



# Privacy Boards and the HIPAA Privacy Rule

## Overview

The Privacy Rule, at 45 CFR parts 160 and 164, establishes a category of health information, defined as protected health information (PHI), that a covered entity may only use or disclose to others in certain circumstances and under certain conditions. In general, the Privacy Rule requires an individual to provide signed permission, known as an Authorization under section 164.508 of the Privacy Rule, before a covered entity can use or disclose the individual's PHI for research purposes. Under certain circumstances, however, the Privacy Rule permits a covered entity to use or disclose PHI for research without an individual's Authorization. One way a covered entity can use or disclose PHI for research without an Authorization is by obtaining proper documentation of a waiver of the Authorization requirement by an Institutional Review Board (IRB) or a new type of review body, a Privacy Board.

This fact sheet is limited to the Privacy Rule's requirements relating to a Privacy Board and approvals of research-related requests for Authorization waivers or alterations and how those requirements relate to the functioning of a Privacy Board. A separate fact sheet entitled *Institutional Review Boards and the HIPAA Privacy Rule* discusses the concurrent authority of IRBs established under the Privacy Rule to approve such waivers or alterations. Additional information about the Privacy Rule can be found in the booklet, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*.

For guidance on the Privacy Rule, see the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) Web site at <http://www.hhs.gov/ocr/hipaa/>. For guidance on the interpretation of HHS or the Food and Drug Administration (FDA) Protection of Human Subjects Regulations at 45 CFR part 46 or 21 CFR parts 50 and 56, respectively,

visit the Office for Human Research Protections (OHRP) Web site at <http://ohrp.osophs.dhhs.gov> or the FDA Web site at <http://www.fda.gov/oc/gcpl/>, respectively.

## 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 by 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, PHI, which may only be used or disclosed to others in certain circumstances or under certain conditions. PHI is a subset of what is termed individually identifiable health information and must be protected when it is created, received, maintained, or transmitted 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 also provide health care 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 new HIPAA privacy policies and procedures. A researcher who is not a covered entity or is not a workforce member of a covered entity may be indirectly affected by the Privacy Rule, if the researcher wants data from a covered entity for research.



## What Is a Privacy Board and What Is its Role Under the Privacy Rule?

### ***Privacy Board***

A Privacy Board is a review body that may be established to act upon requests for a waiver or an alteration of the Authorization requirement under the Privacy Rule for uses and disclosures of PHI for a particular research study. A Privacy Board may waive or alter all or part of the Authorization requirements for a specified research project or protocol. A covered entity may use and disclose PHI, without an Authorization, or with an altered Authorization, if it receives the proper documentation of approval of such alteration or waiver from a Privacy Board.

### ***Privacy Board Role***

The Privacy Rule provides that a Privacy Board may act upon requests for waivers and alterations of the Authorization requirement to permit covered entities to use and disclose PHI for research. Before a covered entity can use or disclose PHI for research under a waiver or an alteration of Authorization, it must obtain documentation of approval of the waiver or an alteration of the Authorization requirement by either a Privacy Board or an IRB. Privacy Boards, however, do not exercise any other powers or authority granted to IRBs under Federal laws relating to federally conducted or supported human subjects research and research involving products regulated by the Food and Drug Administration (FDA). Under the Privacy Rule, Privacy Boards are not involved in creating Authorization forms and do not monitor uses and disclosures of PHI made pursuant to an Authorization. A Privacy Board that meets the membership requirements of the Privacy Rule does not necessarily satisfy the IRB membership requirements of the HHS or FDA Protection of Human Subjects Regulations or the requirements of other Federal laws applicable to the related research.

## Waiver or Alteration of Authorization Requirements

For some types of research, it is impracticable for researchers to obtain written Authorization from research participants. To address this type of situation, the Privacy Rule contains criteria for approval of a waiver or alteration of the Authorization requirement by an IRB or a Privacy Board. Under the Privacy Rule, either board may waive or alter, in whole or in part, the Privacy Rule's Authorization requirements for the use and disclosure of PHI in connection with a particular research project.

A waiver in whole occurs when the Privacy Board determines that no Authorization will be required for a covered entity to use or disclose PHI for a particular research project because certain criteria set forth in the Privacy Rule have been met (see section 164.512(i) of the Privacy Rule). For example, if a study involved the use of PHI pertaining to numerous individuals where contact information is unknown, and it would be impracticable to conduct the research if Authorization were required, a Privacy Board could waive the Authorization requirements for research participants if the Privacy Board determined that all the Privacy Rule waiver criteria had been satisfied. If the Privacy Board approves such a waiver, the receipt of the requisite documentation of the approval permits a covered entity to use or disclose PHI in connection with a particular research project without Authorization. A partial waiver of the Authorization requirements of the Privacy Rule might be requested to allow a researcher to obtain PHI as necessary to recruit potential research subjects. For example, even if a Privacy Board does not waive the Authorization requirement for the entire research study, a Privacy Board may partially waive the Authorization requirement to permit a covered entity to disclose PHI to a researcher for the purposes of contacting and recruiting individuals into the study.

