Clinical Research and the HIPAA Privacy Rule

Overview

Researchers who conduct interventional clinical research have questioned how the Privacy Rule will affect their research activities. Even before the Privacy Rule, of course, physician-investigators have been concerned about the privacy of the medical and research-related information of their patients and subjects. In fact, many have been required under the Department of Health and Human Services (HHS) or the Food and Drug Administration (FDA) Protection of Human Subjects Regulations (45 CFR part 46 or 21 CFR parts 50 and 56, respectively) to take measures to protect such personal health information from inappropriate use or disclosure.

Moreover, in clinical research, physician-investigators often stand in dual roles to the subject: As a treating physician and as a researcher. For the treating physician, duties of confidentiality have long been established under well-known legal and ethical standards. The Privacy Rule adds to these existing obligations. Where a covered entity conducts clinical research involving protected health information (PHI), physician-investigators need to understand the Privacy Rule's restrictions on the use and disclosure of PHI for research purposes. As the Federal privacy standards are implemented throughout the country, one benefit is that many clinical researchers and hospitals may adhere to a common set of national standards for protecting the privacy of patients and clinical research subjects.

This fact sheet discusses the Privacy Rule and its impact on covered entities that conduct clinical research. It places specific emphasis on the Authorization that is generally required for research uses and disclosures of PHI by covered entities. Additional information about the Privacy Rule's potential impact on other research activities, such as repositories, databases, 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*
- *Research Repositories, Databases, and the HIPAA Privacy Rule*
- *Institutional Review Boards and the HIPAA Privacy Rule*
- *Privacy Boards and the HIPAA Privacy Rule*

Introduction to the Privacy Rule

In response to a congressional mandate in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 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 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 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. In addition, it should be noted that the HHS and FDA's Protection of Human Subjects Regulations (45 CFR part 46 and 21 CFR parts 50 and 56, respectively) may also apply to clinical research.

Overview of the Privacy Rule's Impact on Clinical Research

PHI includes what physicians and other health care professionals typically regard as a patient's personal health information, such as information in a patient's medical chart or a patient's test results, as well as an individual's billing information for medical services rendered, when that information is held or transmitted by a covered entity. PHI also includes identifiable health information about subjects of clinical research gathered by a researcher who is a covered health care provider.

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

- If the subject of the PHI has granted specific written permission through an Authorization that satisfies section 164.508
- For reviews preparatory to research with representations obtained from the researcher that satisfy section 164.512(i)(1)(ii) of the Privacy Rule
- For research solely on decedents' information with certain representations and, if requested, documentation obtained from the researcher that satisfies section 164.512(i)(1)(iii) of the Privacy Rule
- If the covered entity receives appropriate documentation that an IRB or a Privacy Board has granted a waiver of the Authorization requirement that satisfies section 164.512(i)
- If the covered entity obtains documentation of an IRB or Privacy Board's alteration of the Authorization requirement as well as the altered Authorization from the individual
- If the PHI has been de-identified in accordance with the standards set by the Privacy Rule at section 164.514(a)-(c) (in which case, the health information is no longer PHI)
- 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, as specified under section 164.514(e)
- Under a "grandfathered" 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 research as specified under the transition provisions of the Privacy Rule at section 164.532(c)

Note that the Privacy Rule also permits covered entities to use and disclose PHI for purposes of treatment, payment, and health care operations without Authorization. The Privacy Rule also permits disclosures to business associates. Business associates are persons or entities that perform certain functions or services on behalf of the covered entity that require the use or disclosure of PHI, provided certain arrangements to safeguard the PHI are in place between the covered entity and the business associates. The Privacy Rule also permits, without Authorization, covered entities to make a number of other disclosures of PHI, including disclosures that are required by law, disclosures to public health authorities authorized by law to collect or receive such information for public health activities, and disclosures for adverse event reporting to certain persons subject to the jurisdiction of the FDA (e.g., clinical trial drug sponsors). (See section 164.512 for a description of other disclosures for which Authorization is not required.)

For a more detailed discussion of permitted uses or disclosures of PHI for research under the Privacy Rule, refer to *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule; Research Repositories, Databases, and the HIPAA Privacy Rule; Institutional Review Boards and the HIPAA Privacy Rule;* and *Privacy Boards and the HIPAA Privacy Rule.*

Authorization for PHI Uses and Disclosures

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 purpose(s) and to the recipient(s) 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 future, unspecified projects. If an Authorization for research is obtained, a covered entity's uses and disclosures must be consistent with what is stated in the Authorization.

