

A Primer of the HIPAA Privacy Rule for Practice-Based Researchers

Anne Victoria Neale, PhD, MPH, and Kendra L. Schwartz, MD, MSPH

Concerns with the privacy of personal health information have grown with increased use of electronic medical records and with the patient-centered philosophy that physician-patient relationships should rest on principles of respect, autonomy, and confidentiality. Practicing clinicians are aware that the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule^{1,2} set rigorous standards for the protection of personal information contained in patient medical records. The Privacy Rule also resulted in more restrictive standards on the research use of “protected health information” (PHI), which can reveal the identity of patients.

To protect patient privacy, “covered entities” (all health plans, health care “clearinghouses,” and health care providers) must obtain specific, written authorization from a patient to use or disclose PHI. Patients must also be notified about their right to restrict the use and disclosure of such information. Covered entities must make reasonable efforts to limit the health information disclosed to the minimum necessary to accomplish the intended purposes. Although these restrictions seem to block some common approaches for patient recruitment and data collection, the Privacy Rule does have several provisions for procedures and processes that allow researchers to access personal health information in the absence of individual consent.

Physicians participating in practice-based research should be aware of how the Privacy Rule limits the use and disclosure of PHI, as well as the current standards for the disclosure of PHI for research purposes. Medical office staff, practice partners, or rotating residents and students may have questions about their ability to support prac-

tice-based research while upholding HIPAA standards for the protection of patient health information. Physician researchers must keep up with the evolving requirements for the ethical conduct of research and its associated vocabulary.

Local Institutional Review Boards (IRB) have the authority to make determinations about whether the proposed procedures of research under their domain meet Privacy Rule requirements. Investigators knowledgeable of accepted interpretations of how the Privacy Rule applies to research are better able to develop strategies for patient recruitment, data collection, and data sharing that meet Privacy Rule standards. In addition, participating members of practice-based research (PBR) networks³ need to understand the specific nature of the research activities that are covered in IRB approval of PBR studies. To this end, we address some common questions about the research use of PHI, and present definitions and interpretations of selected Privacy Rule terms with particular meaning to the conduct of PBR.

Practice-Based Research and Compliance with the HIPAA Privacy Rule

Has the Privacy Rule Replaced the Federal Common Rule?

No. The Privacy Rule has not modified the well-known federal “Common Rule”⁴ that requires IRB approval for all research conducted under its purview. The Common Rule defines the boundaries between research and practice and establishes the eminence of 3 ethical principles in research: respect for persons, beneficence, and justice.⁵ The Common Rule set the ethical standard that all research subjects provide informed consent to participate in a research study. The local IRB has the authority to waive the requirement of informed consent if it decides that the proposed research involves “no more than minimal risk”; that the waiver “will not adversely affect the rights and welfare of subjects”;

Submitted, revised, 13 September 2004.

From the Department of Family Medicine, Wayne State University, Detroit, MI. Address correspondence to: Anne Victoria Neale, PhD, MPH, Department of Family Medicine, Wayne State University, 101 E. Alexandrine, Detroit, MI 48201 (e-mail: vneale@med.wayne.edu).

Table 1. Options for Conducting HIPAA-Compliant Practice-Based Research

-
- HIPAA authorization by individuals to use their protected health information (PHI)
 - De-identified dataset that contains no PHI
 - Limited dataset with data use agreement
 - IRB waiver of HIPAA authorization
-

that “the research could not practicably be conducted without the waiver”; and “whenever appropriate, the subjects will be provided with additional pertinent information after participation” (such as a treatment benefit).^{4,6,7}

The Privacy Rule regulates only the content and conditions of documentation that covered entities must obtain before using or disclosing PHI for research purposes.^{1,2,8} The HIPAA regulations also permit IRBs to grant waivers of patient authorization to use and/or disclose PHI in certain circumstances.^{6,8} However, local IRBs have the authority to interpret how the Privacy Rule applies to individual research studies, and they are known to vary in their interpretations of, and standards for, responsible conduct of research.^{7,9}

As a New PBR Network Member, I’m Asked to Provide Practice Characterization Data. Does the Privacy Rule Prohibit This?

