The Health Insurance Portability and Accountability Act Privacy Rule

A Practical Guide for Researchers

Patrick P. Gunn, JD, Allen M. Fremont, MD, PhD,† Melissa Bottrell, MPH, PhD,‡§ Lisa R. Shugarman, PhD,† Jolene Galegher, PhD,‡ and Tora Bikson, PhD†*

Background: The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, intended to address potential threats to patient privacy posed by the computerization and standardization of medical records, provides a new floor level of federal protection for health information in all 50 states. In most cases, compliance with the Privacy Rule was required as of April 2003. Yet considerable confusion and concern remain about the Privacy Rule and the specific changes it requires in the way healthcare providers, health plans, and others use, maintain, and disclose health information. Researchers worry that the Privacy Rule could hinder their access to health information needed to conduct their research.

Objectives: In this article, we explain how the final version of the Privacy Rule governs disclosure of health information, assess implications of the Privacy Rule for research, and offer practical suggestions for researchers who require access to health information.

Conclusion: The Privacy Rule is fundamentally changing the way that healthcare providers, health plans, and others use, maintain, and disclose health information and the steps that researchers must take to obtain health data. The Privacy Rule requires researchers who seek access to identifiable health information to obtain written authorization from subjects, or, alternatively, to demonstrate that their research protocols meet certain Privacy Rule requirements that permit access without written authorization. To ensure continued access to data, researchers will need to work more closely than before with healthcare providers, health plans, and other institutions that generate and maintain health information.

Key Words: Health Insurance Portability and Accountability Act, confidentiality, health services research, informed consent, privacy

(*Med Care* 2004;42: 321–327)

From the *Cooley Godward LLP, San Francisco, California; †RAND, Santa Monica, California; ‡RAND, Washington, DC; and the §National Center for Ethics in Health Care (Veterans Health Administration), Seattle, Washington.

Reprints: Allen M. Fremont, MD, PhD, RAND Health, 1700 Main Street, Santa Monica, CA 90407. E-mail: fremont@rand.org.

ISSN: 0025-7079/04/4204-0321

DOI: 10.1097/01.mlr.0000119578.94846.f2

On August 14, 2002, the Department of Health and Human Services (DHHS) published final modifications to the Privacy Rule, a set of regulations safeguarding the privacy of health information.[1] Although the Privacy Rule does not directly regulate research, it does limit the ability of healthcare providers, health plans, and other institutions covered by the Privacy Rule (called Covered Entities) to use or disclose health information for research.

DHHS developed the Privacy Rule as part of its implementation of the Health Insurance Portability and Accountability Act (HIPAA), a complex statute intended, in part, to ensure the portability of health insurance.[2] Recognizing that advances in information technology and increased use and transfer of medical records in electronic form threatened medical privacy, Congress included a provision calling for regulations protecting the privacy of health information. Ultimately, DHHS was charged with developing those regulations.

DHHS published an initial version of the Privacy Rule for public comment in November 1999.[3] After several iterations prompted by extensive public criticism and comment, the current version was adopted. Full compliance with the Privacy Rule was required as of April 14, 2003, although small health plans have until April 14, 2004, to comply.[4]

The complexity of the Privacy Rule, along with serious penalties for violations, has generated considerable confusion and concern among researchers, who worry that the Privacy Rule could hinder their access to health information.[5] Although some recent publications, including a detailed analysis from the National Institutes of Health (NIH), consider research-related provisions of the Rule,[6–12] they do not focus specifically on the concerns of health services researchers or necessarily offer practical advice about applying those provisions.

This article explains the major features of the Privacy Rule and describes its implications for health services researchers. Its goals are to inform researchers about access to health information under the regulations, to describe project

management and cost issues, and to suggest practical strategies for conducting health services research in this regulatory environment.

KEY FEATURES OF THE PRIVACY RULE

The Privacy Rule limits the circumstances under which Covered Entities can use or disclose protected health information (PHI), requiring, with some exceptions, authorization from the patient to permit uses and disclosures of PHI for research.