An Authorization differs from an informed consent in that an Authorization is an individual's permission for a covered entity to use or disclose PHI for a certain purpose, such as a research study. An informed consent, on the other hand, is the individual's permission to participate in the research. An informed consent 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 specific core elements and required statements stipulated in the Privacy Rule. A related publication, *Sample Authorization Language*, demonstrates the inclusion of core elements and required statements for Authorizations.

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 Authorization and how to do so, and, if applicable, the exceptions to the right to revoke 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 and no longer protected by the Privacy Rule. This may be a general statement that the Privacy Rule may no longer protect health information disclosed to the recipient.

Limits on Using and Disclosing PHI if Authorization is Revoked

Although an Authorization for research uses and disclosures need not expire, a research subject has the right to revoke, in writing, Authorization at any time. The individual's revocation is effective when the covered entity receives the written revocation, except to the extent that the covered entity has taken action in reliance upon the Authorization. For example, a covered entity is not required to retrieve information that it disclosed under a valid Authorization before receiving the revocation. For research uses and disclosures, the reliance exception would permit the continued use and disclosure of PHI already obtained pursuant to the Authorization to the extent necessary to protect the integrity of the research—for example, to account for a subject's withdrawal from the research study, to conduct investigations of scientific misconduct, or to report adverse events.

Activities Preparatory to Research

Covered entities may permit researchers to review PHI in medical records or elsewhere during reviews preparatory to research. These reviews allow the researcher to determine, for example, whether there is a sufficient number or type of records 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 that the researcher seeks to use or access is necessary for the research purposes.

Additional information on activities preparatory to research can be found in the booklet, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*.

Identifying Research Participants

Under the "preparatory to research" provision, covered entities may use or disclose PHI to researchers to aid in study recruitment. The covered entity may allow a researcher, either within or outside the covered entity, to identify, but not contact, potential study participants under the "preparatory to research" provision. However, before permitting this activity, a covered entity must receive proper representation, as described above, from the researcher. Under the "preparatory to research" provision, no PHI may leave the covered entity.

Contacting Research Participants

Under the "preparatory to research" provision, covered entities may use and disclose PHI to researchers to aid in study recruitment. They may allow a researcher to identify, but not contact, potential study participants. To contact potential study participants, a researcher may do so, without Authorization from the individual, under the following circumstances:

- If the researcher is a workforce member of a covered entity, the researcher may contact the potential study participant, as part of the covered entity's health care operations, for the purposes of seeking Authorization. In addition, a covered health care provider may discuss treatment alternatives, which may include participating in a clinical trial, with the patient as part of the patient's treatment or the covered entity's health care operations. Alternatively, the covered entity may contract with a business associate—who may be a researcher—to assist in contacting individuals on behalf of the covered entity to obtain their Authorizations.
- If the covered entity obtains documentation that an IRB has partially waived the Authorization requirement to disclose PHI to a researcher for recruitment purposes, the covered entity could disclose to the researcher that PHI necessary for the researcher to contact the individual.

Research Uses and Disclosures Under Permissions Obtained Prior to the Privacy Rule's Compliance Date

Sections 164.532(a) and (c) of the Privacy Rule provide that, after the compliance date (for most covered entities, April 14, 2003), a covered entity may use or disclose an individual's PHI without an Authorization, or waiver or alteration of the Authorization requirement, in connection with research, if specific conditions are met. For many such uses and disclosures of PHI in connection with research, a covered entity may rely on any one of the following that was obtained prior to the 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 a new informed consent document is sought after the compliance date

The transition provisions do not apply if any change is made after the compliance date to an informed consent, express legal permission, or IRB waiver for the research obtained before the compliance date that would invalidate these prior permissions. In such cases, an Authorization that complies with section 164.508 of the Privacy Rule is required unless the activity is otherwise permitted by the Privacy Rule without Authorization (e.g., through a waiver of Authorization).

In some instances, express legal permissions, informed consents, or IRB-approved waivers of informed consents are not study specific. These permissions for research and waivers, if obtained before the compliance date, are grandfathered by the transition provisions even if provided for future unspecified research, subject to the conditions described above.

Frequently Asked Questions and Answers

Q: What is the relationship between the Privacy Rule and the HHS and FDA Protection of Human Subjects Regulations?

A: There are two main differences. First, the HHS and FDA Protection of Human Subjects Regulations are concerned with the risks associated with participation in research. These may include, but are not limited to, the risks associated with investigational products and the risks of experimental procedures or procedures performed for research purposes, and the confidentiality risks associated with the research. The Privacy Rule is concerned with the risk to the subject's privacy associated with the use and disclosure of the subject's PHI.