A Privacy Board may also approve a request that removes some, but not all, required

elements of an Authorization (an alteration). For example, a Privacy Board may approve the alteration of the Authorization to remove the element that describes each purpose of the requested use or disclosure where, for example, the identification of the specific research study would affect the results of the study. Before a covered entity could use or disclose PHI pursuant to the altered Authorization, however, it would need to receive documentation that a Privacy Board determined that all the Privacy Rule waiver criteria at section 164.512(i)(2)(ii) had been satisfied. Any subsequent use or disclosure of PHI by a covered entity for a different research study would require an additional Authorization, except as permitted without Authorization under section 164.512(i) (e.g., with a waiver of Authorization) or 164.514(e) (i.e., as a limited data set with a data use agreement).

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

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

## Composition of a Privacy Board for Approval Proceedings

### ***Privacy Board Composition***

The Privacy Rule requires that a Privacy Board consist of at least two members and meet the requirements at section 164.512(i)(1)(i)(B). The members must have varying backgrounds and appropriate professional competencies as necessary to review the effect of a research protocol on the individual's privacy rights and related interests. At least one member of a Privacy Board must be an independent member who is (1) not affiliated with the covered entity that will use or disclose the PHI in connection with the research project, (2) not affiliated with the entity conducting or sponsoring the research, and (3) not related to any person who is affiliated with the covered entity or the entities conducting or sponsoring the research. Furthermore, no Privacy Board member may participate in the review of any project if that person has a conflict of interest. The Privacy Rule permits a covered entity to rely on documentation of waiver or alteration approval from any qualified Privacy Board.

### ***Privacy Board Approval Proceedings***

A Privacy Board's review and action on requests for approval of a waiver or an alteration of the Privacy Rule's Authorization requirement may be conducted through either the normal review procedures (review by the convened Privacy Board) or, in certain cases (explained below), through expedited review procedures.

### ***Review by the Convened Privacy Board***

When a request for a waiver or an alteration of the Authorization requirement is considered by the convened Privacy Board, a majority of the board members must be present at the meeting,



including 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. In order for an approval of a waiver or an alteration of the Privacy Rule's Authorization requirement to be effective, it must be approved by a majority of the Privacy Board members present at the convened meeting. If a member of the Privacy Board has a conflicting interest with respect to the PHI use and disclosure for which a waiver or an alteration approval is being sought, that member may not participate in the review.

### ***Expedited Review***

A Privacy Board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of individuals who are the subject of the PHI for which the use or disclosure is being sought. If the Privacy Board chooses to use an expedited review procedure to act on the request, the review and approval may be carried out by the Privacy Board chair or by one or more Privacy Board members designated by the chair. A member with a conflicting interest may not participate in an expedited review.

## **Documentation of Authorization Waiver or Alteration Determinations**

Before a covered entity may use or disclose PHI for research based on a waiver or an alteration of Authorization by a Privacy Board, a covered entity must receive documentation showing:

- The identity of the approving Privacy Board
- The date of the waiver or alteration approval
- A statement that the Privacy Board has determined that all the specified criteria for a waiver or an alteration were met (see **Waiver or Alteration of the Authorization Requirements**)
- A brief description of the PHI for which use or access has been determined by the

Privacy Board to be necessary in connection with the specific research activity

- A statement that the waiver or alteration was reviewed and approved under either normal or expedited review procedures (see **Privacy Board Approval Proceedings**)
- The required signature of the Privacy Board chair or the chair's designee

As noted, the Privacy Board's documentation of its approval must describe the PHI for which use or access has been determined to be necessary for the research. This would include stating, for example, that the waiver was limited to only certain information in a patient's medical record, instead of the entire record. If a covered entity uses or discloses PHI based on a Privacy Board approval of a waiver or an alteration of the Authorization requirement, the covered entity must retain the Privacy Board's documentation on which it relied for at least 6 years from the date the waiver or alteration was obtained, or the date when it was last in effect, whichever is later.

## **Verification Requirements: Right to Rely**

In some circumstances, Privacy Boards and IRBs will coexist. Where these boards coexist, the Privacy Rule requires approval of a waiver or an alteration of Authorization by only one of them. Furthermore, a covered entity may use or disclose PHI based on a waiver or an alteration of Authorization approved by any Privacy Board or IRB, without regard to the location or affiliation of the Privacy Board or IRB. The Privacy Rule permits a covered entity reasonably to rely on a Privacy Board's or an IRB's documentation granting a waiver or alteration of the Authorization requirement so long as the documentation is proper. The documentation on which the covered entity relies must be in writing and meet the signature and other requirements discussed in the **Documentation of Authorization Waiver or Alteration Determinations** section.