Protected Health Information

In general, PHI is health information that is individually identifiable. "Health information" is defined as "any information, whether oral or recorded in any form or medium, that: 1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and 2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual."[13] "Individually identifiable" refers to information collected from an individual that identifies him or her or for which there is a "reasonable basis" to believe the information could be used to identify the individual.[13] The definition of PHI excludes individually identifiable health information contained in certain educational or employment records.[14]

Covered Entities and Researchers

The Privacy Rule regulates the use and disclosure of PHI by Covered Entities. Covered Entities are health plans (eg, health insurers), healthcare clearinghouses (entities that receive healthcare transactions from providers or others, translate the data into a form acceptable to the payor, and forward the processed transaction to payors and clearinghouses), and healthcare providers (eg, hospitals and physicians that transmit health information in connection with a specified transaction).[13]

The Privacy Rule's definition of Covered Entities does not include researchers. Also, researchers do not become Covered Entities merely by contracting with a Covered Entity to conduct research.[9] The Privacy Rule could, nevertheless, apply to researchers if they work at a Covered Entity such as a hospital or a health plan. Researchers could also be considered covered healthcare providers if they furnish health care to subjects as part of their research, like in a clinical trial. Some researchers could be covered because they work at hybrid institutions such as universities that provide health care as well as unrelated services. Whether researchers in these settings are covered depends on legal decisions by management and formal designations made to DHHS.[15]

Covered Entities that violate the Privacy Rule could face substantial civil and criminal penalties,[16] which could extend to individuals who act as Covered Entities (eg, physicians) or who are employed by a Covered Entity. The Privacy Rule allows Covered Entities to use and disclose PHI for treatment, payment, and healthcare operations. "Treatment" and "payment" have commonsense meanings, but the definition of "healthcare operations" is more complex. It refers to internal functions of the Covered Entity such as "conducting quality assurance and quality improvement, including outcomes evaluation and development of clinical guidelines," provided that the work is primarily intended to improve the operations of a specific organization rather than for research.[14] The Privacy Rule defines "research" as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge," a definition that could exclude quality assurance and quality improvement studies that are part of a larger project to produce generalizable results.[14]

Business Associates

The Privacy Rule recognizes that Covered Entities disclose PHI to third parties, which it calls "business associates," to assist in quality assurance, claims processing, utilization review, and billing.[13] Such disclosures can continue under the Privacy Rule, but Covered Entities must develop data safeguarding agreements called "business associate agreements." Researchers are not business associates; neither are business associate agreements required for disclosures of PHI to researchers as long as the researcher has fulfilled other requirements of the Privacy Rule.[17] Third parties such as business associates can deidentify health information, thus making PHI available for research. As the following discussion indicates, business associates are thus important actors in the post-Privacy Rule research environment.

Use and Disclosure of Deidentified Data or a Limited Dataset

The Privacy Rule treats deidentified health information differently than PHI. A Covered Entity generally cannot use or disclose PHI for research without authorization from the patient or a waiver of authorization approved by an Institutional Review Board (IRB) or a Privacy Board, a body that must meet requirements similar to, but somewhat less stringent than, traditional IRB requirements.[18] However, if the Covered Entity or a business associate first strips some or all of the identifying elements from the PHI, the resulting data could be used or disclosed without authorization.

The Privacy Rule recognizes 2 categories of data that could be disclosed without authorization. The first category, called a "limited dataset," was created with research purposes in mind. In a limited dataset, health information is stripped of 16 direct identifiers relating to the individual and his or her

relatives, household members, and employers.[19] A limited dataset *can* retain identifiers potentially useful for research, including age, date of birth and death, zip code (5 digits only), state, county, city, geocode, dates of admission and discharge, and other characteristics or codes not listed as direct identifiers (Fig. 1). Because inclusion of these identifiers poses a risk of identification by inference, the Privacy Rule permits use and disclosure of a limited dataset only for research, public health, or healthcare operations. To obtain access, the individual or organization seeking disclosure must enter into a "data use agreement." The required elements of a data use agreement include assurances that the researcher will safeguard the data and prevent unauthorized disclosure, refrain from identifying or contacting individuals, and report unauthorized use or disclosure to the Covered Entity.[19]

