Research Repositories, Databases, and the HIPAA Privacy Rule

Overview

Researchers in medical and health-related disciplines require access to many sources of health information, from archived medical records and epidemiological databases to disease registries, tissue repositories, hospital discharge records, and government compilations of vital and health records. As the Privacy Rule is implemented, researchers are asking how these rules might affect research that uses records within databases and repositories.

As of April 14, 2003, the Privacy Rule requires many health care providers and health insurers to obtain additional documentation from researchers before disclosing health information to them, 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 for research, 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 fact sheet discusses the Privacy Rule and its potential to affect the creation of research databases and repositories, and research that uses identifiable health information in repositories and databases. Additional information about the Privacy Rule's potential impact on other research activities, such as clinical research, health services research, institutional review boards (IRBs) and Privacy Boards can be found in related publications, including:

- *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*
- *Health Services Research and the HIPAA Privacy Rule*
- *Clinical Research 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 Department of Health and Human Services (HHS) issued regulations entitled, *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 are 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 insurer), they may have to comply with that entity's HIPAA privacy 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. The HHS and the Food and Drug Administration's (FDA) Protection of Human Subjects Regulations (45 CFR part 46 and 21 CFR parts 50 and 56, respectively) may also apply to research involving the development or use of research repositories and associated data.

Overview of the Privacy Rule's Impact on Repositories and Databases

The Privacy Rule was not intended to impede research using records within databases and repositories that include individuals' health information, but the Privacy Rule does place new conditions on the use and disclosure of PHI by covered entities for research. The creation of a research database or repository, and the use or disclosure of PHI from a database or repository for research, may each be considered a research activity under the Privacy Rule. For more specific information about how the Privacy Rule could affect health services research, refer to the related publication, *Health Services Research and the HIPAA Privacy Rule*.

It is important to know that the Privacy Rule permits covered entities, such as hospitals, clinics, and other health care providers to continue amassing information on their patients for treatment, payment, and health care operations purposes, and to enter this information into their own databases without Authorization. The Privacy Rule also allows the disclosure of PHI to government-authorized public health authorities for disease surveillance, disease prevention, and other public health purposes, such as reporting disease and injury. When required by law, other disclosures are permitted, for example, state-mandated reporting to cancer registries. Covered entities may also continue to disclose PHI for adverse event and related reports to FDA and others for public health purposes (see section 164.512 of the Privacy Rule and additional information at *http://www.cdc.gov/mmwr/early_release.html*). Thus, many databases that are now used for records research continue to be maintained and updated, and will remain available to records researchers, although in some cases, under new terms.

The Privacy Rule permits a covered entity to use or disclose PHI for research under the following circumstances and conditions:

- For reviews preparatory to research if certain representations are obtained from the researcher
- For research solely on decedents' information if certain representations are obtained from the researcher
- If the subject of the PHI has granted specific written permission through an Authorization
- If the covered entity receives appropriate documentation that an IRB or Privacy Board has granted a waiver or an alteration of the Authorization requirement
- If the PHI has been de-identified in accordance with the standards set by the Privacy Rule (in which case, the health information is no longer PHI)
- If the information is released in the form of a limited data set, with certain identifiers removed, and with a data use agreement between the researcher and the covered entity
- If informed consent of the individual to participate in the research, an IRB waiver of such informed consent, or other express legal permission to use or disclose the information for the research is grandfathered by the transition provisions

For some records and database research, Authorization may not be needed. Some of the most important exceptions to the Authorization requirement that pertain to research using repositories and databases are the waiver of Authorization and the limited data set.

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

For some types of research, it 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 the waiver or alteration of 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 received 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 evaluated by an IRB or Privacy Board in approving an Authorization waiver or alteration. For a covered entity to use or disclose PHI under a waiver or alteration of the Authorization requirement, it must receive documentation of, among other things, the IRB or Privacy Board's determination that the following criteria have been met:

- The PHI 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.
- The research could not practicably be conducted without access to and use of the PHI.

Additional information about 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*.

