, to disclose PHI to a business associate to create de-identified data or a limited data set that may function as a research database? Or does the covered entity need an Authorization or a waiver or alteration of the Authorization requirement for this activity?

A: In the Privacy Rule, creating de-identified data or a limited data set is a health care operation of the covered entity and, thus, does not require the covered entity to obtain an individual's Authorization or a waiver of the Authorization requirement, even if the limited data set or de-identified data will function as a research database. However, if a business associate is hired by a covered entity to create de-identified data or a limited data set, such activity must be conducted in accordance with the business associate requirements at sections 164.502(e) and 164.504(e).

A covered entity's subsequent disclosure of a limited data set–in any form, including as a database–for research must be made pursuant to a data use agreement between the covered entity and the recipient of the limited data set.

Q: Does the Privacy Rule permit a researcher who is a covered workforce member of a covered entity to transfer PHI, without individual Authorization, to another institution if, for example, the researcher changes jobs?

A: No, unless the original permission under which the researcher obtained or created the data (such as the individual's Authorization or a waiver by an IRB) was granted explicitly for the researcher himself or herself, rather than solely for the covered entity. Otherwise, any transfer of PHI from one covered entity to another entity for these research purposes must be done according to a new permission (Authorization, waiver, etc.) that covers such disclosure.

Q: I work at a community health center that is named for our city. Does the name of our health center need to be removed from the data before they can be considered de-identified under the de-identification safe harbor provisions at section 164.514(b)(2)(i) of the Privacy Rule? All other required data elements to be removed for de-identification have been stripped from the data.

A: No, provided the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify the individual, the name of the health center need not be stripped. The de-identification provisions at section 164.514(b)(2)(i) require, among other things, that most elements of the individual's address, including the name of the city, be removed from the data, not that the name or address of the provider be removed.

Q: Does the Privacy Rule permit covered entities to disclose PHI, to be used for public health activities described in section 164.512(b), to government agencies, such as the Agency for Healthcare Research and Quality (AHRQ), that also carry out research with this PHI and other data?

A: Yes, under appropriate conditions. Covered entities may disclose PHI to a government agency such as AHRQ, which has research and public health missions or mandates, as a public health disclosure to a public health authority if the conditions for such disclosures under section 164.512(b) are met. Thus, for example, the disclosure would be permitted under section 164.512(b)(1)(i) if the government agency is a public health authority (i.e., it is responsible for public health matters as part of its official mandate) and is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability or for the conduct of public health surveillance, investigations, or interventions. Examples of disclosures that may be permitted under section 164.512(b)(1)(i), where the public health authority is authorized by law to collect such information, are situations in which reports of adverse drug events are requested by the public health authority to find and publicize common prescription errors (the purpose of which is to improve public safety through the prevention of injury or disability) or the public health authority collects health care utilization data to monitor surgical outcomes (the purpose of which is public health surveillance). There may be cases where PHI that is disclosed for the conduct of public health activities also may be used by the government agency for research (e.g., monitoring patient safety trends and performing analysis of the data for research on systemic causes of medical error). In those cases, disclosures of PHI may be made either under the research provisions or under the public health provisions; the covered entity need not comply with both sets of requirements. For additional guidance on disclosures of PHI for public health purposes to a government agency that also conducts research, see *HIPAA Privacy Rule and Public Health: Guidance from CDC and the U.S. Department of Health and Human Services*, located at http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm.

---

[1] The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed: (1) Names; (2) all geographic subdivisions smaller than a State, except for the initial three digits of the ZIP Code if the geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people; (3) all elements of dates, except year, and all ages over 89 or elements indicative of such age; (4) telephone numbers; (5) fax numbers; (6) email addresses; (7) Social Security numbers; (8) medical record numbers; (9) health plan beneficiary numbers; (10) account numbers; (11) certificate or license numbers; (12) vehicle identifiers and license plate numbers; (13) device identifiers and serial numbers; (14) URLs; (15) IP addresses; (16) biometric identifiers; (17) full-face photographs and any comparable images; and (18) any other unique, identifying characteristic or code, except as permitted for re-identification in the Privacy Rule.

[2] A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.

[3] The following direct identifiers of the individual or of relatives, employers, or household members must be removed for PHI to qualify as a limited data set: (1) Names; (2) postal address information, other than town or city, State, and ZIP Code; (3) telephone numbers; (4) fax numbers; (5) email addresses; (6) Social Security numbers; (7) medical record numbers; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate or license numbers; (11) vehicle identifiers and license plate numbers; (12) device identifiers and serial numbers; (13) URLs; (14) IP addresses; (15) biometric identifiers; and (16) full-face photographs and any comparable images.

NIH Publication Number 05-5308 May 2005