The second category of data that could be disclosed without authorization is truly deidentified data. A Covered Entity could use either of 2 methods to confirm that data are satisfactorily deidentified. Under the first route, a statistician, or other person with "appropriate training," must document that enough identifiers have been removed so that the risk that the information could be used to identify an individual, either by itself or in combination with other information, is very small.[20] The U.S. Office of Management and Budget's guidelines identify the "statistical and scientific principles" that should be applied to make such determinations.[21] For example, the guidelines warn that even if obvious identifiers are removed, subjects could be reidentified when sample sizes are small or the records contain unique characteristics (eg, patients with advanced age). To address the risk of reidentification, the guidelines suggest approaches such as recoding variables into fewer categories. The Privacy Rule also provides a second, more mechanical deidentification method, called the "safe harbor" approach, which requires that the Covered Entity (or a business associate operating at the behest of the Covered Entity) remove certain identifiers from the data (Fig. 2).[20]

Once the identifiers are removed, the health information is considered deidentified, provided that the Covered Entity has no knowledge that the information could be used alone or in combination to identify an individual. Covered Entities could assign a linking code to deidentify health information allowing them to later reidentify that information. Any code is acceptable, provided the code is not itself derived from individually identifying information (eg, scrambling the medical record number) and the Covered Entity does not disclose the code or mechanism for reidentification to the researcher.[22]

Authorization for Uses and Disclosures of Protected Health Information

The Privacy Rule takes the default position that Covered Entities are required to obtain authorization before using or disclosing a patient's PHI.[18] An authorization is a statement, signed and dated by the patient, granting permission to disclose his or her PHI. Although the Privacy Rule does not provide a specific form for authorizations, to be legally valid,

Identifiers that can be retained:

- All ages including age in months, days and/or hours
- Date of birth and death
- Date of admission and discharge
- Five digit zip code or any other geographic subdivision such as state, county, city precinct or their equivalent geocodes
- Other numbers, characteristics or codes not listed as direct identifiers

Identifiers that must be removed:

- Names
- Postal address information other than town and city, State and 5 or 9-digit Zip Code
- Telephone numbers
- Fax numbers
- E-mail addresses
- Web Universal Resource Locators (URLs)
- IP addresses
- Device identifiers and serial numbers
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle serial numbers, including license plate
- Biometric indicators such as finger or voice prints
- Full face photographic images

FIGURE 1. Identifiers that can and cannot be retained in a "Limited Data Set."

- Name
- Address (including all geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo-codes, except for the initial three digits of most zip codes)
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death
- All ages over 89 and all elements of dates (including year) indicative of age over 89, except that ages over 89 may be aggregated into a single category of "age 90 or older"
- Names of relatives
- Names of employers
- Telephone and fax number
- Social security number
- E-mail address
- Medical record number
- Health plan beneficiary number or account
- Certificate/license number
- Vehicle serial number
- URL or IP address
- Biometric indicators such as finger or voice prints
- Full face photographic images
- Any other uniquely identifying characteristic

FIGURE 2. Identifiers that must be removed under "Safe Harbor" method of deidentification.

an authorization must contain 6 "core elements" and 2 "required statements." It must also be written in plain language, and a signed copy must be provided to the individual (Fig. 3).[23]

Authorization should not be confused with informed consent. The Privacy Rule does not modify laws or regulations (such as the Common Rule) obligating researchers to disclose to subjects the rationale, risks, and benefits of the research project and to obtain informed consent.[24] Thus, if a research project involves a hospital chart review, the Common Rule would (absent an IRB waiver) require the researcher to obtain the subject's informed consent to participate in the project.[25] At the same time, the Privacy Rule would require the hospital to obtain a signed authorization from the patient before disclosing the patient's chart to the researcher. As a practical matter, researchers will need to obtain an authorization from the subject at the time of recruitment and pass that authorization on to the Covered Entity. To mitigate the burden of collecting multiple permissions, a researcher could combine the informed consent for research form with a Privacy Rule authorization to release PHI.[26]

Exceptions to and Waivers of the Authorization Requirement

The Privacy Rule specifies 4 situations in which Covered Entities could use or disclose PHI for research without first obtaining written authorization.