De-identified Data Sets

The Privacy Rule permits covered entities to release data that have been de-identified without obtaining an Authorization and without further restrictions upon use or disclosure because de-identified data is not PHI and, therefore, 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, is to remove all 18 identifiers enumerated at section 164.514(b)(2) of the regulations.[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 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 know 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 that code is not derived from or related to the information about the individual and is not otherwise capable of being translated to identify the individual. For example, an encrypted individual identifier (e.g., a social security number) would not meet the conditions for use as a re-identification code for de-identified health information because it is derived from individually identified information. (See 67 *Federal Register* 53233, August 14, 2002.) In addition, the covered entity may not (1) use or disclose the code or other means of record identification for any purposes other than as a re-identification code for the de-identified data, and (2) disclose its method of re-identifying the information.

Limited Data Sets

Where only certain identifiers are needed, it may be permissible for a covered entity to provide a researcher with 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. They are not de-identified information under the Privacy Rule. Importantly, unlike de-identified data, protected health information 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.[3]

Before disclosing a limited data set to a researcher, a covered entity must enter into a data use agreement with the researcher, identifying the researcher as the recipient of the limited data set, establishing how the data may be used and disclosed by the recipient, and providing assurances that the data will be protected, among other requirements. 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*.

Activities Preparatory to Research

Covered entities may permit researchers to review PHI in medical records or elsewhere to prepare a research protocol, or for similar purposes preparatory to research. This review allows the researcher to determine, for example, whether a sufficient number or type of records exists 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.
- The PHI 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* and *Clinical Research 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: Representations that the decedents' PHI is necessary for the research and is being sought solely for research on the PHI of decedents (not, for example, living relatives of decedents); and, upon request of the covered entity, documentation of the deaths of the study subjects. No Authorization or alteration or waiver of Authorization by an IRB or Privacy Board is needed for use or disclosure of PHI for research only on the PHI of deceased persons, if these conditions are met.

Other Privacy Rule Requirements

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. If an IRB or Privacy Board has granted the researcher a waiver or an alteration of Authorization, a covered entity may reasonably rely upon the researcher's request consistent with the description of PHI in documentation from the IRB or Privacy Board as the minimum necessary amount of PHI for the research. Additional information on the minimum necessary standard can be found in the booklet, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*.

Right to an Accounting of Disclosures

The Privacy Rule grants individuals new rights, including the right to receive an accounting of disclosures made for research 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. For such

disclosures, in general, individuals who request an accounting must be told what 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 for 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.

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 a more general accounting to the requestor. The covered entity would provide the following information in the general accounting:

- 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
- The contact information of the researcher and the research sponsor
- 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, upon 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 of disclosures can be found in the booklet, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*.

Frequently Asked Questions and Answers

Q: Are tissue repositories covered entities?

A: Not unless the organization maintaining the tissue repository conducts some other activity that makes it a covered entity. For example, tissue repositories that conduct testing of specimens for the benefit of transplant recipients based on another health care provider's orders would be covered providers under HIPAA if they conduct electronic transactions for which the HHS has adopted standards.

Q: A researcher does not receive names, addresses, social security or medical record numbers, or other obvious identifiers from data sources. If the IRB has not considered this data to be individually identifiable in the past, and thus, determined that the research was not human subjects research under 45 CFR part 46, or that the research was exempt under 45 CFR 46.101(b), will this change under the Privacy Rule?

A: No. The Privacy Rule does not change the applicability or the requirements of the HHS and FDA Protection of Human Subjects Regulations. However, where the information sought by the researcher is held by a covered entity, the covered entity's use or disclosure of that information is subject to the Privacy Rule, unless the information is de-identified by the Privacy Rule's standards. The Privacy Rule's de-identification safe-harbor method is likely more stringent than what has been applied in the past to render information no longer identifiable for research purposes. De-identification under the Privacy Rule's safe-harbor standard may be accomplished through the removal of all 18 identifiers (section 164.514(b)(2) of the Privacy Rule).

Alternatively, fewer identifiers may need to be removed for health information to be de-identified if a qualified statistician determines that the risk of re-identification is very small (section 164.514(b)(1) of the Privacy Rule).

The Privacy Rule also permits a covered entity to retain, with the de-identified health information, a code for re-identification as long as the code is not related to or derived from information about the individual and is not otherwise capable of being translated to identify the individual, and as long as the covered entity does not disclose its method of re-identification or use or disclose its code for other purposes (section 164.514(c) of the Privacy Rule). For example, a randomly assigned re-identification code would not make the de-identified information to which it is assigned PHI, because a random code would not be derived from or related to information about the individual.

