How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule?

Key Points:

- De-identified health information, as described in the Privacy Rule, is not PHI, and thus is not protected by the Privacy Rule.
- PHI may be used and disclosed for research with an individual's written permission in the form of an Authorization.
- PHI may be used and disclosed for research without an Authorization in limited circumstances: Under a waiver of the Authorization requirement, as a limited data set with a data use agreement, preparatory to research, and for research on decedents' information.

The Privacy Rule describes the ways in which covered entities can use or disclose PHI, including for research purposes. In general, the Rule allows covered entities to use and disclose PHI for research if authorized to do so by the subject in accordance with the Privacy Rule. In addition, in certain circumstances, the Rule permits covered entities to use and disclose PHI without Authorization for certain types of research activities. For example, PHI can be used or disclosed for research if a covered entity obtains documentation that an Institutional Review Board (IRB) or Privacy Board has waived the requirement for Authorization or allowed an alteration. The Rule also allows a covered entity to enter into a data use agreement for sharing a limited data set. There are also separate provisions for how PHI can be used or disclosed for activities preparatory to research and for research on decedents' information.

It is important to note that there are circumstances in which health information maintained by a covered entity is not protected by the Privacy Rule. PHI excludes health information that is de-identified according to specific standards. Health information that is de-identified can be used and disclosed by a covered entity, including a researcher who is a covered entity, without Authorization or any other permission specified in the Privacy Rule. Under the Privacy Rule, covered entities may determine that health information is not individually identifiable in either of two ways. These are described below.

De-identifying Protected Health Information Under the Privacy Rule

Covered entities may use or disclose health information that is de-identified without restriction under the Privacy Rule. Covered entities seeking to release this health information must determine that the information has been de-identified using either statistical verification of de-identification or by removing certain pieces of information from each record as specified in the Rule.

The Privacy Rule allows a covered entity to de-identify data by removing all 18 elements that could be used to identify the individual or the individual's relatives, employers, or household members; these elements are enumerated in the Privacy Rule. The covered entity also must have no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is the subject of the information. Under this method, the identifiers that must be removed are the following:

1. Names.
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. Social security numbers.

equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
    a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
    b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.
14. Web universal resource locators (URLs).
15. Internet protocol (IP) address numbers.
16. Biometric identifiers, including fingerprints and voiceprints.
17. Full-face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

Covered entities may also use statistical methods to establish de-identification instead of removing all 18 identifiers. The covered entity may obtain certification by "a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" that there is a "very small" risk that the information could be used by the recipient to identify the individual who is the subject of the information, alone or in combination with other reasonably available information. The person certifying statistical de-identification must document the methods used as well as the result of the analysis that justifies the determination. A covered entity is required to keep such certification, in written or electronic format, for at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.

Under the first method, unique identifying numbers, characteristics, or codes must be removed if the health information is to be considered de-identified. However, the Privacy Rule permits a covered entity to assign to, and retain with, the health information a code or other means of record identification if that code is not derived from or related to the information about the individual and could not be translated to identify the individual. The covered entity may not use or disclose the code or other means of record identification for any other purpose and may not disclose its method of re-identifying the information. For example, a randomly assigned code that permits re-identification through a secured key to that code would not make the information to which it is assigned PHI, because a random code would not be derived from or related to information about the individual and because the key to that code is secure.

A covered entity is permitted to de-identify PHI or engage a business associate to de-identify PHI. For example, a researcher may be a covered entity him/herself performing, or may be hired as a business associate to perform, the de-identification. In most cases, the covered entity must have a written contract with the business associate containing the provisions required by the Privacy Rule before it provides PHI to the business associate. In addition, a covered entity, if a hybrid entity, could designate in its health care component(s) portions of the entity that conduct business associate-like functions, such as de-identification.

Partners policy on
De-identification of Data

De-identifying PHI according to Privacy Rule standards may enable many research activities; however, the Privacy Rule recognizes that researchers may need access to and generate identifiable health information during the course of research. Where PHI is needed for research activities, the Privacy Rule permits its use and disclosure if certain standards are met. These standards are discussed in the following sections.

Authorization for Research Uses and Disclosures

One way the Privacy Rule protects the privacy of PHI is by generally giving individuals the opportunity to agree to the uses and disclosures of their PHI by signing an Authorization form for uses and disclosures not otherwise permitted by the Rule. The Privacy Rule establishes the right of an individual, such as a research subject, to authorize a covered entity to use and disclose his/her PHI for research purposes. This requirement is in addition to the informed consent to participate in research required under the HHS Protection of Human Subjects Regulations and other applicable Federal and State law.