Core Elements

- Description of the PHI to be used or disclosed
- Identity of individuals or organizations who may disclose PHI
- Purpose of the use or disclosure
- Identity of person or organization to whom PHI may be disclosed
- Expiration date or event
- Signature (dated) of patient or guardian

Required Statements

- Statement that individual may revoke authorization in writing, along with a description of how to effect revocation, and any exceptions to revocation (or alternatively, a reference to Covered Entity's general privacy notice form containing such information)
- Statement advising individual whether Covered Entity will or will not condition treatment, payment, enrollment or eligibility for benefits on the individual's decision to sign the authorization,

Other General Provisions

- Must be written in plain language
- Signed copy of authorization must be provided to the individual

FIGURE 3. Authorizations: core elements and requirements.

First, PHI could be disclosed to researchers for "reviews preparatory for research." To obtain such access, the researcher must assure the Covered Entity that 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.[27] DHHS' Office of Civil Rights (OCR), the agency that enforces the Privacy Rule, has stated that researchers employed by Covered Entities might take advantage of this exception to recruit research subjects by identifying those with certain characteristics and contacting them to seek their authorization to release their PHI for research. However, researchers should note that some commentators and IRBs have disagreed with the OCR's interpretation of this provision, taking a more cautious approach. Moreover, researchers not employed by Covered Entities would not be permitted to recruit subjects in this manner, because the procedure would involve removing PHI from the site of the Covered Entity.[17] (Outside researchers could, however, request an IRB to waive the authorization requirement for the limited purpose of recruiting subjects.)

Second, PHI regarding a deceased person could be disclosed to a researcher without authorization from the decedent's representatives. To obtain such access, the researcher must assure the Covered Entity that the disclosure is sought solely for research involving the PHI of the decedent and that the requested PHI is necessary for the research.[28] The Covered Entity could also require the researcher to provide proof of death.

Third, PHI could be disclosed for research if an IRB or Privacy Board has waived the authorization requirement.[29] The IRB or Privacy Board must document that the circumstances of the research satisfy criteria (Fig. 4) similar, but not identical, to those now used by IRBs to waive the Common Rule requirement for informed consent for research participation.

DHHS expects the waiver procedure will most often be used to conduct records research when researchers are unable to use deidentified information and, when it is not practicable, to obtain authorization from research participants.[30] Research projects involving review of existing records probably fall into this category. The waiver procedure could also facilitate subject recruitment. An IRB or Privacy Board could partially waive the authorization requirement to enable researchers, including researchers not employed by the Covered Entity, to review PHI to identify prospective subjects.[17,31]

Fourth, the Privacy Rule includes transition provisions that "grandfather in" permissions for research obtained before the compliance date of April 14, 2003. Generally, a Covered Entity could use and disclose for research any PHI created or received before or after the compliance date, provided that, before the compliance date, the Covered Entity obtained permission from the subject to use or disclose the PHI for

- Use or disclosure of PHI involves no more than minimal risk to the subjects, as determined by:
  - An adequate plan to protect the identifiers from improper use and disclosure.
  - An adequate plan to destroy identifiers at the earliest opportunity, consistent with conduct of the research, unless there is a health, research, or legal justification for retaining them.
  - Adequate written assurances that PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected heath information would be permitted.
    - Research could not practicably be conducted without the waiver or alteration.
    - Research could not practicably be conducted without access to and use of the protected health information.[27]

FIGURE 4. Criteria for waiving the authorization requirement.

research, the subject gave informed consent to participate in the research, or an IRB waived the informed consent requirement. However, this transition provision is limited. If a waiver of informed consent was obtained before the compliance date, but informed consent is sought after the compliance date (ie, the subjects are reconsented as a result of a change in protocol), the Covered Entity must obtain a Privacy Rule-compliant authorization or demonstrate that some exception to the authorization requirement applies to permit use or disclosure of PHI for research.[32]

Relationship Between the Privacy Rule and Existing State Privacy Laws

Passage of the Privacy Rule does not mean that researchers can ignore existing state medical privacy laws. Congress and DHHS have made it clear that the Privacy Rule provides a new federal floor level of privacy protection. Put differently, the regulations provide new federal protection for medical information in states that afford lesser privacy protections and generally preempt state laws that are contrary to it.[33] However, where state law provides more protection than the Privacy Rule, state rules are not preempted.[34] Researchers should seek the advice of their IRB's attorneys as to how their research protocols relate to state privacy laws.