Where a researcher needs data elements that would render the information identifiable under the Privacy Rule, but where certain direct identifiers (set forth in section 164.514(e)) are not needed, a limited data set may be sufficient for the research. A limited data set is information stripped of only the direct identifiers listed at section 164.514(e), which include, but are not limited to, the name and street address of the individual. To use or disclose a limited data set, the covered entity must enter into a data use agreement with the recipient of the information.

In practice, this means that records research that may not require IRB approval under the HHS Protection of Human Subjects Regulations, still may require an Authorization or a waiver of Authorization under the Privacy Rule, or be subject to a data use agreement if a limited data set is used or disclosed.

Q: How may a covered entity use or disclose PHI for the creation of a research repository or database when it is unknown at the time of collection what specific protocols will make use of the repository or database in the future?

A: There are two separate activities to consider: (1) The use or disclosure of PHI for creating a research database or repository and (2) The subsequent use or disclosure of PHI in the database for a particular research protocol.

A covered entity's use or disclosure of PHI to create a research database or repository, and use or disclosure of PHI from the database or repository for a future research purpose, are each considered a separate research activity under the Privacy Rule. In general, the Privacy Rule requires Authorization for each activity, unless, for example, an IRB or Privacy Board waives or alters the Authorization requirement. (See **Overview of Privacy Rule's Impact on Repositories and Databases**.) Documentation of a waiver or an alteration of Authorization to use or disclose PHI to create a research database requires, among other things, a statement that an IRB or Privacy Board has determined that the researcher has provided adequate written assurances that PHI in the database will not be further used or disclosed except as permitted by the Privacy Rule (e.g., for research uses and disclosures with an Authorization or waiver). A covered entity also could use or disclose a limited data set to create a research repository or database under conditions set forth in a data use agreement.

For subsequent use or disclosure of PHI for research purposes from a repository or database maintained by the covered entity, the covered entity may:

- Obtain the individual's Authorization for the research use or disclosure of PHI as specified under section 164.508
- Obtain documentation of an IRB or Privacy Board's waiver of the Authorization requirement that satisfies section 164.512(i)
- Obtain satisfactory documentation of an IRB or Privacy Board's alteration of the Authorization requirement as well as the altered Authorization from the individual
- Use or disclose PHI for reviews preparatory to research with representations that satisfy

section 164.512(i)(1)(ii) of the Privacy Rule
- Use or disclose PHI for research on decedents' PHI with representations that satisfy section 164.512(i)(1)(iii) of the Privacy Rule
- Provide a limited data set and enter into a data use agreement with the recipient as specified under section 164.514(e)
- Use or disclose PHI based on permission obtained prior to the compliance date of the Privacy Rule—informed consent of the individual to participate in the research, an IRB waiver of such informed consent, or Authorization or other express legal permission to use or disclose the information for the research as specified under section 164.532(c) of the Privacy Rule

A covered entity may also use or disclose PHI from databases and repositories for other purposes without Authorization as permitted by the Privacy Rule, such as if required by law or to a public health authority for a public health activity (e.g., disclosures to cancer registries). Covered entities may also de-identify PHI according to standards set forth in the Privacy Rule so that its use and disclosure are not protected by the Privacy Rule.

Q: May a single Authorization permit a covered entity to use or disclose PHI for multiple activities of a specific research study, including the collection and storage of tissues for only that study? Does the option for using a single Authorization differ if a research study also collects and stores PHI as part of a central repository for future research?

A: A single Authorization may cover uses and disclosures of PHI for multiple activities of a specific research study, including the collection and storage of tissues for that study. In addition, where two different research studies are involved, such as where a research study collects information for the study itself, and collects and stores PHI in a central repository for future research, the Privacy Rule generally would permit them to be combined into a single, compound Authorization form.

However, a compound Authorization is not allowed where the provision of research-related treatment, payment, or eligibility for benefits is conditioned on only one of the Authorizations, and not the other. See section 164.508(b)(3)(iii) of the Privacy Rule. For example, a covered entity that conducts an interventional clinical trial that also involves collecting tissues and associated PHI for storage in a central repository for future research would not be permitted to obtain a compound Authorization for both research purposes if research-related treatment is conditioned upon signing the Authorization for the clinical trial. Any compound Authorization must clearly specify the different research studies covered by the Authorization so the individual is adequately informed.

