Uncovering the Relationship between IRBs and the HIPAA Privacy Rule

by Kathy Gilles

More than 18 months after the HIPAA privacy rule compliance date, there is still one area that remains problematic for many covered entities—the use and disclosure of protected health information (PHI) for research purposes. One point of significant confusion is the relationship between the privacy rule, the common rule, and protection of human subjects regulations. This article aims to weed through the confusion and help readers uncover the basics of institutional review boards (IRBs) and get to the heart of achieving compliance.

Regulation of medical research activities is not new. Most biomedical and behavioral research conducted in the US is governed by either the federal policy for the protection of human subjects (also known as the common rule) or the Food and Drug Administration's protection of human subjects regulations. These regulations were intended to protect the rights, safety, and welfare of individuals who participate in research studies, but weren't specifically written as privacy regulations.

The privacy rule supplements these regulations by adding a layer of privacy protection for participants in research studies that involve a covered entity. Some researchers may not be subject to the privacy rule if they don't meet the definition of a covered entity. However, the privacy rule will indirectly impact any researcher employed by or attempting to access or obtain PHI from a covered entity.

IRB Fundamentals

The common rule requires that an IRB review and approve research that is subject to regulation by any federal department or agency. An IRB must be composed of at least five members with varying backgrounds, including 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, an IRB must include at least one member who is not affiliated with the institution. IRB members cannot participate in the review of any project in which they have a conflicting interest, except to provide information requested by the IRB.

The IRB review process is designed to ensure that there are adequate provisions to protect the rights and safety of research participants, including measures to maintain privacy and the confidentiality of data. The privacy rule doesn't change IRB membership or its jurisdiction over safety issues, but it does add new responsibility and authority to the IRB regarding the privacy rights of participants in research studies.

Distinguishing between Consent and Authorization

The difference between consent and authorization has been a point of confusion for covered entities. A key component of the common rule and FDA regulations is a requirement that researchers explain the risks and benefits of participation in a research study and obtain informed consent from the participant. Part of the IRB review and approval process is to ensure the consent is compliant with the common rule and FDA regulations. The privacy rule supplements this by requiring a covered entity to obtain signed authorization from individuals before it can use or disclose PHI for research purposes. The authorization can either be separate or combined with the consent. If it is combined, the IRB must review and approve it.

The privacy rule further expands the role of the IRB by granting it the authority to approve a waiver or alteration to the requirement to obtain authorization. Before an IRB can approve a waiver or alteration, it must first determine that use or disclosure of the PHI involves no more than minimal risk to the privacy of individuals based on the following elements:

- An adequate plan to protect health information identifiers from improper use and disclosure

- An adequate plan to destroy identifiers at the earliest opportunity consistent with conduct of the research (absent a health or research justification for retaining them or a legal requirement to do so)
- Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of the PHI would be permitted under the privacy rule
- The research could not practically be conducted without the waiver or alteration or without access to and use of the PHI

The privacy rule allows a covered entity to rely on a waiver or alteration of authorization by any IRB without regard to its location or affiliation. If a waiver or alteration of authorization is not sought or granted, then the covered entity must ensure that the participant has signed a written authorization that contains the core elements and statements required in the privacy rule in section 164.508.

Issues for Covered Entities to Consider

After working under the privacy laws for more than a year, covered entities have learned how to work with issues surrounding privacy and research. Here are some additional issues to consider.