The Right of Patients to Access Their Protected Health Information

With few exceptions, the Privacy Rule requires Covered Entities to allow individuals to inspect and copy their medical records, to the extent those records are maintained with a defined group of documents called a "designated record set" (generally, the individual's treatment, billing, enrollment, and claims information). Research data kept by a Covered Entity could be part of a designated record set if, for example, the data are related to health or used by the Covered Entity to make decisions concerning treatment. This "right of access" has implications for researchers cooperating with healthcare providers in clinical trials, because individual patients could demand to inspect their PHI and discover facts about their treatment that might skew research results. To address this issue, the Privacy Rule permits a researcher to temporarily suspend an individual's access to PHI created in research that includes treatment while the research is in progress, provided that the individual agreed to the denial of access when giving his or her informed consent to participate in the research and the individual was informed that the right of access would be reinstated on completion of the research.[35] Thus, researchers who intend to suspend access to PHI during clinical trials will need to discuss this plan with potential subjects and ensure that their informed consent forms contain the relevant language.

PRACTICAL SUGGESTIONS AND IMPLICATIONS FOR RESEACHERS

Understanding the research-related provisions of the Privacy Rule means, primarily, understanding how they affect Covered Entities. To ensure continued access to health information, researchers need to work with Covered Entities as educators and facilitators.

As educators, researchers need to guide Covered Entities through what could appear to be a complicated maze of new regulations. As facilitators, researchers need to take specific actions to reduce the Covered Entities' cost of cooperation, in both time and dollars. This process should begin at the proposal stage. Some concrete suggestions are set forth subsequently.

Consider Use of Deidentified Health Information or a Limited Dataset

Researchers should consider from the outset whether their project requires PHI. If deidentified health information or health information in the form of a limited dataset would suffice, many Privacy Rule requirements, including the authorization requirement, can be avoided.

If deidentified health information or a limited dataset is acceptable, researchers can obtain the data directly from the Covered Entity. If the Covered Entity is unable or unwilling to undertake the work required to deliver the data in this form, researchers could locate and propose a business associate to undertake this work for the Covered Entity. The Privacy Rule also allows researchers to act as business associates of a Covered Entity to create a limited dataset.[36] This means that researchers seeking disclosure of data in the form of a limited dataset could either help the Covered Entity recruit a third-party business associate or could undertake the work themselves. The Privacy Rule is unhelpfully silent on

the issue of researchers performing data deidentification. It could be more expedient, however, for researchers to find business associates who are experienced in conducting these tasks. Of course, whether researchers or third parties carry out deidentification, there will be costs associated with the process. NIH has acknowledged that complying with the Privacy Rule will increase the cost of research and has encouraged investigators to include such costs in their budgets when applying for grants.[37]

If Protected Health Information Is Required, Work With Covered Entity to Develop Authorization Form

When research requires identifiable health information, the researcher must generally obtain informed consent under the Common Rule and authorization under the Privacy Rule from all subjects. Some Covered Entities have already developed Privacy Rule-compliant authorization forms. Researchers can profit from this work by consulting with the Covered Entity to see whether it has approved authorization language. However, researchers should be aware that the Privacy Rule permits authorizations for research to contain special provisions that might not be included in a Covered Entity's standard authorization form. As noted earlier, research authorizations could be combined with informed consent forms.[26] The Privacy Rule also recognizes that it could be undesirable (or simply impractical) to require researchers to specify the end date of research at the outset of a study and allows research authorizations to indicate "no expiration date."[38] A research authorization could also condition participation in a study involving treatment on the individual's signing the authorization form.[39] Covered Entities could be unfamiliar with these provisions, so researchers should be prepared to explain them if necessary. The final version of the authorization form should be vetted with the Covered Entity to ensure that the Covered Entity will agree to disclose PHI based on it, and, if the authorization is to be combined with informed consent, the form should also be discussed with the researcher's IRB and/or the Covered Entity's IRB.