A covered entity's ability reasonably to rely on documentation of an Authorization waiver or



alteration may be especially important for research projects taking place at multiple sites and/or requiring the use and disclosure of PHI created or maintained by more than one covered entity (collectively, multisite projects). Often, different Privacy Boards or IRBs are involved in multisite project reviews. For these situations, HHS has stated (65 *Federal Register* 82692, December 28, 2000) that a covered entity's responsibility is only to "obtain the documentation that one IRB or [P]rivacy [B]oard has approved the alteration or waiver of Authorization" [emphasis added]. Consequently, the Privacy Rule allows a waiver or an alteration of Authorization obtained from a single Privacy Board or IRB for obtaining PHI in connection with multisite projects. However, HHS also recognizes that "covered entities may elect to require Privacy Board or IRB reviews before disclosing [PHI] to requesting researchers" (67 *Federal Register* 53232, August 14, 2002). The Privacy Rule does not require entities to change their practices with respect to how they address potential splits between review boards. However, HHS "strongly encourages researchers to notify IRBs and [P]rivacy [B]oards of any prior IRB or [P]rivacy [B]oard review of a research protocol" (65 *Federal Register* 82692, December 28, 2000).

A covered entity must limit the use or disclosure of PHI for research that is based on documentation of an approved waiver or alteration of Authorization to the minimum necessary to accomplish the intended purpose of the particular research protocol or project (see section 164.502(b) of the Privacy Rule). Documentation supporting a Privacy Board's approval of a waiver or an alteration of Authorization must include a description of the PHI without access to and use of which the Privacy Board has determined the research could not practicably be conducted. If a Privacy Board has granted a waiver or an alteration of Authorization, a covered entity may rely, if such reliance is reasonable under the circumstances, on the Privacy Board's documentation to satisfy itself that the requested PHI use or disclosure is limited to the minimum necessary for the

stated research purpose (see section 164.514(d)(3)(iii) of the Privacy Rule). Such reliance is appropriate regardless of whether the documentation of waiver or alteration is obtained from an external Privacy Board or one that is associated with the covered entity relying on the documentation (see 67 *Federal Register* 53198, August 14, 2002).

## 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 ongoing research if specific conditions are met. For many such uses and disclosures of PHI in connection with ongoing research, a covered entity may rely on any one of the following that was obtained prior to the compliance date:

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

The transition provisions also 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. Under all of these circumstances, 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 they provide for future unspecified research, subject to the conditions described above.

## Frequently Asked Questions and Answers

**Q: How does the composition of Privacy Boards vary from that of IRBs?**

A. The HHS and FDA Protection of Human Subjects Regulations at 45 CFR 46.107 and 21 CFR 56.107, respectively, require, among other things, that IRBs have at least five members, with varying backgrounds, to promote complete and adequate review of research activities commonly conducted by the institution. The IRB must be sufficiently qualified through the experience and expertise of its members, and the diversity of members, including consideration of race, gender, and cultural backgrounds and sensitivity to such issues as community attitudes, to promote respect for its advice and counsel in safeguarding the rights and welfare of human subjects. The IRB must also ascertain the acceptability of proposed research in terms of institutional commitments and regulations, applicable law, and standards of professional conduct and practice. The IRB must also include at least one member whose primary concerns are in scientific areas, and at least one member whose primary concerns are in nonscientific areas. In addition, the IRB must include at least one member who is not otherwise affiliated with the institution and who is not part of the immediate family of a person affiliated with the institution.

The Privacy Rule, at section 164.512(i)(1)(i)(B), requires that a Privacy Board have members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests and include at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of these entities. In addition, a Privacy Board may not have any member participating in a review of any project in which the member has a conflict of interest.

Of note, covered entities may reasonably rely on documentation from an IRB that satisfies the membership requirements of the HHS or FDA Protection of Human Subjects Regulations in order to use or disclose PHI without Authorization, as permitted by the Privacy Rule at section 164.512(i)(1)(i).

**Q: How do the requirements regarding members with conflicting interests vary between the Privacy Boards under the Privacy Rule and IRBs under the HHS and FDA Protection of Human Subjects Regulations?**

A: The HHS and FDA Protection of Human Subjects Regulations at 45 CFR 46.107(e) and 21 CFR 56.107(e), respectively, prohibit an IRB member who has a conflicting interest from participating in an initial or continuing review or approval of research, except to provide information at the request of the IRB.

Similarly, the Privacy Rule, at section 164.512(i)(1)(i)(B)(3), prohibits a Privacy Board member from participating in a review of any project in which the member has a conflicting interest.

**Q: Who furnishes the description of the PHI for inclusion in the Privacy Board's documentation?**

A: The Privacy Rule does not state who furnishes the description of the PHI to be included in the Privacy Board's documentation. However, the researcher requesting the waiver or alteration of the Privacy Rule's Authorization requirement from the Privacy Board may be in the best position

to adequately describe the PHI to be used and disclosed and could submit this information as part of the request for such approval. Regardless of who provides the description of the PHI, the Privacy Board is the entity that decides whether or not, and the extent to which, a waiver or alteration of Authorization is granted, and, therefore, the Privacy Board makes the final decision regarding the description of the PHI to be included in the Privacy Board's documentation.