Second, the scope of the HHS and FDA Protection of Human Subjects Regulations differs from that of the Privacy Rule. The FDA regulations apply only to research over which the FDA has jurisdiction, primarily research involving investigational products. The HHS Protection of Human Subjects Regulations apply only to research that is conducted or supported by HHS, or conducted under an applicable Office for Human Research Protections (OHRP)-approved assurance where a research institution, through its Multiple Project Assurance (MPA) or Federal-Wide Assurance (FWA), has agreed voluntarily to follow the HHS Protection of Human Subjects Regulations for all human subjects research conducted by that institution regardless of the source of support. By contrast, the Privacy Rule applies to a covered entity's use or disclosure of PHI, including for any research purposes, regardless of funding or whether the research is regulated by the FDA.

Q: Under certain circumstances, the "preparatory to research" provision at section 164.512(i)(1)(ii) of the Privacy Rule permits covered entities to use or disclose PHI for purposes preparatory to research. What kinds of activities are considered preparatory to research?

A: Covered entities that obtain certain required representations from a researcher may use and disclose PHI for activities preparatory to research that include, but are not limited to, the following:

- Preparing a research protocol
- Assisting in the development of a research hypothesis
- Aiding in research recruitment, such as identifying prospective research participants who would meet the eligibility criteria for enrollment into a research study

Under this provision, no PHI may be removed from the covered entity during the course of the review.

Q: When do the requirements under HHS regulations at 45 CFR part 46 related to IRB review and informed consent apply to "preparatory to research" activities as permitted by the Privacy Rule at section 164.512(i)(1)(ii)?

A: HHS Protection of Human Subjects Regulations at 45 CFR part 46 do not reference "preparatory to research" activities.

HHS regulations at 45 CFR 46.102(d) define "research" as "a systematic investigation, including *research development*, testing and evaluation, designed to develop or contribute to generalizable knowledge." (Emphasis added.)

HHS regulations at 45 CFR 46.102(f) define "human subject" as

> a living individual about whom an investigator (whether professional or student) conducting research obtains (1) data through intervention or interaction with the individual or (2) identifiable private information.... *Private information* includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record). Private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator or associated with the information) in order for obtaining the information to constitute research involving human subjects.

When a "preparatory to research" activity (i) involves human subjects research, as defined above; (ii) is conducted or supported by HHS or conducted under an applicable OHRP-approved assurance; and (iii) does not meet the criteria for exemption under HHS regulations at 45 CFR 46.101(b), the research must be reviewed and approved by an IRB in accordance with HHS regulations at 45 CFR 46.109(a). In addition, informed consent of the subjects must be sought and documented in accordance with, and to the extent required by, HHS regulations at 45 CFR 46.116 and 46.117, respectively. However, under HHS Protection of Human Subjects Regulations at 45 CFR 46.116(c) and (d), an IRB may approve a consent procedure for such a "preparatory to research" activity that does not include, or that alters, some or all the elements of informed consent, or may waive the requirements to obtain informed consent for such a "preparatory to research" activity if certain criteria are satisfied.

The Privacy Rule permits, under section 164.512(i)(1)(ii), a covered entity to provide investigators with access to PHI for purposes preparatory to research, such as for purposes of identifying potential human subjects to aid in study recruitment, among other things. Such access is permitted provided that the covered entity receives certain required representations from the researcher and the researcher does not remove any PHI from the covered entity during the course of the review.

Activities in which an investigator obtains and records individually identifiable health information for purposes of identifying potential human subjects to aid in study recruitment, among other things, would involve human subjects research under the HHS regulations at 45 CFR part 46 and would not satisfy the criteria for any exemption under HHS regulations at 45 CFR 46.101(b). As a result, if such activities are conducted or supported by HHS or conducted under an applicable OHRP-approved assurance, the research activities must be reviewed and approved by an IRB in accordance with HHS regulations at 45 CFR 46.109(a). In addition, informed consent of the subjects, about whom identifiable private information (e.g., health information) is being obtained, must be sought and documented in accordance with, and to the extent required by, HHS regulations at 45 CFR 46.116 and 46.117, respectively.

For example, if an investigator who is covered by an applicable OHRP-approved assurance obtains and records identifiable private information from medical records for the purpose of contacting these individuals to determine if they would be interested in participating in a research study, this activity constitutes human subjects research and thus would require either (1) that subjects' informed consent be sought as required by the HHS regulations at 45 CFR 46.116, or (2) that the IRB approve an informed consent procedure that does not include or that alters

some or all the elements of informed consent, or waive the requirement to obtain informed consent in accordance with the provisions of the HHS regulations at 45 CFR 46.116(c) or (d). Informed consent also must be documented in accordance with, and to the extent required by, the HHS regulations at 45 CFR 46.117.