If Obtaining Authorization Is Impractical, Consider Seeking an Institutional Review Board/Privacy Board Waiver

If the researcher determines that obtaining authorization from subjects would be impractical, the researcher should consider requesting a waiver of the authorization requirement from an IRB or Privacy Board. If qualifying circumstances exist, the researcher should document them, advise the Covered Entity, the Covered Entity's IRB/Privacy Board (assuming it has one), and the researcher's IRB of the intent to seek a waiver and allow time for these bodies to review the request.

Given the penalties for improper disclosures of PHI, researchers requesting waivers should also be prepared to address detailed questions from Covered Entities concerning their procedures for protecting the data they seek. Some Covered Entities could seek indemnity from researchers for improper disclosures of data and could demand insertion of indemnity provisions in data use agreements or confidentiality agreements. Researchers should seek the advice of legal counsel before entering into such agreements.

Be Familiar With Burdens the Privacy Rule Imposes on Covered Entities

The Privacy Rule's specifications regarding authorization are only a few of the obligations that the Rule imposes on Covered Entities. They must also comply with administrative requirements, at least 2 of which Covered Entities could regard as burdensome. One such requirement is the "accounting requirement," which gives patients the right to request that Covered Entities provide, on demand, a written accounting of any disclosures of PHI for purposes other than treatment, payment, or healthcare operations within the preceding 6-year period.[40] The accounting must inform the individual of the date of the disclosure, the name of the person who received the PHI, the nature of the information disclosed, and the purpose for which it was disclosed.[41] No accounting is required, however, for disclosures made pursuant to written authorizations, disclosures of deidentified health information, or disclosures of health information included in a limited dataset. For some research, a more limited accounting obligation could apply. When an IRB/Privacy Board has waived the authorization requirement and the research protocol involves PHI from more than 50 individuals, the Covered Entity is only required to provide a list of protocols for which the individual's data *might* have been used rather than a detailed account indicating that the individual's data *were* used for a specific protocol.[42] However, even when this exception applies, the Covered Entity is obligated to help the individual contact the researcher if it is reasonably likely that information was disclosed to the researcher.[43]

Researchers are not specifically required to maintain accounting information, but they could lessen the administrative burdens imposed on Covered Entities by the accounting requirement by maintaining on their behalf a research database of accounting information. There is at least 1 other reason for researchers to maintain some accounting information. As noted previously, in protocols involving disclosure of 50 or more records, Covered Entities are obligated to assist individuals who inquire to contact researchers who have received their information. Researchers who maintain some form of accounting information will be better positioned to respond to such inquiries.

The Privacy Rule also includes a "minimum necessary" requirement, which generally requires Covered Entities to limit disclosures of PHI to the minimum necessary to accomplish the intended purpose.[44] Thus, Covered Entities are

obligated to ensure that researchers who seek disclosure of PHI have demonstrated that it is required to conduct the research. The minimum necessary requirement applies to disclosures of health information included in a limited dataset and to disclosures of PHI for research under an IRB/Privacy Board-approved waiver. Researchers should be prepared to justify their requests for each data element.

CONCLUSION

The Privacy Rule has fundamentally changed the way that healthcare providers, health plans, and others use, maintain, and disclose health information. Although the Privacy Rule was not intended to preclude research access to health information, the complexity and administrative burdens associated with the Rule could hinder such access, particularly as Covered Entities learn about and adapt to the regulations. To help ensure continued data access, researchers need to understand how the Rule works and structure their research protocols accordingly. Researchers should be prepared to educate Covered Entities about the research-related provisions of the Privacy Rule and to facilitate disclosures of information by taking steps to reduce administrative burdens associated with compliance with the Rule.

ACKNOWLEDGMENTS

Work on this article was supported by RAND Health and RAND's Institutional Review Board. The opinions expressed here are those of the authors and do not necessarily represent the views of the sponsors or any affiliated institutions. The authors thank Robert Brook, Michael Greenberg, Jose Escarce, and Rick Eden for their helpful comments and suggestions on previous drafts of the paper.