Area of Distinction	HIPAA Privacy Rule	HHS Protection of Human Subjects Regulations Title 45 CFR Part 46	FDA Protection of Human Subjects Regulations Title 21 CFR Parts 50 and 56
Permissions for Research	Authorization	Informed Consent	Informed Consent
IRB/Privacy Board Responsibilities	Requires the covered entity to obtain Authorization for research use or disclosure of PHI unless a regulatory permission applies. Because of this, the IRB or Privacy Board would only see requests to waive or alter the Authorization requirement. In exercising Privacy Rule authority, the IRB or Privacy Board does not review the Authorization form.	The IRB must ensure that informed consent will be sought from, and documented for, each prospective subject or the subject's legally authorized representative, in accordance with, and to the extent required by, HHS regulations. If specified criteria are met, the IRB may waive the requirements for either obtaining informed consent or documenting informed consent. The IRB must review and approve the Authorization form if it is combined with the informed consent document. Privacy Boards have no authority under the HHS Protection of Human Subjects Regulations.	The IRB must ensure that informed consent will be sought from, and documented for, each prospective subject or the subject's legally authorized representative, in accordance with, and to the extent required by, FDA regulations. If specified criteria are met, the requirements for either obtaining informed consent or documenting informed consent may be waived. The IRB must review and approve the Authorization form if it is combined with the informed consent document. Privacy Boards have no authority under the FDA Protection of Human Subjects Regulations.

A valid Privacy Rule Authorization is an individual's signed permission that allows a covered entity to use or disclose the individual's PHI for the purposes, and to the recipient or recipients, as stated in the Authorization. When an Authorization is obtained for research purposes, the Privacy Rule requires that it pertain only to a specific research study, not to nonspecific research or to future, unspecified projects. The Privacy Rule considers the creation and maintenance of a research repository or database as a specific research activity, but the subsequent use or disclosure by a covered entity of information from the database for a specific research study will require separate Authorization unless the PHI use or disclosure is permitted without Authorization (discussed later in this section). If an Authorization for research is obtained, the actual uses and disclosures made must be consistent with what is stated in the Authorization. The signed Authorization must be retained by the covered entity for 6 years from the date of creation or the date it was last in effect, whichever is later.

An Authorization differs from an informed consent in that an Authorization focuses on privacy risks and states how, why, and to whom the PHI will be used and/or disclosed for research. An informed consent, on the other hand, provides research subjects with a description of the study and of its anticipated risks and/or benefits, and a description of how the confidentiality of records will be protected, among other things. An Authorization can be combined with an informed consent document or other permission to participate in research. Whether combined with an informed consent or separate, an Authorization must contain the following specific core elements and required statements stipulated in the Rule:

Authorization Core Elements:

- A description of the PHI to be used or disclosed, identifying the information in a specific and meaningful manner.
- The names or other specific identification of the person or persons (or class of persons) authorized to make the requested use or disclosure.
- The names or other specific identification of the person or persons (or class of persons) to whom the covered entity may make the requested use or disclosure.
- A description of each purpose of the requested use or disclosure.
- Authorization expiration date or expiration event that relates to the individual or to the purpose of the use or disclosure ("end of the research study" or "none" are permissible for research, including for the creation and maintenance of a research database or repository).
- Signature of the individual and date. If the individual's legally authorized representative signs the Authorization, a description of the representative's authority to act for the individual must also be provided.

Authorization Required Statements:

- A statement of the individual's right to revoke his/her Authorization and how to do so, and, if applicable, the exceptions to the right to revoke his/her Authorization or reference to the corresponding section of the covered entity's notice of privacy practices.
- Whether treatment, payment, enrollment, or eligibility of benefits can be conditioned on Authorization, including research-related treatment and consequences of refusing to sign the Authorization, if applicable.
- A statement of the potential risk that PHI will be re-disclosed by the recipient. This may be a general statement that the Privacy Rule may no longer protect health information disclosed to the recipient.

The Privacy Rule does not specify who may draft the Authorization, so a researcher could draft it regardless of whether the researcher is a covered entity. However, in order to have a Privacy Rule-compliant Authorization, it must be written in plain language and contain the core elements and required statements, and a signed copy must be provided to the individual signing it if the covered entity itself is

seeking the Authorization. The companion piece *Sample Authorization Language* contains language that illustrates the inclusion of core elements and required statements.