Similarly, if such an investigator obtains and records identifiable private information to develop a database of potential research subjects for future research studies, this activity is also human subjects research as defined in 45 CFR part 46 and thus must meet the requirements of the HHS regulations as discussed above.

The above interpretation does not conflict in any way with OCR's interpretation of the Privacy Rule. It should be noted that Authorization for use or disclosure of PHI provided for under the Privacy Rule and legally effective informed consent for research provided for under HHS regulations at 45 CFR 46.116 and 46.117 are not the same.

Furthermore, the Privacy Rule does not override any requirements of 45 CFR part 46, and vice versa. In situations where both 45 CFR part 46 and the Privacy Rule apply, institutions must adhere to both sets of regulations.

Q: If, under the "preparatory to research" provisions, a researcher identifies subjects that meet the study's eligibility criteria, how can the researcher contact the potential participant to obtain Authorization after identifying these individuals?

A: Under the "preparatory to research" provision, covered entities may use and disclose to researchers PHI to aid in study recruitment. They may allow a researcher to identify, but not contact, potential study participants. In order to contact potential study participants, a researcher may do so, without Authorization from the individual, under the following circumstances:

- If the researcher is a workforce member of a covered entity, the researcher may contact the potential study participant, as part of the covered entity's health care operations, for the purposes of seeking Authorization. Alternatively, the covered entity may contract with a researcher as a business associate to assist in contacting individuals on behalf of the covered entity to obtain their Authorizations.
- If the covered entity obtains documentation that an IRB has partially waived the Authorization requirement to disclose PHI to a researcher for recruitment purposes, the covered entity could disclose to the researcher that PHI necessary for the researcher to contact the individual.

Q: Is a covered entity required to account for disclosures made pursuant to an IRB or Privacy Board's alteration of the Authorization requirement?

A: Yes. Covered entities are required to account for disclosures made pursuant to an altered Authorization. Where an Authorization has been altered, pursuant to the process provided for by section 164.512(i) of the Privacy Rule, it is no longer an "authorization as provided in section 164.508" and thus, no longer exempt from the accounting requirements pursuant to section 164.528(a)(1)(iv). However, where a covered entity discloses the records of 50 or more individuals for a particular research purpose during the period covered by the accounting, the Privacy Rule permits the covered entity to provide a more general accounting to the requestor. See section 164.528(b)(4) of the Privacy Rule. The period covered by the accounting is no more than 6 years prior to the date on which the accounting is requested (or less than 6 years if requested by the individual) but does not include disclosures made prior to the compliance date—usually April 14, 2003.

Q: When must an IRB review and approve the language of an Authorization for use or disclosure of PHI related to human subjects research activities regulated by HHS Protection of Human Subjects Regulations at 45 CFR part 46 and FDA Protection of Human Subjects Regulations at 21 CFR parts 50 and 56?

A: The HHS and FDA Protection of Human Subjects Regulations do not expressly require that Privacy Rule Authorizations be reviewed or approved by an IRB. However, under HHS regulations at 45 CFR 46.117(a) and FDA regulations at 21 CFR 50.27(a), IRB review and approval is required for any document that contains the required informed consent document for human subjects research. Therefore, if the Authorization language is part of the informed consent document, such as when the Authorization form is combined with an informed consent form, the IRB is required to review such language.

Generally, neither HHS regulations at 45 CFR part 46 nor FDA regulations at 21 CFR parts 50 and 56 require that stand-alone Authorizations (i.e., Authorizations that are not incorporated into the informed consent document) for use or disclosure of PHI be reviewed and approved by the IRB. However, FDA regulations at 21 CFR 56.108(a) would require such review if required by the IRB's written procedures. In the exercise of ongoing enforcement discretion, however, with respect to the requirements of 21 CFR 56.108(a), to the extent that an IRB's written procedures require the review and/or approval of stand-alone Authorizations, FDA will not take enforcement action against an IRB for failing to review them even when the IRB's written procedures otherwise would require such review and/or approval.

The Privacy Rule does not require IRBs to review or approve Authorizations used for research or other disclosures; it only requires that the Authorization comply with the requirements of the Rule at section 164.508. For Office for Civil Rights (OCR) guidance on this topic, see *http://www.hhs.gov/ocr/hipaa/privguideresearch.pdf.*

Q: Does the Privacy Rule require IRBs to review and/or approve Authorizations, either as stand-alone documents (i.e., Authorizations that are not combined with informed consent documents) or when combined with informed consent?

A: No.

Q: Do FDA regulations require IRBs to review and/or approve stand-alone Authorizations, i.e., Authorizations that are not combined with informed consent documents?