Q: How could the Privacy Rule affect research involving data from repositories or databases that were created prior to the Privacy Rule's compliance date (April 14, 2003)?

A: The Privacy Rule contains a transition provision that, under certain conditions, allows covered entities to continue to use or disclose PHI without an Authorization, or waiver or alteration of the Authorization requirement, in connection with ongoing research, including research involving repositories or databases. For many such uses and disclosures of PHI in connection with ongoing research, a covered entity may rely on any one of the following that was obtained prior to the compliance date:

- An Authorization or other express legal permission from an individual to use or disclose PHI for research
- The informed consent of the individual to participate in the research
- 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

If the transition provisions do not apply and the information is not de-identified, subse-

quent uses and disclosures of PHI from databases and repositories held by covered entities generally require an individual's Authorization unless otherwise permitted by the Privacy Rule (e.g., with a waiver of Authorization or as a limited data set).

In addition, if the database or repository, which is held or maintained by a covered entity, contains only de-identified health information (which may include a re-identification code) meeting the Privacy Rule's requirements at section 164.514(a)-(c), the Privacy Rule does not apply.

Q: Does the Privacy Rule apply if a covered entity maintains and conducts research on a database of pre-existing specimens and data that are considered exempt from the HHS Protection of Human Subjects Regulations?

A. Yes, if the database contains PHI, the Privacy Rule applies. The covered entity, however, may de-identify the data by either: (1) Removing the 18 identifiable data elements listed at section 164.514(b)(2) of the Privacy Rule and having no actual knowledge that the information could be used, alone or in combination with other information, to identify the subject; or (2) having a qualified statistician's certification, with appropriate documentation, that there is a very small risk of identification by an anticipated recipient. If the information is not de-identified, subsequent uses and disclosures of PHI from databases and repositories held by covered entities generally require an individual's Authorization unless otherwise permitted by the Privacy Rule (e.g., with a waiver of Authorization or as a limited data set).

Q: A covered entity has a research repository and database of individually identifiable data for which the IRB waived informed consent for its creation and subsequent uses and disclosures of identifiable data prior to April 14, 2003. Is the covered entity required to obtain Authorization for research use and disclosure of PHI from the repository or database after April 14, 2003?

A: No, because the waiver, as described, meets the transition provisions of the Privacy Rule at 164.532(c). However, if informed consent is being sought from specimen donors after the compliance date, Authorization by the donors will be needed unless an IRB approves a waiver of the Authorization requirement, or another permitted use or disclosure applies.

Q: Does the Privacy Rule apply to databases held by covered entities that only receive de-identified participant data?

A: No, so long as the health information is de-identified according to the Privacy Rule, the Privacy Rule does not apply to the database or to future uses and disclosures of de-identified data from the database.

Q: May ongoing longitudinal studies continue after April 14, 2003?

A: Yes. Permissions or waivers obtained prior to the Privacy Rule's compliance date of April 14, 2003, for ongoing longitudinal studies are grandfathered by the Privacy Rule if they meet the transition provisions at 164.532(c). For many such uses and disclosures of PHI in connection with ongoing research, a covered entity may rely on any one of the following that was obtained prior to the compliance date:

- An Authorization or other express legal permission from an individual to use or disclose PHI for research
- The informed consent of the individual to participate in the research
- 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

Q: A researcher requests data that assigns 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. The data contain none of the other listed HIPAA identifiers at section 164.514(b)(2). Are the data de-identified under the Privacy Rule?

A: No. Under the Privacy Rule, a de-identified data set may not contain unique identifying codes, except for codes that have not been 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 does not meet this test.

Q: Does the Privacy Rule permit a covered entity to de-identify health information or create a limited data set without obtaining 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, creating de-identified health information 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, a waiver of the Authorization requirement, or representations for reviews preparatory to research. If a business associate is hired by a covered entity to de-identify health information or 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).

Q: What is a limited data set, and what are its advantages?