NOTE: If an Authorization permits disclosure of the individual's PHI to a person or organization that is not a covered entity or a business associate acting on behalf of a covered entity (such as a sponsor or funding source of the research), the Privacy Rule does not continue to protect the PHI disclosed to such entity. However, other applicable Federal and State laws between the disclosing covered entity and the PHI recipient may establish continuing protections for the disclosed information. Under the HHS Protection of Human Subjects Regulations or the FDA Protection of Human Subjects Regulations, an IRB may impose further restrictions on the use or disclosure of research information to protect subjects.

An Authorization for research uses and disclosures need not have a fixed expiration date or state a specific expiration event; the form can list "none" or "the end of the research project." However, although an Authorization for research uses and disclosure need not expire, a research subject has the right to revoke, in writing, his/her Authorization at any time. The individual's revocation is effective, except to the extent that the covered entity has taken action in reliance upon the Authorization prior to revocation. For example, a covered entity is not required to retrieve information that it disclosed under a valid Authorization before learning of the revocation. And the preamble to the Privacy Rule states that, for research uses and disclosures, the reliance exception would permit the continued use and disclosure of PHI already obtained with an Authorization to the extent necessary to protect the integrity of the research—for example, to account for a subject's withdrawal from the research study, to conduct investigations of scientific misconduct, or to report adverse events.

Waiver or Alteration of the Authorization Requirement

Many health research projects and protocols cannot be undertaken using health information that has been de-identified. Also, it may not be feasible for a researcher to obtain a signed Authorization for all PHI the researcher needs to obtain for the research study. In other cases, a researcher may determine that consents obtained prior to April 14, 2003, that permit the use and disclosure of information obtained from research subjects are inadequate, insufficient, or restrict the research protocol or procedure such that an Authorization may be necessary to permit the PHI use or disclosure for the research.

To address these and other situations that may arise in the course of a research project or protocol, the Privacy Rule contains criteria for waiver or alterations of Authorizations by an IRB or another review body called a Privacy Board. Many of the provisions were modeled on the HHS Protection of Human Subjects Regulations. The Privacy Rule does not change current requirements that specify when researchers must submit protocols to the IRB for review and approval, and obtain informed consent documents. The Privacy Rule adds to such requirements only when a researcher requests a waiver or an alteration of Authorization. If a covered entity has used or disclosed PHI for research with an IRB or Privacy Board approval of waiver or alteration of Authorization, documentation of that approval must be retained by the covered entity for 6 years from the date of its creation or the date it was last in effect, whichever is later.

For research uses and disclosures of PHI, an IRB or Privacy Board may approve a waiver or an alteration of the Authorization requirement in whole or in part. A complete waiver occurs when the IRB or Privacy Board determines that no Authorization will be required for a covered entity to use and disclose PHI for a particular research project. A partial waiver of Authorization occurs when an IRB or Privacy Board determines that a covered entity does not need Authorization for all PHI uses and disclosures for research purposes, such as disclosing PHI for research recruitment purposes. An IRB or Privacy Board may also approve a request that removes some PHI, but not all, or alters the requirements for an Authorization (an alteration).

The Privacy Rule does not alter IRB membership requirements, jurisdiction on matters concerning the protection of human subjects, or other procedural IRB matters. The Privacy Rule states that the required documentation must indicate that the IRB followed normal or expedited procedures in reviewing and

approving the waiver or alteration. Thus, an IRB's authority to act on waiver or alteration requests under the Privacy Rule is in addition to the other authorities derived from the HHS Protection of Human Subjects Regulations and other applicable statutes and regulations. The process and criteria for obtaining a waiver of Authorization under the Privacy Rule is similar to the process and criteria for waiving informed consent in the HHS Protection of Human Subjects Regulations. Additional information on the Privacy Rule and IRBs can be found in the companion piece entitled *Institutional Review Boards and the HIPAA Privacy Rule*.

Privacy Boards are new, alternative review boards authorized by the Privacy Rule to review requests for alteration or waiver of a research Authorization. If a covered entity is to use or disclose PHI on the basis of a waiver or an alteration of Authorization from a Privacy Board, the Board must be established in accordance with Section 164.512(i) of the Privacy Rule. These provisions state that:

- Members must have varying backgrounds and appropriate professional competencies as necessary to review the effect of the research protocol on individuals' privacy rights and related interests.
- Each Board must have at least one member who is not affiliated with the covered entity or with any entity conducting or sponsoring the research and who is not related to any person who is affiliated with such entities.
- Members may not have conflicts of interest regarding the projects they review.