No. A covered entity may give researchers access to medical records without IRB review or authorization by individual patients to prepare a research proposal.^{6,7} Thus, it is permitted to use personal health records to characterize your patient population if this is preliminary to an actual research study (eg, preliminary information about the patient population for a grant proposal). These data can be organized as either a limited or de-identified dataset and compiled in a summary table. However, the researcher must adhere to the following restrictions on “reviews preparatory for research”^{7,10}: (1) disclosure is sought solely to prepare a research protocol or for similar purposes; (2) no PHI is to be physically removed from the covered entity; and (3) the PHI is necessary to plan the research (Table 1).

May Researchers Do Direct Study Recruitment in the Clinical Practice Setting?

Yes. Researchers who are not part of the covered entity would be allowed to review PHI to identify potentially eligible research subjects if a “waiver of

individual authorization” was obtained from the IRB. Such waivers may permit the disclosure of contact information necessary to recruit potential participants into the study. Note that a Privacy Rule waiver does not eliminate the requirement that participants provide informed consent to participate in the study, as required by the Common Rule.⁷

The preparatory research provision also permits covered entities to disclose PHI to aid study recruitment.^{7,10} In this case, an employee or member of the covered entity’s workforce would be allowed to identify prospective research participants for purposes of seeking their authorization to use or disclose PHI for a research study. Clinician researchers and clinical staff are permitted to directly recruit their patients. It is also permitted for outside researchers to develop a “generic” recruitment letter for clinicians to sign and mail or hand to potential study participants. If the generic letter includes PHI (eg, name or address), the clinical staff must generate the letter.

Is It Permitted to Combine the Form for Patient Informed Consent (Required by the Common Rule), and the Patient Authorization to Use PHI (Required by the Privacy Rule) into a Single Consent/Authorization?

Yes. Although there are important differences between the Privacy Rule’s requirement for individual authorization for the research use or disclosure of PHI and the Common Rule’s requirement to consent to participate in a research study as a whole, “both sets of requirements can be met by use of a single, combined form, which is permitted by the Privacy Rule.”^{1,2,7,10} However, local IRBs have the authority to require separate forms.

Does the Privacy Rule Permit the Creation of a Research Database That Contains PHI?

Yes. The regulations permit researchers to access and use all PHI with patients’ authorization.^{1,2,8} If such patient authorization is not possible or “practicable,” researchers can apply to their IRB for a waiver of individual authorization, making sure to document that the specific waiver criteria are satisfied.^{1,2,7,8,10} Researchers who apply for a waiver are advised to thoroughly address the following concerns: (1) the use or disclosure of the PHI involves no more than minimal risk to the privacy

Table 2. The Privacy Rule Defines These as PHI Identifiers (6, 7)

-
- Names
 - Geographic subdivisions smaller than a state if it contains less than 20,000 people (the initial three digits of the zip code are allowed)
 - Dates: all elements of dates except year, and all ages over 89
 - Telephone numbers
 - Fax numbers
 - E-mail addresses
 - Social security numbers
 - Medical record numbers
 - Health plan beneficiary numbers
 - Account numbers
 - Certificate or license numbers
 - Vehicle identifiers and license plate numbers
 - Device identifiers and serial numbers
 - Internet URLs
 - Computer IP addresses
 - Biometric identifiers
 - Full-face photographs and comparable images
 - Any other unique identifying characteristic or code, except as permitted for re-identification
-

of the individual; (2) the research could not practicably be conducted without access to and use of the PHI; (3) only the “minimum necessary” information is requested and each data element is justified; (4) the research could not practicably be conducted without the waiver; and (5) there is an adequate plan to protect the identifiers from improper use and disclosure.

What Is the Difference between a “De-Identified” and a “Limited” Dataset?