A: A limited data set is PHI that does not include a specified list of direct identifiers. The limited data set is not considered to be de-identified information, and unlike de-identified information, a limited data set may include identifiers such as ZIP codes, elements of dates, and unique identifiers not listed as direct identifiers at section 164.514(e). The advantage of a limited data set is that even though it is not de-identified, it can still be used or disclosed for research purposes without an Authorization or a waiver of the Authorization requirement. A covered entity must, however, enter into a data use agreement with the recipient of the limited data set before using or disclosing it. (See section 164.514(e) of the Privacy Rule.)

Q: What types of information (direct identifiers) must be omitted from PHI in order to qualify the information as a limited data set?

A: All the following direct identifiers of the individual or of relatives, employers, or household members of the individual must be removed:

- Name
- Street name or street address or post office box (i.e., not including city, state, or ZIP code)
- Telephone and fax numbers
- Email address
- Social security number
- Certificate/license numbers
- Vehicle identifiers and serial numbers
- URLs and IP addresses
- Full-face photos and other comparable images
- Medical record numbers, health plan beneficiary numbers, and other account numbers
- Device identifiers and serial numbers.
- Biometric identifiers, including finger and voice prints

Q: What is the difference between a de-identified data set and a limited data set?

A: A de-identified data set is one in which either: (1) The 18 identifiers specified in 164.514(b)(2)(i) have been removed and 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 (safe harbor method); or (2) a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, determines the risk is very small that the information could be used by the recipient, alone or in combination with other reasonably available information, to identify an individual (section 164.514(b)(1)), and documents the basis for such determination. A de-identified data set is not protected by the Privacy Rule and may be used and disclosed without restriction.

A limited data set is one that excludes the direct identifiers in 164.514(e)(2). Unlike a de-identified data set, a limited data set is PHI because it may include dates, city, state, and ZIP codes, and other unique identifying codes or characteristics not listed as direct identifiers. A limited data set may be used or disclosed, without Authorization, for research, public health, or health care operations purposes, in accordance with section 164.512(e), only if the covered entity and limited data set recipient enter into a data use agreement. However, if the use or disclosure could be made under another provision of the Privacy Rule, such as for public health purposes in accordance with section 164.512(b), such agreement is not required.

Q: Are an individual's initials considered to be identifiers under the Privacy Rule?

A: Yes, because an individual's name is an identifier and initials are derived from the individual's name, initials are considered identifiers under the Privacy Rule. Thus, for information to be de-identified using the safe harbor method of the Privacy Rule, an individual's initials must be stripped from the information. However, it may be possible for initials to remain as part of de-identified information if the statistical method for de-identification at section 164.514(b)(1) allows it.

Q: May a limited data set include the geographic subdivision code with the five-digit ZIP code (or a nine-digit ZIP code)?

A: Yes, the limited data set may include the five-digit or nine-digit ZIP code plus any other geographic subdivision, such as state, county, city, precinct, and their equivalent geocodes, except for street name or street address or post office box.

Q: May a covered entity use or disclose PHI to locate or identify the whereabouts of a research participant (e.g., subjects who are "lost to follow-up")?

A: A covered entity is permitted to use or disclose PHI to identify or locate the whereabouts of a research participant during the study as long as the use or disclosure is not limited in the individual's Authorization (or grandfathered prior permission, if relevant) or waiver or alteration of Authorization. In addition, such use or disclosure is permissible if, for example, it is necessary for treatment of the individual or for a permissible public health purpose.

Q: What special requirements apply to research involving PHI from mental health providers?

A: The Privacy Rule provides individuals special protection for psychotherapy notes, which are notes recorded by a mental health provider that document or analyze counseling session conversations, and are maintained separately from the medical record. Unless the covered provider obtained, prior to the compliance date, 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. Information in the medical record and certain types of information, even if maintained separately from the medical record (e.g., information about test results, length and frequency of treatment, diagnosis, symptoms, or progress), is excluded from the definition of psychotherapy notes and may be released to researchers who obtain an Authorization or a waiver of Authorization from an IRB or Privacy Board, as part of a limited data set, or if appropriate, for reviews preparatory to research or for research involving decedent's information where required representations are obtained. Special requirements also apply to compound authorizations involving the use or disclosure of psychotherapy notes. (See section 164.508(b)(3)(ii) of the Privacy Rule.) Various state laws governing the use or disclosure of mental health records, including psychotherapy notes, which are more stringent than the Privacy Rule provisions, may also apply.

Q: How does the Privacy Rule apply to research involving blood or tissue samples?