Additional information on the Privacy Rule and Privacy Boards can be found in the companion piece entitled *Privacy Boards and the HIPAA Privacy Rule.*

Documentation of the waiver or alteration of Authorization must include a statement identifying the IRB or Privacy Board that made the approval and the date of approval. Among other things, the documentation must also include statements that the IRB or Privacy Board has determined that the waiver or alteration of Authorization, in whole or in part, satisfies the following criteria:

1. The use or disclosure of the PHI involves no more than minimal risk to the privacy of individuals based on, at least, the presence of the following elements:
    a. An adequate plan to protect health information identifiers from improper use and disclosure.
    b. An adequate plan to destroy identifiers at the earliest opportunity consistent with conduct of the research (absent a health or research justification for retaining them or a legal requirement to do so).
    c. Adequate written assurances that the PHI will not be reused or disclosed to (shared with) any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of the PHI would be permitted under the Privacy Rule.
2. The research could not practicably be conducted without the waiver or alteration.
3. The research could not practicably be conducted without access to and use of the PHI.

The Privacy Rule does not require an IRB or Privacy Board to review the form or content of the Authorization a researcher or covered entity intends to use, or the proposed uses and disclosures of PHI made according to an Authorization. Under the Privacy Rule, an IRB or Privacy Board need only review requests to waive or alter the Authorization requirement.

Many research projects take place at multiple sites and/or require the use and disclosure of PHI created or maintained by more than one covered entity (collectively, *multisite projects*). Often, different IRBs are involved in multisite project reviews. The same situation is expected to occur with Privacy Boards. In some circumstances, Privacy Boards and IRBs will coexist. Where these boards coexist, the Privacy Rule does *not* require approval of a waiver or an alteration of Authorization by both bodies because a covered

entity may rely on a waiver or an alteration of Authorization approved by any IRB or Privacy Board, without regard to the location of the approver.

HHS has stated (65 *Federal Register* 82692, December 28, 2000) that a covered entity's responsibility is to "obtain the documentation that *one* [emphasis added] IRB or privacy board has approved the alteration or waiver of Authorization." Consequently, the Privacy Rule allows a waiver or an alteration of Authorization obtained from a single IRB or Privacy Board to be used to obtain PHI in connection with a multisite project. However, HHS also recognizes that "covered entities may elect to require duplicate IRB or Privacy Board reviews before disclosing [PHI] to requesting researchers" (67 *Federal Register* 53232, August 14, 2002). While the Privacy Rule does not address potential splits between IRBs and Privacy Boards, HHS "strongly encourages researchers to notify IRBs and privacy boards of any prior IRB or privacy board review of a research protocol" (65 *Federal Register* 82692, December 28, 2000).

Area of Distinction	HIPAA Privacy Rule	HHS Protection of Human Subjects Regulations Title 45 CFR Part 46	FDA Protection of Human Subjects Regulations Title 21 CFR Parts 50 and 56
Review of Cooperative Research	Requests to waive or alter the Authorization requirement are reviewed and approved by an IRB or Privacy Board. The Privacy Rule permits a covered entity to reasonably rely on the determination of an IRB or Privacy Board, if the covered entity obtains appropriate documentation of such determination.	Each institution is responsible for safeguarding the rights and welfare of human subjects and for complying with the HHS Protection of Human Subjects Regulations. With the approval of HHS, an institution participating in a cooperative project may enter into a joint review arrangement, rely upon the review of another qualified IRB, or make similar arrangements for avoiding duplication of effort.	Cooperative research/multi-institutional studies may use joint review, reliance upon the review of another qualified IRB, or similar arrangements aimed at avoiding duplication of effort.
Waivers of Authorization or Informed Consent Requirements	Allows waiver or alteration of Authorization when IRB or Privacy Board deems the following criteria are met: (1) Use or disclosure involves no more than minimal risk to the privacy of individuals because of the presence of at least the following elements: (a) An adequate plan to protect health information identifiers from improper use or disclosure, (b) an adequate plan to destroy	Permits an IRB to waive some or all of the elements of informed consent, or to waive the requirement to obtain informed consent, provided the IRB finds and documents that (1) the research involves no more than minimal risk to the subjects; (2) the waiver or alteration will not adversely affect the rights and welfare of the subjects; (3) the research	Permits FDA to waive the IRB review requirement. Permits an IRB to approve a clinical investigation without subjects' informed consent in certain circumstances specified in 21 CFR 50.23 and 21 CFR 50.24. These include (1) circumstances in which immediate use of the test article is, in the investigator's opinion, required to preserve the