A: No. FDA regulations do not specifically require IRBs to review and/or approve stand-alone Authorizations. However, FDA regulations governing IRBs require, in pertinent part, that IRBs adopt and follow written procedures for reviewing clinical research. See 21 CFR 56.108(a). Pursuant to this provision, IRBs that have written procedures requiring them to review all written materials provided to potential research subjects would have to review and approve stand-alone Authorizations, even though such review is not otherwise required under the Privacy Rule, HHS Protection of Human Subjects Regulations, or FDA regulations governing IRBs. However, in the exercise of ongoing enforcement discretion with respect to the requirements of 21 CFR 56.108(a), to the extent that an IRB's written procedures require the review and/or approval of stand-alone Authorizations, FDA will not take enforcement action against an IRB for failing to review them even when the IRB's written procedures otherwise would require such review and/or approval. For OCR guidance on this topic, see *http://www.hhs.gov/ocr/hipaa/privguideresearch.pdf.*

Q: Do international guidelines (the ICH Good Clinical Practice Guidelines) require IRBs to review and/or approve stand-alone Authorizations, i.e., Authorizations that are not combined with informed consent documents?

A: No. The International Conference on Harmonisation (ICH) Good Clinical Practice: Consolidated Guideline (E6) states, for example, "Before initiating a trial, the investigator/institution should have written and dated approval/favourable opinion from the IRB/IEC [Independent Ethics Committee] for the trial protocol, written informed consent form, consent form updates, subject recruitment procedures (e.g., advertisements), *and any other written information to be provided to*

subjects." (Emphasis added.) (See ICH E6 4.4.1.) This language recommends, but does not require, such review. In general, the ICH Good Clinical Practice guidelines are recommendations, not legal requirements. As such, they are not subject to enforcement by U.S. authorities.

Q: May a covered health care provider discuss with a patient his or her enrollment in clinical research without the patient's Authorization? What if the individual is not a patient of the covered provider?

A: Yes. These types of conversations may arise under a variety of circumstances. For example, a physician may for treatment purposes discuss treatment alternatives with the individual, which may include the option of enrolling in a clinical trial. In addition, a physician may speak to the individual about a clinical trial as part of asking the individual to sign an Authorization to permit the covered provider to use or disclose the individual's PHI for the research study. Also, the Privacy Rule generally permits a covered entity to communicate with individuals and to disclose their PHI to them. Therefore, covered health care providers and patients may continue to discuss the option of enrolling in a clinical trial without patient Authorization, regardless of whether the individual is a patient of the covered provider, and without an IRB or Privacy Board waiver of the Authorization. However, the covered health care provider must obtain the individual's Authorization or an IRB or Privacy Board waiver of Authorization, or meet certain other conditions, before using or disclosing the individual's PHI as part of the research study.

Similarly, if a physician knows of a study in which his or her patient might enroll that is being conducted by others, the physician may discuss such a trial with the patient and give the patient the researcher's contact information so the patient may contact the researcher directly. However, the physician may only contact the researchers about the patient so long as de-identified information is disclosed, the individual's Authorization or IRB or Privacy Board waiver of Authorization is obtained, or other conditions that satisfy the Privacy Rule are met. For example, it is acceptable to give a clinical summary of a patient to a researcher to determine if the patient might meet enrollment criteria, if such discussions omit the patient's name, address, medical record number, and any other identifying information set forth in section 164.514(a)-(c) of the Privacy Rule.

Q: May a covered entity obtain an individual's Authorization to include his or her PHI in a clinical research recruitment database of possible research participants, such as a pre-screening log?

A: Yes. The Privacy Rule permits a covered entity to include an individual's PHI in a clinical research recruitment database and permit researchers access to the recruitment database, provided the individual has given permission through a written Authorization. The Authorization must inform the individual of the purpose for which (e.g., for the pre-screening log for one or more clinical trials) and what PHI will be used and meet the other requirements at section 164.508 of the Privacy Rule. Alternatively, a covered entity may provide a researcher access to the PHI for reviews preparatory to research, provided the required representations are obtained. See section 164.512(i) of the Privacy Rule. Unless otherwise permitted by the Privacy Rule, a subsequent Authorization must be obtained from the individual before a covered entity may use or disclose the individual's PHI for the clinical trial itself.

Q: One common method for recruiting research participants involves organizing a call center for potential research participants to contact in response to advertisements about the research. Would a call center be required to obtain the individual's Authorization before speaking to the individual about the trial?

A: Call centers in many cases will not be part of a covered entity (health plan, health care clearinghouse, certain health care providers), and thus, are not required to comply with the

Privacy Rule. A call center for research is an entity established to receive and answer calls from interested individuals about a research project. Commonly, a call center will collect identifiable information about a caller who may be interested in the research study and then transmit such information to researchers involved in the study or send information about a study directly to callers.