A: Under the Privacy Rule, neither blood nor tissue, in and of itself, is considered individually identifiable health information; therefore, research involving only the collection of blood or tissue would not be subject to the Privacy Rule's requirements. Remember, however, blood and tissue are often labeled with information (e.g., admission date or medical record number) that the Privacy Rule considers individually identifiable and thus, PHI. A covered entity's use or disclosure of this information for research is subject to the Privacy Rule. In addition, the results from an analysis of blood and tissue, if containing or associated with individually identifiable information, would be PHI.

Q: Do the transition provisions apply to a surgical consent obtained by a covered provider that was signed or agreed to prior to the removal of tissues that were later added to a repository?

A: Yes, the transition provisions would apply in this case if, in the surgical consent or other express legal permission, the individual specifically agreed to the use and disclosure of PHI for research.

Q: Do the transition provisions at section 164.532(c) of the Privacy Rule apply to informed consent or waiver of informed consent to store and use PHI in a repository or database that was obtained before the compliance date?

A: Yes. HHS has stated, "…some express legal permissions and informed consents have not been study-specific and sometimes authorize the use or disclosure of information for future unspecified research. Furthermore, some IRB-approved waivers of informed consent have been for future unspecified research. Therefore, the final Rule at [section] 164.532 permits covered entities to rely on an express legal permission, informed consent, or IRB-approved waiver of informed consent for future unspecified research, provided the legal permission, informed consent or IRB-approved waiver was obtained prior to the compliance date." (See 67 *Federal Register* 53226, August 14, 2002.)

Q: Does the Privacy Rule limit, to specific types of research studies, disclosures permitted as preparatory to research or for research on decedents' information?

A: No. The Privacy Rule does not limit the types of research studies that may rely upon the provisions for reviews preparatory to research or for research on decedents' information set forth at section 164.512(i). However, representations made to satisfy these provisions must include, among other requirements at sections 164.512(i)(1)(ii) and 164.512(i)(1)(iii), a statement that the use or disclosure of protected health information is "necessary for the research purposes."

Q: Does the Privacy Rule restrict access for research purposes to information held by the Medicaid or SCHIP programs?

A: Yes. Local and state Medicaid authorities are covered entities under HIPAA, as are the State Children's Health Insurance Program (SCHIP) programs. These agencies or programs are covered under the Privacy Rule because they are listed in the Privacy Rule's definition of a "health plan." All SCHIP programs and state Medicaid agencies must consequently comply with the Privacy Rule; if they are hybrid entities, they must ensure that their designated health care components comply with the Privacy Rule. These government units will have some mechanism (a privacy officer, a Privacy Board, and/or an IRB) for controlling access to PHI for research purposes. A researcher will need to identify the responsible party and discuss with that office or official the ways in which access to PHI may be granted for research.

Q: In conducting records research, will a researcher who is a covered entity still be required to comply with state laws relating to medical records privacy, such as state HIV/AIDS confidentiality laws?

A: Probably. If the state law does not conflict with the Privacy Rule, the state law is not preempted by HIPAA, and the covered entity will be required to comply with both the state law and the Privacy Rule. If the state law conflicts with a provision of the Privacy Rule, the Privacy Rule has a preemption provision that allows state medical privacy laws to remain in place, if they are more stringent than the federal privacy standards. The Privacy Rule does not prohibit states from adopting privacy protections that are more stringent than the federal privacy standards.

Q: I am a researcher, and my research data source is asking me to sign a business associate agreement. Is this necessary?

A: Business associates are persons who perform certain services for, or functions or activities on behalf of, the covered entity that require access to PHI, but who are not part of the workforce of the covered entity. If the data source is not a covered entity, no business associate contract is required because the Privacy Rule only applies to covered entities.

If the data source is a covered entity, whether a business associate contract is required depends on the services, functions, or activities that the researcher is providing to or performing for the covered entity. Researchers are not business associates solely by virtue of their own research activities (although they may become business associates in some other capacity, e.g., if de-identifying PHI on behalf of a covered entity). A business associate agreement will typically be a legally enforceable contract, so a researcher may wish to consult legal counsel before signing one.

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

A. No. The accounting requirement does not apply to limited data set disclosures.

[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; (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 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 04-5489 January 2004