	identifiers at the earliest opportunity absent a health or research justification or legal requirement to retain them, and (c) adequate written assurances that the PHI will not be used or disclosed to a third party except as required by law, for authorized oversight of the research study, or for other research uses and disclosures permitted by the Privacy Rule; (2) research could not practicably be conducted without the waiver or alteration; and (3) research could not practicably be conducted without access to and use of PHI.	could not practicably be carried out without the waiver or alteration; and (4) whenever appropriate, the subjects will be provided with additional pertinent information after participation. Permits an IRB to waive the requirement for the investigator to obtain a signed consent for some or all of the subjects if it finds either (1) that the only record linking the subject and the research would be the consent document and the principal risk would be potential harm resulting from a breach of confidentiality; or (2) that the research presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context.	life of the subject, and time is not sufficient to obtain informed consent; (2) circumstances when the U.S. President may waive informed consent for military personnel for administration of an investigational product to members of the armed forces; and (3) circumstances involving emergency research.

Limited Data Set and Data Use Agreement

The Privacy Rule permits a covered entity, without obtaining an Authorization or documentation of a waiver or an alteration of Authorization, to use and disclose PHI included in a limited data set. A covered entity may use and disclose a limited data set for research activities conducted by itself, another covered entity, or a researcher who is not a covered entity if the disclosing covered entity and the limited data set recipient enter into a data use agreement. Limited data sets may be used or disclosed only for purposes of research, public health, or health care operations. Because limited data sets may contain identifiable information, they are still PHI.

Limited Data Set - Refers to PHI that excludes 16 categories of direct identifiers and may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's Authorization or a waiver or an alteration of Authorization for its use and disclosure, with a data use agreement.

Data Use Agreement - An agreement into which the covered entity enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected.

A limited data set is described as health information that excludes certain, listed direct identifiers (see below) but that may include city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers. The direct identifiers listed in the Privacy Rule's limited data set provisions apply both to information about the individual and to information about the individual's relatives,

employers, or household members. The following identifiers must be removed from health information if the data are 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. Electronic mail addresses.
6. Social security numbers.
7. Medical record numbers.
8. Health plan beneficiary numbers.
9. Account numbers.
10. Certificate/license numbers.
11. Vehicle identifiers and serial numbers, including license plate numbers.
12. Device identifiers and serial numbers.
13. Web universal resource locators (URLs).
14. Internet protocol (IP) address numbers.
15. Biometric identifiers, including fingerprints and voiceprints.
16. Full-face photographic images and any comparable images.

A data use agreement is the means by which covered entities obtain satisfactory assurances that the recipient of the limited data set will use or disclose the PHI in the data set only for specified purposes. Even if the person requesting a limited data set from a covered entity is an employee or otherwise a member of the covered entity's workforce, a written data use agreement meeting the Privacy Rule's requirements must be in place between the covered entity and the limited data set recipient.

The Privacy Rule requires a data use agreement to contain the following provisions:

- Specific permitted uses and disclosures of the limited data set by the recipient consistent with the purpose for which it was disclosed (a data use agreement cannot authorize the recipient to use or further disclose the information in a way that, if done by the covered entity, would violate the Privacy Rule).
- Identify who is permitted to use or receive the limited data set.
- Stipulations that the recipient will
    - Not use or disclose the information other than permitted by the agreement or otherwise required by law.
    - Use appropriate safeguards to prevent the use or disclosure of the information, except as provided for in the agreement, and require the recipient to report to the covered entity any uses or disclosures in violation of the agreement of which the recipient becomes aware.
    - Hold any agent of the recipient (including subcontractors) to the standards, restrictions, and conditions stated in the data use agreement with respect to the information.
    - Not identify the information or contact the individuals.

If a covered entity is the recipient of a limited data set and violates the data use agreement, it is deemed to have violated the Privacy Rule. If the covered entity providing the limited data set knows of a pattern of activity or practice by the recipient that constitutes a material breach or violation of the data use agreement, the covered entity must take reasonable steps to correct the inappropriate activity or practice. If the steps are not successful, the covered entity must discontinue disclosure of PHI to the recipient and notify HHS.