A “de-identified dataset” excludes 18 specified identifiers (Table 2). A covered entity may de-identify PHI so that such information may be used and disclosed freely, without being subject to the Privacy Rule’s protections.¹¹ However, a de-identified dataset may contain a nominal linking code that could allow the covered entity to later re-identify that information.

A “limited dataset” excludes the same 18 defined “identifiers,” yet does not have to be fully de-identified. It allows for the retention of dates (birth, death, admission, discharge), and of limited geographic information. Thus, with a data use agreement, a limited dataset may be used or disclosed for purposes of research if it is stripped of most personal identifiers.⁷

Strategies to Professionalize PBR Networks

PBR networks (PBRNs) must be professional research organizations with high-quality research capability,¹² and researchers should be prepared to educate covered entities about the research-related provisions of the Privacy Rule.¹⁰ The following are potentially supportive strategies that PBRNs can pursue to position their studies to be favorably reviewed by IRBs.

- Provide university appointments as voluntary faculty for community-based PBRN physicians.⁹ With such formal affiliations, physician researchers may have legitimate standing within a covered entity.
- Ensure that clinical staff who will be involved in data collection or medical record review have completed training in the responsible conduct of research that includes both the Common Rule ethical principles and guidelines for the protection of human subjects, and the Privacy Rule restrictions on, and allowances for, the use of PHI.

The HIPAA Privacy Rule was not specifically designed to facilitate or limit medical research,⁶ and it does not directly regulate research.¹⁰ Compliance with the Privacy Rule can be achieved with the following strategies:

- I. Determine whether the research can be conducted with a limited or de-identified dataset.
 - A. The covered entity can provide the dataset or can authorize a third party “business associate” with permitted access to PHI to create limited and de-identified datasets.
 - B. In grant proposal budgets, include funding requests to cover expenses for the level of effort involved by the covered entity or its business associate to generate the dataset.¹⁰
- II. Implement a data use agreement between a covered entity and a researcher to create a limited dataset.
 - A. Researchers could either help the covered entity recruit a third-party business associate to create the limited dataset or could undertake the work themselves, with a business associate agreement.^{10,11}
 - B. Required elements of the business associate agreement include a statement of the pur-

pose of the agreement (including a description of the permitted uses of PHI), and the period of time for which it is in effect.^{7,8} Note that a business associate agreement is *not* required to disclose PHI to a researcher with a patient authorization or a waiver of authorization from an IRB.

- III. Seek a “waiver of individual authorization” from the IRB to collect personal health information that may include some PHI.
 - A. Waivers are appropriate for many studies, including some with a medical record review and abstraction methodology.
 - B. Be sure to address the waiver criteria in detail (see above).

Glossary of Selected HIPAA Privacy Rule Terms of Importance to Practice-Based Researchers

A **Business Associate** is a person or entity who, on behalf of a covered entity, performs a function involving the use or disclosure of individually identifiable health information, such as data analysis, utilization review, and quality assurance reviews.^{7,8}

- Business associates also may perform accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, where performing those services involves disclosure of individually identifiable health information to or by the covered entity.
- A member of a covered entity’s workforce is not one of its business associates.
- A researcher may set up a business associate agreement with a covered entity.
- Business associate agreements are not required for disclosures of PHI to researchers as long as the researcher has fulfilled other requirements of the Privacy Rule.

Data Use Agreements describe permitted uses and disclosure of PHI and prohibit re-identifying or using information to contact individuals.^{7,8}

- A data use agreement is not required for use within the covered entity; it is required for “disclosure” outside the covered entity.
- Limited datasets require a data use agreement.
- De-identified data do not require a data use agreement.