If a call center is part of a covered entity, e.g., part of a covered health care provider that is also a researcher, it may speak with an individual without Authorization for purposes of communicating about the research study or obtaining the individual's Authorization to use or disclose his or her PHI for the study. However, any use or disclosure of the individual's PHI for the research study itself or other purposes is subject to the conditions set forth in the Privacy Rule.

Q: Is a covered health care provider that conducts clinical research required to provide the Notice of Privacy Practices to participants of that trial?

A: Maybe. The Privacy Rule requires covered health care providers that have a direct treatment relationship with the individuals to provide to individuals the Notice of Privacy Practices in accordance with section 164.520(c)(2). A direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship. An indirect treatment relationship between an individual and a health care provider is one in which:

- The health care provider delivers health care to the individual based on the orders of another health care provider.
- The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products to the individual.

Where a covered health care provider does not have a direct treatment relationship with the individual, the Privacy Rule does not require that provider to give to the individual the Notice of Privacy Practices. However, the covered provider is still responsible for making its Notice of Privacy Practices available to any person that requests it, and prominently posting and making available its Notice of Privacy Practices on any Web site it maintains that provides information about its customer services or benefits.

Q: How does the written Authorization required under the Privacy Rule differ from the written informed consent required under the HHS and FDA Protection of Human Subjects Regulations?

A: Under the Privacy Rule, a patient's Authorization is for the use and disclosure of PHI, which can include use or disclosure for research purposes. In contrast, an individual's informed consent, as required by the HHS or FDA Protection of Human Subjects Regulations, is a consent to participate in the research study as a whole, not simply a consent for the research use or disclosure of PHI. While there are important differences between the Privacy Rule's requirements for individual Authorization, and HHS or FDA's Protection of Human Subjects Regulations requirements for informed consent, the Privacy Rule's Authorization elements are compatible with the informed consent elements of the HHS Protection of Human Subjects Regulations. Thus, both sets of requirements can be met by use of a single, combined form, which is permitted by the Privacy Rule. For example, the Privacy Rule allows the Authorization for research to state that the Authorization will be valid until the conclusion of the research study, or to state that the Authorization will not have an expiration date or event. This is compatible with HHS' Protection of Human Subjects Regulations requirement for an explanation of the expected duration of the research subject's participation in the study. It should be noted that where the Privacy Rule, the HHS Protection of Human Subjects Regulations, and/or FDA's Protection of Human Subjects Regulations apply, each applicable regulation must will be followed.

Q: May the Authorization required under the Privacy Rule be part of the informed consent document required under the HHS and FDA Protection of Human Subjects Regulations?

A: Yes. The two documents may be combined, or they may be separate.

Q: If an Authorization to use or disclose PHI for research is combined with an informed consent form, does a covered entity need to obtain a signature authorizing the use or disclosure of PHI separately from a signature that may be required for informed consent under 45 CFR part 46 or 21 CFR parts 50 and 56?

A: No. Where an individual's signature is sought for a single form that combines Authorization with informed consent [also known as a compound Authorization at 164.508(b)(3)(i)], one signature satisfies the Authorization requirement at 164.508(c)(1)(vi).

Q: Do HHS regulations at 45 CFR part 46 and FDA regulations at 21 CFR parts 50 and 56 permit the IRB to review and approve the insertion of Authorization language as a single modification that applies to the informed consent documents of multiple protocols previously approved by the IRB?

A: Yes, when Authorizations for use or disclosure of PHI will be incorporated into previously approved informed consent documents for a series of protocols, and the Authorizations are composed entirely of identical template language, the IRB may approve the insertion of the Authorization language as a single modification that applies to the entire series of protocols.

However, when Authorizations for use or disclosure of PHI will be incorporated into previously approved informed consent documents for a series of protocols and the Authorization statements include protocol-specific information unique to each of the protocols, the IRB should review and approve the insertion of the Authorization language separately for each protocol.

In both cases, an expedited review procedure may be used.

Q: Do the core elements of an Authorization differ from a medical records release form?

A: Probably. A Privacy Rule Authorization may be a more detailed document than what physicians and hospitals are accustomed to using as a release of medical records. Medical records release forms usually are phrased very generally, but Authorizations are much more specific with regard to what information is being released, to whom, for what purpose, and for how long. An Authorization must also inform patients of certain rights they have in relation to their PHI. An Authorization may contain more information than required by the Privacy Rule, as long as the additional information is not inconsistent with the information required for the Authorization. See section 164.508 for the specific requirements for a Privacy Rule Authorization.