Section 164.512 of the Privacy Rule also establishes specific PHI uses and disclosures that a covered entity is permitted to make for research without an Authorization, a waiver or an alteration of Authorization, or a data use agreement. These limited activities are the use or disclosure of PHI preparatory to research and the use or disclosure of PHI pertaining to decedents for research.

Activities Preparatory to Research

For activities involved in preparing for research, covered entities may use or disclose PHI to a researcher without an individual's Authorization, a waiver or an alteration of Authorization, or a data use agreement. However, the covered entity must obtain from a researcher representations that (1) the use or disclosure is requested solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research, (2) the PHI will not be removed from the covered entity in the course of review, and (3) the PHI for which use or access is requested is necessary for the research. The covered entity may permit the researcher to make these representations in written or oral form.

According to HHS guidance on the Privacy Rule,

The preparatory to research provision permits covered entities to use or disclose protected health information for purposes preparatory to research, such as to aid study recruitment. However, the provision at 45 CFR 164.512(i)(1)(ii) does not permit the researcher to remove protected health information from the covered entity's site. *As such, a researcher who is an employee or a member of the covered entity's workforce could use protected health information to contact prospective research subjects* [emphasis added]. The preparatory research provision would allow such a researcher to identify prospective research participants for purposes of seeking their Authorization to use or disclose protected health information for a research study.

Under the preparatory to research provision, a covered entity may permit a researcher who works for that covered entity to use PHI for purposes preparatory to research. A covered entity may also permit, as a disclosure of PHI, a researcher who is not a workforce member of that covered entity to review PHI (within that covered entity) for purposes preparatory to research. Within a hybrid entity, the situation is similar. A covered entity that is a hybrid entity may permit a researcher within its health care component to use, without an individual's Authorization, PHI for activities preparatory to research. A covered entity may also permit a researcher who is outside the hybrid entity's health care component to review PHI within that health care component without an individual's Authorization for purposes preparatory to research.

Researchers should note that any preparatory research activities involving human subjects research as defined by the HHS Protection of Human Subjects Regulations, which are not otherwise exempt, must be reviewed and approved by an IRB and must satisfy the informed consent requirements of HHS regulations.

Research on Decedents' Protected Health Information

To use or disclose PHI of the deceased for research, covered entities are not required to obtain Authorizations from the personal representative or next of kin, a waiver or an alteration of the Authorization, or a data use agreement. However, the covered entity must obtain from the researcher who is seeking access to decedents' PHI (1) oral or written representations that the use and disclosure is sought solely for research on the PHI of decedents, (2) oral or written representations that the PHI for which use or disclosure is sought is necessary for the research purposes, and (3) documentation, at the request of the covered entity, of the death of the individuals whose PHI is sought by the researchers.

Other Uses and Disclosures of Protected Health Information

Some of the PHI uses and disclosures that are permitted under the Privacy Rule at Section 164.512 without Authorization, waiver or alteration of Authorization, or data use agreement are summarized below. Covered entities seeking to use and disclose PHI for these or other purposes permitted under Section 164.512 should consult the Privacy Rule for information on the relevant implementation requirements.

Among other limited purposes, a covered entity may use or disclose PHI without an Authorization, as follows:

- To the extent the use or disclosure is required by law and complies with, and is limited to, the relevant requirements of such law. For example, a covered entity may disclose, without Authorization, PHI to cancer registries if the disclosure (or reporting) is required by law. In addition, a covered entity may disclose to the Federal Government, without Authorization, PHI associated with data first produced under a Federal award in accordance with 45 CFR 74.36[3] .
- For disclosure to a public health authority that is authorized by law to collect or receive the information for purposes of preventing or controlling disease, injury, or disability. Activities included here are reporting disease, injury, and vital events, such as birth or death, as well as conducting public health surveillance, investigations, and interventions. For example, a covered entity may disclose PHI, without Authorization, related to an adverse event to NIH or FDA as public health authorities. Additional guidance on the use and disclosure of PHI for public health purposes is available at: Centers for Disease Control and Prevention (2003). HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Services. *Morbidity and Mortality Weekly Report,* 52.
- To a person subject to the jurisdiction of the FDA with respect to an FDA-regulated product or activity for which that person has responsibility, for purposes related to the quality, safety, or effectiveness of the FDA-regulated product or activity (including, but not limited to, adverse event reporting; FDA-regulated product tracking; post-marketing surveillance; and enabling product recalls, repairs, replacements, or lookback). For example, a covered entity may disclose adverse event/safety reports to sponsors of investigational new products.
- To health oversight agencies for oversight activities authorized by law that are necessary, for example, for the appropriate oversight of government-regulated programs. For example, because Office for Human Research Protections (OHRP) is a health oversight agency under the Privacy Rule, a covered entity may disclose PHI, without Authorization, to OHRP for purposes of determining compliance with the HHS Protection of Human Subjects Regulations.

