THE USE AND DISCLOSURE OF PROTECTED HEALTH
INFORMATION FOR RESEARCH UNDER THE HIPAA PRIVACY
RULE: UNREALIZED PATIENT AUTONOMY AND BURDENSONE
GOVERNMENT REGULATION

STACEY A. TOVINO†

I. INTRODUCTION

“Americans support both protecting the privacy of medical records and en-
couraging medical research.”1 With such varying attitudes towards the use and
disclosure of health information for research activities, it is not surprising that
the research provisions set forth in the federal privacy regulations (hereinafter,
the “Privacy Rule”) implementing the Administrative Simplification provisions
of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are
so controversial.

A hypothetical situation highlights the issue: A woman who has struggled
with infertility and depression sees a newspaper advertisement recruiting sub-
jects to participate in a clinical trial involving a new combined treatment for in-
fertility and depression. The woman is eager to participate in the trial, until she
is told that she must authorize the researchers to use and disclose all of her old
medical records (which detail her complex and, she believes, embarrassing
medical history), as well as all of the new records that will be created by the re-
searchers who will be documenting her response to the new medication. The
woman also is told that other recipients of her information will include addi-
tional research collaborators, the major pharmaceutical company that is sponsor-
ing the research and that contractually owns all of the patient information created
during the clinical trial, a local data coordinating center that will receive and
process all of the subjects’ information, the institutional review board that has
approved the research, as well as a regional data safety and monitoring board.
The woman is further told that if she does not wish to authorize the use and dis-
closure of her information, she is always free to join another similar clinical trial
in which an institutional review board has approved the waiver of her authorization.
The woman is conflicted. She wants to participate in the trial and receive
treatment for her physical and mental conditions, but she does not want to risk
the accidental disclosure of what she considers to be embarrassing health infor-
mation. The researchers genuinely want the woman to participate in their trial
because they believe their new combined therapy will bring hope to the thou-
sands of women who suffer from depression caused by infertility. The research-

† Research Professor, Health Law & Policy Institute, University of Houston Law Center. B.A.
1994, Tulane University; J.D. 1997, University of Houston Law Center; Ph.D. candidate, Institute for
Medical Humanities, University of Texas Medical Branch.
1. George J. Annas, Medical Privacy and Medical Research — Judging the New Federal Regula-
tions, 346 NEW ENG. J. MED. 216, 216 (Jan. 17, 2002).
ers also are excited about the funding they have received from the large pharmaceutical company that is sponsoring the research.

The preambles to the various proposed and final versions of the Privacy Rule, including the November 3, 1999, notice of proposed rulemaking (hereinafter, the “1999 Proposed Rule”),\(^2\) the December 28, 2000, final rule (hereinafter, the “2000 Final Rule”),\(^3\) the March 27, 2002, proposed modifications (hereinafter, the “2002 Proposed Modifications”),\(^4\) and the August 14, 2002, final modifications (hereinafter, the “2002 Final Modifications”),\(^5\) including the public comments that are documented in such preambles, highlight the public’s and the health care industry’s exceptional interest in, concern regarding, and conflicting attitudes toward the use and disclosure of health information in situations similar to that described in the preceding paragraph.\(^6\)

Before the general April 14, 2003, compliance date for the Privacy Rule,\(^7\) much of the human subjects research conducted in the United States was governed solely by either the federal Department of Health and Human Services (HHS) under the “Common Rule”\(^8\) or by the Food and Drug Administration

---

6. Indeed, in one study seeking the attitudes of 1,005 American adults, thirty-four percent felt the use of medical records to detect insurance fraud was “very acceptable,” while only eighteen percent felt the use of medical records for research purposes reached the same level of acceptability even if the identity of records were kept strictly confidential and it were not feasible to obtain advance permission for records use. Nancy E. Kass et al., The Use of Medical Records in Research: What Do Patients Want? 31 J.L. MED. & ETHICS 429, 429-430 (Fall 2003) (citing L. Harris, Equifax-Harris Consumer Privacy Survey, Study Number 638114, Oct. 8, 1996). On the other hand, of 214,000 patients from the Mayo Clinic who returned forms sent with appointment notices asking for consent to use and disclose their information for future research, “96 percent agreed to have their medical records accessible to Mayo Clinic researchers.” Id. at 430 (citing L.J. Melton, The Threat to Medical Records Research, 337 NEW ENG. J. MED. 1466-70 (1997)). “Similarly, all patients seen at the Olmstead Medical Center in Minnesota for two months in 1997 were asked to give general authorization to release their medical records for research. Of 15,997 patients, 91 percent granted authorization.” Id. (citation omitted). Finally, in a study conducted by Johns Hopkins of “602 persons with a serious genetic or other chronic medical condition (or family history of such condition),” thirty-one percent of the respondents agreed that medical researchers should be able to get their medical records without respondents’ permission “if it will help them to do research that will advance medical knowledge.” Id. at 430, 432. Interestingly, “those with incomes less than $20,000 were twice as likely to agree that researchers should be able to use records” without permission. Id. at 430.
7. See Dep’t of Health and Human Services Security and Privacy, 45 C.F.R. § 164.534 (2003). Most covered entities were required to comply with the Privacy Rule by April 14, 2003. Id. Small health plans (those health plans with less than $5M in annual receipts) have an additional year (until April 14, 2004) to comply. Id.
8. The Nuremberg Code, frequently referred to as one of the historical and philosophical bases for the ethical treatment of human subjects and the articulation of research standards as an international norm, was developed after the Nazi War Crimes Trials in 1949 to address permissible medical experiments. The text of the Nuremberg Code is available at http://ohsr.od.nih.gov/nuremberg.php3. Fifteen years later, in 1964, the World Medical Association affirmed the Nuremberg Code by adopting the “Ethical Principles for Medical Research Involving Human Subjects,” also known as the “Declaration of Helsinki.” The text of the Declaration of Helsinki is available at http://www.wma.net/e/policy/b3.htm. In the United States, the National Research Act, enacted on July 12, 1974, created the National Commis-
PROTECTED HEALTH INFORMATION UNDER HIPAA