Q: Does the Authorization form need to have a termination date for research?

A: No. 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."

Q: Must a separate Authorization be obtained for each research use or disclosure of PHI?

A: No. As long as each use or disclosure is part of a specific research activity and the Authorization describes the types of uses or disclosures that will occur as part of that research activity, only one Authorization is required from each subject. That Authorization will generally be obtained at the time of enrollment in the trial itself, as part of the informed consent process. It is important, therefore, that researchers, research nurses, or others involved in informed consent discussions with subjects also

understand the Authorization and its meaning so that subjects' questions and concerns can be answered accurately.

Q: Does the Privacy Rule specify who must develop the Authorization form?

A: No. The Privacy Rule does not specify who may draft the Authorization, so a researcher could draft it. However, in order to comply with the Privacy Rule, an Authorization must be written in plain language and contain the core elements and required statements specified at section 164.508 of the Privacy Rule. A covered entity may disclose PHI as specified in a valid Authorization that has been created by another covered entity or a third party, such as a researcher.

Q: When a covered entity chooses to combine the Authorization with the informed consent document for a research study, can the compound document cross-reference required elements for both permissions (i.e., to minimize redundant language)?

A: Yes. The Privacy Rule permits the compound Authorization to cross-reference relevant sections of an informed consent document, provided the compound document includes the core elements and statements required by section 164.508(c). In addition, under the HHS and FDA Protection of Human Subjects Regulations, all the required elements for informed consent must be included in the informed consent document, unless an IRB alters or waives the requirements.

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. 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 public, including state, cancer registries). Covered entities may also de-identify PHI according to standards set forth in the Privacy Rule so that its use and disclosure is not protected by the Privacy Rule.

Q: What documentation of an IRB or Privacy Board waiver or alteration of the requirement for an Authorization must a covered entity receive in order to permit a use or disclosure of PHI for research without Authorization?

A: Under the Privacy Rule at section 164.512(i), a covered entity may use or disclose PHI for a research study without Authorization (or with an altered Authorization) from the research participant if the covered entity obtains proper documentation that an IRB or Privacy Board has granted a waiver (or alteration) of the Authorization requirements. Among other requirements under section 164.512(i), a covered entity must obtain a statement that an IRB or a Privacy Board has determined that the alteration or waiver, in whole or in part, of Authorization satisfies the following three criteria in the Privacy Rule:

1. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
   a) An adequate plan to protect the identifiers from improper use and disclosure
   b) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of research, unless there is health or research justification for retaining the identifiers or such retention is otherwise required by law
   c) Adequate written assurances that the PHI will not be reused or disclosed except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted by 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.

Clinical research will not generally qualify for a waiver of the Authorization if a clinical research participant will be asked to sign an informed consent before entering the study. We anticipate that waiver of Authorization will be more common in research that involves, for example, retrospective medical chart reviews. Additionally, when Authorization is waived for research access to medical records or other PHI, the covered entity must take reasonable steps to limit the information disclosed to that which is the minimum necessary for the research purpose. If appropriate documentation of an IRB or Privacy Board waiver or alteration of Authorization is presented to the covered entity, the covered entity may rely, if reliance is reasonable under the circumstances, upon documentation of such waiver that the request represents the minimum necessary amount of PHI for the research.

Q: Once an individual's information has been de-identified according to Privacy Rule standards, does the subject's Authorization have to be obtained for use or disclosure of that de-identified information for research?

A: No. De-identified information is not considered PHI and as such is not governed by the Privacy Rule, and no Authorization or waiver is necessary for its use or disclosure.

Q: Does a covered entity need an individual's Authorization before de-identifying the PHI or creating a limited data set?

A: No. The Privacy Rule does not require a covered entity to obtain an individual's

Authorization before using or disclosing the PHI for creating de-identified health information or a limited data set. The Privacy Rule considers such activity to be a health care operation, as defined at section 164.501, of the covered entity. As such, a covered entity could contract with a business associate, including a researcher, to create de-identified data or a limited data set.

Q: What kind of information must be removed from health information for it to be de-identified?

A: The Privacy Rule provides two ways to de-identify PHI. One way is to remove the following identifiers of the individual and of the individual's relatives, employers, or household members: (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; (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.

In addition to removing these identifiers, the covered entity must have no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual.

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.

Q: If a subject signed an informed consent to participate in clinical research prior to the Privacy Rule compliance date (April 14, 2003), does the researcher have to get the subject to sign an Authorization in order to use or disclose that subject's PHI after April 14, 2003?