Minimum Necessary Restriction

With some exceptions, the Privacy Rule imposes a minimum necessary requirement on all permitted uses and disclosures of PHI by a covered entity. This means that a covered entity must apply policies and procedures, or criteria it has developed, to limit certain uses or disclosures of PHI, including those for research purposes, to "the information reasonably necessary to accomplish the purpose [of the sought or requested use or disclosure]." For uses and routine and recurring disclosures of and requests for PHI, the covered entity must develop policies and procedures (which may be standard protocols) to reasonably limit such uses, disclosures, and requests to the minimum necessary to achieve the purpose of the use or disclosure. For non-routine disclosures and requests, a covered entity must review each disclosure or request individually against criteria it has developed.

There are several exceptions to the minimum necessary requirements that may affect researchers (Sections 164.502(b) and 164.514(d) of the Privacy Rule). The minimum necessary standard does not apply to the following:

- Uses and disclosures made with an individual's Authorization.
- Disclosures to, or requests by, a health care provider for treatment.
- Disclosures to the individual.
- Uses or disclosures required by law.
- Disclosures to HHS for purposes of determining compliance with the Privacy Rule.

- When required for compliance with other HIPAA rules (e.g., to fill out required or situationally required data fields in standard transactions).

Unless otherwise excepted, covered entities are required to implement policies and procedures or establish criteria that limit the PHI used, disclosed, or requested to the minimum amount reasonably necessary to achieve the purposes (e.g., necessary for the specific research) for which disclosure is sought. These covered entity policies and procedures will apply to researchers who are members of the covered entity's workforce and may apply to business associates.

The Privacy Rule does not require a covered entity to independently determine, in all instances, whether a request for PHI meets the minimum necessary requirement. As relevant here, the Privacy Rule permits the covered entity to rely, when reasonable, on a request for disclosure of PHI as the minimum necessary when making permitted disclosures to public officials, disclosing information requested by another covered entity, or when disclosing PHI to researchers who have documentation of an IRB or Privacy Board waiver or alteration of Authorization or certain other representations permitted by the Privacy Rule, which are discussed in detail in related publications, *Institutional Review Boards and the HIPAA Privacy Rule* and *Privacy Boards and the HIPAA Privacy Rule*.

How Are Research Subjects' Rights Affected by the Privacy Rule?

Key Points:

- The Privacy Rule provides individuals with certain rights about how their health information is used and disclosed as well as how they can gain access to health records and information about when their PHI was released without their permission.
- The Privacy Rule describes how covered entities can implement these rights while maintaining the integrity of the research project.

In addition to establishing conditions for the use and disclosure of PHI, the Privacy Rule establishes certain rights of individuals with respect to their health information. Covered entities must provide individuals with written notice of the entity's privacy practices and the individual's privacy rights. In addition, the Rule permits individuals to gain access to, request amendment of, request restrictions on, and request confidential communication of certain records related to their health care. Individuals are also given the right to request and receive a written account from a covered entity of when and why their PHI has been disclosed without their Authorization, except under limited circumstances. Individuals also have the right to complain to the covered entity and to the Secretary of Health and Human Services if they believe a violation of the Privacy Rule has occurred. This document discusses an individual's rights to access PHI and receive an accounting of PHI disclosures.

Access to Protected Health Information

With few exceptions, the Privacy Rule guarantees individuals access to their medical records and other types of health information to the extent the information is maintained by the covered entity or its business associate within a designated record set. Research records maintained by a covered entity may be part of a designated record set if, for example, the records are medically related or are used to make decisions about research participants.

