



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

- nance 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 require-

ments 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