A: No. Under the transition provisions of the Privacy Rule, as long as the informed consent was signed prior to April 14, 2003, the covered entity may use or disclose that subject's data, even if the data were not generated or received until after the compliance date, consistent with any agreed upon restriction on the use or disclosure of the information. However, the transition provision does not apply to the PHI of subjects enrolled after the compliance date (usually April 14, 2003). These subjects may have to complete an Authorization form, unless, for instance, an IRB or Privacy Board has approved a waiver of the Authorization requirement.

Q: If a use or disclosure could be made under the Privacy Rule as a research activity or another permitted activity, such as a permitted public health activity, does the use or disclosure have to satisfy both sets of requirements?

A: No. There may be cases where an activity may be permitted under more than one provision of the Privacy Rule, e.g., a disclosure for

public health and research, such as for adverse event reporting. In this case, disclosures may be made under either the research provisions or the public health provisions, as appropriate—the covered entity need not comply with both sets of requirements.

However, activities that are considered both public health and research under the Privacy Rule, and that also meet the definition of "research" as defined under the HHS Protection of Human Subjects Regulations, must be conducted in compliance with the HHS Protection of Human Subjects Regulations if the research is conducted or supported by HHS, or conducted under an applicable Assurance approved by the Office for Human Research Protections. Similarly, if an activity is both a public health and research activity that is subject to FDA's Protection of Human Subjects Regulations, then compliance with FDA's regulations would also be required.

Q: Would a covered entity be required to account for disclosures of PHI made pursuant to an informed consent or authorization for the research that was grandfathered under the transition provisions?

A: Yes, a covered entity would be required to account for such disclosures unless the consent or Authorization to participate in the research would constitute a valid Authorization under section 164.508 of the Privacy Rule.

Q: Does the Privacy Rule give subjects a right to access their research records during the course of a clinical trial?

A: The Privacy Rule does afford subjects and patients a right to inspect and obtain a copy of their PHI held by covered entities in what is termed a "designated record set." A designated record set includes any record that is maintained by the covered entity or its business associate that is a medical, billing, enrollment, or payment record or other record that is used to make decisions about the subject of the information. It may be, in some cases, that research data would not be considered part of the designated record set if, for example, the research data is not used to make decisions about the individual and not part of the medical record. In that case, the individual would not have a right to access the data, but this should be examined on a case-by-case basis with institutional officials. In the case of research that includes treatment, including clinical trials, the Privacy Rule permits a covered entity to suspend the individuals' access rights until the end of the research study, provided the individual agreed to the suspension when consenting to participate in the research and was informed that right of access would be re-instated upon completion of the research. The Privacy Rule permits the covered entity to insert in the Authorization form a statement by which the subject agrees to the suspension of the right to access during the clinical trial and that informs the individual that the right to access will be reinstated upon completion of the research.

Covered entities are required to have policies and procedures for responding to access requests, and researchers that are workforce members of a covered entity may wish to coordinate any response to a subject's request with the medical records department, privacy officer, or legal counsel to ensure compliance with both the Privacy Rule and institutional policies.

Q: Does the Privacy Rule permit a researcher in a covered entity to make adverse event reports to the IRB during a research study, which includes visit dates, a subject's initials, and other identifying information?

A: The Privacy Rule permits PHI to be used or disclosed for adverse event reporting if the use or disclosure is, for example, (1) permitted by the individual's Authorization, (2) pursuant to a waiver or alteration of Authorization, (3) required by law, or (4) for permitted public health activities, which may include reports to persons who are subject to the jurisdiction of the FDA when the report concerns an FDA-regulated product for which the person has responsibility, e.g., sponsors or FDA-regulated IRBs. Where the Privacy Rule requires a covered entity to meet a minimum necessary

requirement, researchers should work with their IRB, institutional officials, and research sponsors to develop an adverse event reporting process that uses as few identifiers as possible. For example, consider coding adverse event reports to de-identify data, for example, by using study numbers unrelated to the participant's name and indicating relevant dates as "day X of the study." Also note that while an Authorization need not explicitly list each of the multitude of uses and disclosures of PHI that will comprise the research study (so long as the Authorization describes the purpose of the research study and persons or classes of persons to whom the information may be disclosed in a meaningful and specific manner), covered entities may nonetheless wish to include specific language about adverse event reporting, if relevant, in the Authorization to more fully inform the individual.

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: 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: Does the Privacy Rule apply to individually identifiable health information of non-U.S. citizens held or maintained by a covered entity?

A: Yes. All individually identifiable health information, including individually identifiable health information of non-U.S. citizens, is PHI when it is held by a covered entity, unless it is otherwise excepted from the definition of PHI at Section 164.501 of the Privacy Rule.

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.

NIH Publication Number 04-5495 February 2004