In most cases, patients or research subjects can have access to their health information in a designated record set at a convenient time and

Designated Record Set - A group of records maintained by or for a covered entity that includes (1) medical and billing records about individuals

place. One exception, among others, is during a clinical trial, when the individual's right of access can be suspended while the research is in progress if, in consenting to participate in research including treatment, the individual agreed to the temporary denial of access. The covered entity, however, must inform the individual that the right to access his/her health records in the designated record set will be restored upon conclusion of the clinical trial.

maintained by or for a covered health care provider; (2) 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.

Accounting of Disclosures of Protected Health Information

The Privacy Rule permits individuals to obtain a record of certain disclosures of their PHI by covered entities or their business associates, including certain disclosures made by researchers who must comply with the Rule. This is known as an accounting of disclosures. It is important to emphasize the difference between a use and a disclosure of PHI. In general, the use of PHI means communicating that information within the covered entity. A disclosure of PHI means communicating that information to a person or entity outside the covered entity, or the communication of PHI from a health care component to a non-health care component of a hybrid entity. The Privacy Rule restricts both uses and disclosures of PHI, but it requires an accounting only for certain PHI disclosures.

Upon receiving an individual's request, a covered entity must account for disclosures of that individual's PHI made on or after the covered entity's compliance date (for most entities, April 14, 2003), unless a particular disclosure or type of disclosure is excluded from this accounting requirement in Section 164.528(a) of the Privacy Rule. For example, an accounting is not needed when the PHI disclosure is made:

Accounting of Disclosures - Information that describes a covered entity's disclosures of PHI other than for treatment, payment, and health care operations; disclosures made with Authorization; and certain other limited disclosures. For those categories of disclosures that need to be in the accounting, the accounting must include disclosures that have occurred during the 6 years (or a shorter time period at the request of the individual) prior to the date of the request for an accounting. However, PHI disclosures made before the compliance date for a covered entity are not part of the accounting requirement.

Use - With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within the entity or health care component (for hybrid entities) that maintains such information.

Disclosure - The release, transfer, access to, or divulging of information in any other manner outside the entity holding the information.

- For treatment, payment, or health care operations.
- Under an Authorization for the disclosure.
- To an individual about himself or herself.
- As part of a limited data set under a data use agreement.
- Prior to the compliance date.

An individual's right to receive an accounting of disclosures (unless an exception applies) starts with the covered entity's compliance date and goes back 6 years from the date of the request, not including periods prior to the compliance date. A covered entity must therefore keep records of such PHI disclosures for 6 years.

The Privacy Rule allows three methods for accounting for research-related disclosures that are made without the individual's Authorization or other than a limited data set: (1) A standard approach, (2) a multiple-disclosures approach, and (3) an alternative for disclosures involving 50 or more individuals. Whatever approach is selected, the accounting is made in writing and provided to the requesting individual. Accounting reports to individuals may include results from more than one accounting method.

Standard Accounting

Standard accounting includes, for each disclosure, the following information:

- The date the disclosure was made.
- The name and, if known, address of the person or entity receiving the PHI.
- A brief description of the PHI disclosed.
- A brief statement of the reason for the disclosure.

Multiple Disclosures Accounting

Multiple disclosures accounting is permissible if the covered entity has made multiple disclosures of PHI to the same person or entity for a single purpose under Sections 164.502(a)(2)(ii) or 164.512 of the Privacy Rule. For each disclosure, the following must be included:

- The date the initial disclosure was made during the accounting period.
- The name and, if known, address of the person or entity receiving the PHI.
- A brief description of the PHI disclosed.
- A brief statement of the reason for the disclosure.
- The frequency, periodicity, or number of the disclosures made during the accounting period.
- The date of the last such disclosure during the accounting period.

Alternative Accounting

If a covered entity has made disclosures regarding 50 or more individuals for a particular research project under Section 164.512(i) of the Privacy Rule, the accounting may be limited to the following information:

- The name of the protocol or research activity.
- A plain-language description of the research protocol or activity, purpose of the research, and criteria for selecting particular records.
- A description of the type of PHI disclosed.
- The date or period of time during which the disclosure(s) occurred or may have occurred, including the date of the last disclosure during the accounting period.
- The name, address, and telephone number of the entity that sponsored the research and of the researcher who received the PHI.
- A statement that the individual's PHI may or may not have been disclosed for a particular protocol or research activity.

If the covered entity uses the alternative accounting method, it must, if requested to by the individual, assist the individual in contacting the research sponsor and the researcher. Such assistance, however, is limited to those situations in which there is a reasonable likelihood that the individual's PHI was actually disclosed for the research protocol or activity.

*Adapted from NIH Website