A **De-identified Dataset** contains no PHI, although it may have personal health information if it cannot be linked to an individual. There are 2 ways of de-identifying datasets so that the Privacy Rule will not apply^{1,2,7,10}:

- Remove the 18 specific identifiers (Table 2) that define PHI from the dataset (referred to as the “safe harbor method”);¹¹ or
- Obtain the expert opinion of a qualified statistician that the risk of identification of an individual by the use of PHI is very small.
 - ▶ Acceptable techniques include removing direct identifiers, reducing the number of variables on which a match might be made, and limiting the distribution of records through a data use agreement, in which the recipient agrees to limit who can use or receive the data.
 - ▶ The IRB will determine whether these criteria have been satisfied.
- **Protected Health Information (PHI)** is not actually health information; rather, it is information with any personal identifiers, including information about an individual or his or her relatives, household members, or employer that alone or in combination could identify an individual. If the information leads to a person’s identify, the Privacy Rule applies, and researchers may access the PHI with either:
 - ▶ Written permission (“HIPAA authorization”) obtained from the individuals; or
 - ▶ A waiver of the requirement for authorization from the IRB.

Research is a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.^{1,2,8} This includes the development of research repositories and databases for research.⁷ A covered entity may always use or disclose, for research purposes, health information that has been de-identified without regard to the Privacy Rule.⁸ Note that research differs from the “health care operations” of covered entities, which are exempt from the Privacy Rule, and may include “quality assurance and quality improvement, including outcomes evaluation and development of clinical guidelines.”¹⁰ (See Doezema and Hauswald¹³ for a

discussion of the distinction between quality improvement and research.)

References

1. Public Welfare: Subtitle A—Department of Health and Human Services, General Administrative Requirements, 45 C.F.R. Part 160; 2002 [cited 2004 Sep 9]. Available from: <http://www.hhs.gov/ocr/hipaa/finalreg.html>.
2. Public Welfare: Subtitle A—Department of Health and Human Services, Security and Privacy, 45 C.F.R. Part 164, Subparts A and E; 2002 [cited 2004 Sep 9]. Available from: <http://www.hhs.gov/ocr/hipaa/finalreg.html>.
3. Lindbloom EJ, Ewigman BG, Hickner JM. Practice-based research networks. The laboratories of primary care research. *Med Care* 2004;42 Suppl 4:III-45-9.
4. Public Welfare: Subtitle A—Department of Health and Human Services, Protection of Human Subjects, 45 C.F.R. Part 46, Subpart A; 1991 [cited 2004 Aug 13]. Available from: <http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm>.
5. The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont Report: ethical principles and guidelines for the protection of human subjects of research [monograph on the Internet]. Washington: Department of Health, Education, and Welfare; 1979 [cited 2004 Aug 13]. Available from: <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.htm>.
6. Standards for privacy of individually identifiable health information [monograph on the Internet]. Washington: Office of Civil Rights, Department of Health and Human Services; 2003 [cited 2004 Aug 26]. Available from: <http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf>.
7. Privacyruleandresearch.nih.gov [homepage on the Internet]. Washington (DC): National Institutes of Health, Department of Health and Human Services; c2001 [updated 2004 Aug 4; cited 2004 Aug 9]. Available from: <http://privacyruleandresearch.nih.gov>.
8. Annas GJ. Medical privacy and medical research—Judging the new federal regulations. *N Engl J Med* 2002;346:216-20.
9. Wolf LE, Croughan M, Lo B. The challenges of IRB review and human subjects protections in practice-based research. *Med Care* 2002;40:521-9.
10. Gunn PP, Fremont AM, Bottrell M, Shugarman LR, Galegher J, Bikson T. The Health Insurance Portability and Accountability Act Privacy Rule: a practical guide for researchers. *Med Care* 2004;42:321-7.
11. Office for Civil Rights, HHS. Standards for privacy of individually identifiable health information. Final rule. *Fed Regist* 2002;67:53181-273.
12. Smith LFP, Carter YH, Cox J. Accrediting research practices. *Br J Gen Pract* 1998;48:1464-5.
13. Doezema D, Hauswald M. Quality improvement or research: a distinction without a difference? *IRB* 2002;24(4):9-12.