REFERENCES

1. 67 Federal Register 53182 (August 14, 2002) (codified at 45 CFR § 160–164).
2. Health Insurance Portability and Accountability Act, P. L. 104–191, 110 Stat 2023 (1996).
3. 65 Federal Register 82462 (December 28, 2000).
4. 45 CFR § 164, 534.
5. Kaiser J. Researchers say rules are too restrictive. *Science*. 2001;294: 2070–2071.
6. Annas GJ. Medical privacy and medical research—judging the new federal regulations. *N Engl J Med*. 2002;346:216–220.
7. Barnes M, Kraus S. The effect of HIPAA on human subjects research. *BNA's Health Law Reporter*. 2001;10:1026–1041.
8. Barnes M, Gallin KE. Exempt research after the Privacy Rule. *IRB: Ethics & Hum Res*. 2003;25:5–6.
9. Department of Health and Human Services. Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule (NIH Publication #03–5388). Available at: http://privacyruleandresearch.nih-.gov/pdf/HIPAA_Booklet_4-14-2003.pdf. Accessed September 22, 2003.
10. Kulynych J, Korn D. The effect of the new federal medical-privacy rule on research. *N Engl J Med*. 2002;346:201–204.
11. Kulynych J, Korn D. The new federal medical-privacy rule. *N Engl J Med*. 2002;347:1133–1134.
12. Centers for Disease Control and Prevention. HIPAA Privacy Rule and public health: guidance from CDC and the US Department of Health and Human Services. *MMWR Morb Mortal Wkly Rep*. 2003;52:1–20.
13. 45 CFR § 160, 103.
14. 45 CFR § 164, 501.
15. Centers for Medicare and Medicaid Services. Covered Entity Decision Tools. 2003. Available at: http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp. Accessed February 27, 2003.
16. 42 USC §§ 1320d-5(a)(1), 1320d-6(b), 2000.
17. Department of Health and Human Services Office of Civil Rights. Medical privacy—National standards to protect the privacy of personal health information: OCR guidance explaining significant aspects of the Privacy Rule—December 4, 2002. Available at: http://www.hhs.gov/ocr/hipaa/privacy.html. Accessed December 15, 2002.
18. 45 CFR § 164, 508 (a).
19. 45 CFR § 164, 514 (e).
20. 45 CFR § 164, 514 (b).
21. Office of Management and Budget. Statistical Policy Working Paper 22: Report on Statistical Disclosure Limitation Methodology; 1994. Available at: http://www.fcsm.gov/working-papers/wp22.html. Accessed November 20, 2002.
22. 45 CFR § 514(c).
23. 45 CFR § 164, 508 (c).
24. 67 Federal Register 53230–53032, August 14, 2002.
25. 45 CFR § 46, 116.
26. 45 CFR § 164, 508 (b)(3)(i).
27. 45 CFR § 164, 512 (i)(1)(ii).
28. 45 CFR § 164, 512 (i)(1)(iii).
29. 45 CFR § 164, 512 (i)(1)(i).
30. 67 Federal Register 53229–53232, August 14, 2002.
31. 45 CFR § 164, 512 (i)(2)(i).
32. 45 CFR § 164, 532.
33. 45 CFR § 160, 201–205.
34. 45 CFR § 160, 203.
35. 45 CFR § 164, 524(a)(2)(iii).
36. 67 Federal Register 53237, August 14, 2002.
37. National Institutes on Health. Impact of the HIPAA Privacy Rule on NIH Processes Involving the Review, Funding, and Progress Monitoring of Grants, Cooperative Agreements and Research Contracts. 2003. Available at: http://grants1.nih.gov/grants/guide/notice-files/NOT-OD-03-025.html. Accessed March 4, 2003.
38. 45 CFR § 164, 508(c)(1)(v).
39. 45 CFR § 164, 508(b)(4)(i).
40. 45 CFR § 164, 528 (a).
41. 45 CFR § 164, 528 (b).
42. 45 CFR § 164, 508 (b)(4).
43. 67 Federal Register 53245, August 14, 2002.
44. 45 CFR § 164, 502 (b).