- **Reshuffle your IRB**. Covered entities should look at the composition of their IRBs. Many IRBs, especially those at smaller, nonacademic covered entities, have not traditionally included members who are familiar with the privacy rule and, as a result, may rely too heavily on researchers to know and follow the requirements. The IRB may then inadvertently approve authorizations or waivers that do not meet the privacy rule requirements. Including your organization's privacy officer as either a voting or consulting member of your IRB can help educate the other IRB members and minimize the potential risk to your organization.
- **Review the risks**. As stated earlier, the privacy rule allows a covered entity to rely on IRB approval for a waiver or alteration to authorization regardless of its location or affiliation. However, reliance on external IRB approval may be risky if there isn't a good process for ensuring compliance with the privacy rule. Consult with your risk attorney to determine if you should require your own IRB review process before allowing the use or disclosure of your patients' PHI.
- **Confirm authorization**. IRBs are not required to review and approve authorizations unless they are combined with consent. However, since a covered entity cannot use or disclose PHI for research without either a valid authorization or a waiver, IRB approval of stand-alone authorizations should be included as part of the research approval process. Ensuring that the authorization contains the required components prior to the research study benefits everyone—the researcher, the covered entity, and the participant. If you don't, you run the risk of either inappropriately disclosing or using PHI or delaying the research study while valid authorizations are obtained from the participants.
- **Remove identifiers**. Researchers may use de-identified information for research purposes without restriction. However, the covered entity and its IRB must determine that the information has been appropriately de-identified using statistical verification or by removing all of the following identifiers: names, addresses (other than state), all elements of date except for year, telephone and fax numbers, e-mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate and license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, URLs, IP addresses, biometric identifiers, full-face photographic images, and any other unique identifying number, characteristic, or code unless permitted by the privacy rule for re-identification.
- **Use limited data sets**. An alternative is for a researcher to enter into a data use agreement with the covered entity to use a limited data set. Again, the covered entity and IRB must ensure that a valid data use agreement is in place and that certain direct identifiers are removed. Section 165.514 of the privacy rule has a complete description of the elements that must be removed in order to qualify as either de-identified or a limited data set.
- **Know your state laws**. Researchers and IRB members must be familiar with state laws that may provide stricter rights to privacy than HIPAA. For example, in Washington State, an authorization is not valid for healthcare received more than 90 days after signing, so the open-ended expiration date allowed under the privacy rule is not valid. Make sure your IRB includes someone who knows and understands your state's privacy laws.

The common rule, FDA regulations, and the HIPAA privacy rule are all very complex regulations. You can improve your compliance by including members with the appropriate expertise on your IRB. Most traditional IRBs already have members who are familiar with the common rule. The addition of your privacy officer to the IRB membership will provide your

organization with an additional level of expertise to protect the privacy of your patients and minimize the risk to your organization.

The privacy rule recognizes the importance of medical research and was not intended to hamper it. It does, however, define a framework for accessing important medical information in a way that provides better privacy protection for individuals who participate in research studies.

References

Food and Drug Administration (FDA), Department of Health and Human Services. "Protection of Human Subjects." Code of Federal Regulations, 2002. 21 CFR 50. Available online at www.fda.gov/oc/ohrt/irbs/appendixb.html.

FDA, Department of Health and Human Services. "Institutional Review Boards." Code of Federal Regulations, 2002. 21 CFR 560. Available online at www.fda.gov/oc/ohrt/irbs/appendixc.html.

National Institutes of Health (NIH), Department of Health and Human Services. "Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule," NIH publication number 03-5388. Available online at http://privacyruleandresearch.nih.gov/pr_02.asp.

NIH, Department of Health and Human Services. "Institutional Review Boards and the HIPAA Privacy Rule," NIH publication number 03-5428, 2002. Available online at http://privacyruleandresearch.nih.gov/irbandprivacyrule.asp.

Public Welfare, Department of Health and Human Services. "Protection of Human Subjects." Code of Federal Regulations, 2001. 45 CFR 46. Available online at www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm.

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR, Parts 160 and 164. *Federal Register* 67, no. 157 (2002): 58181–273.

Kathy Gilles *(kgilles@evergreenhealthcare.org) is the chief privacy officer for Evergreen Healthcare.*

Article citation:
Gilles, Kathy. "Uncovering the Relationship between IRBs and the HIPAA Privacy Rule." *Journal of AHIMA* 75, no.10 (Nov-Dec 2004): 48-49,52.