(FDA) under its “Protection of Human Subjects” regulations. Although both the Common Rule and the Protection of Human Subjects regulations include some provisions designed to protect the privacy of human research subjects and the confidentiality of their information, the intent of HHS’ new Privacy Rule is to supplement these protections by requiring certain persons and organizations, referred to as “covered entities,” to implement specific measures to safeguard the confidentiality of individually identifiable health information.

This article offers a legal and ethical analysis of the Privacy Rule’s requirements relating to the use and disclosure of individually identifiable health information for research activities (hereinafter, the “research provisions”). Section II of this article provides a legal summary of the Privacy Rule’s complex research provisions. Sections III and IV of this article analyze the Privacy Rule’s research provisions from a legal and ethical perspective. Specifically,
Section III addresses whether the Privacy Rule promotes autonomy by analyzing certain of the legal rights attributed to individuals who are the subjects of health information including: (1) the general right\(^{13}\) of an individual to authorize (or refuse to authorize) a covered entity’s use or disclosure of health information for research activities; (2) the right of an individual to receive a notice of privacy practices, the purpose of which is to provide the individual with adequate notice of the uses and disclosures of health information that may be made by the covered entity, including uses and disclosures for research activities; and (3) the right of an individual to receive an accounting of health information disclosures made by the covered entity.

Section IV of this article addresses the Privacy Rule’s research provisions which permit, in certain situations, covered entities to use and disclose individually identifiable health information for research activities without patient authorization. Section IV analyzes the regulatory approaches chosen by HHS, including its decision to waive the requirement for patient authorization when: (1) an institutional review board or privacy board has approved the waiver of, or an alteration to, the otherwise required authorization; (2) the review of the information by the researcher is preparatory to, or in anticipation of, research; (3) the research involves decedents’ information; or (4) the covered entity is only using or disclosing a limited data set of information pursuant to a data use agreement for the research activity.

Finally, Section V of this article concludes that, although well-intended, the Privacy Rule’s research provisions establish onerous administrative requirements the burden of which may outweigh any autonomy that could be realized by the research subjects.

II. LEGAL SUMMARY OF THE HIPAA PRIVACY RULE

A. APPLICATION OF THE HIPAA PRIVACY RULE

The HIPAA Privacy Rule regulates the use and disclosure of certain individually identifiable health information (hereinafter referred to as “Protected Health Information” or “PHI”)\(^{14}\) by certain persons and organizations that fall within the definition of a “covered entity.” Covered entities include all health plans,\(^{15}\) all health care clearinghouses,\(^{16}\) and certain health care providers\(^{17}\) (i.e.,

---

\(^{13}\) As discussed in more detail in Sections II and IV, the right of an individual to authorize (or refuse to authorize) a covered entity’s use or disclosure of the individual’s health information for research activities is not absolute. In certain situations, the Privacy Rule’s research provisions permit a covered entity to use or disclose health information without the patient’s authorization. See discussion infra Parts II, IV.

\(^{14}\) 45 C.F.R. § 164.501 (generally defining protected health information as “individually identifiable health information,” and excluding from such definition: (i) education records protected by the federal Family Education Rights and Privacy Act (FERPA); (ii) certain student treatment records excepted from protection by FERPA; and (iii) employment records held by a covered entity in its role as an employer).

\(^{15}\) Dept’l of Health and Human Services, General Administrative Requirements, 45 C.F.R. § 160.103 (2003) (defining a health plan as “an individual or group plan that provides, or pays the cost of,
those health care providers who transmit any health information in electronic form in connection with certain standard transactions. 18 These standard transactions generally include: (1) claims for reimbursement and patient encounter information; (2) payment for health care services and remittance advice; (3) coordination of benefits; (4) health care claim status; (5) enrollment and disenrollment in a health plan; (6) eligibility for a health plan; (7) health plan premium payments; (8) referral certification and authorization; (9) first report of injury; and (10) health claims attachments. 19 All organizations satisfying the definition of a health plan or a health care clearinghouse constitute covered entities. However, only certain health care providers constitute covered entities – those providers who electronically transmit health information in connection with a claim for reimbursement or another one of the transactions listed in this paragraph.

Because the Privacy Rule does not apply to all health care providers but, instead, only “covered” health care providers, the Privacy Rule’s research provisions usually become implicated in one of two ways: (1) when a covered hospital or other covered health care provider discloses PHI to a researcher upon the researcher’s request; or (2) when a researcher who is a covered entity (e.g., a researcher who is providing treatment 20 as part of a clinical trial and who transmits health information in electronic form in connection with a claim for reimbursement for that treatment, or another standard transaction 21 wishes to use PHI in medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. § 300gg-91(a)(2))

16. Id. (defining a health care clearinghouse as a:
public or private entity, including a billing service, re-pricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.)

17. Id. (defining a health care provider as “a provider of services (as defined in section 1861(u) of the [Social Security] Act . . ., a provider of medical or health services (as defined in section 1861(s) of the [Social Security] Act . . ., and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.”)

18. Id. (defining a covered entity as: “(1) A health plan[;] (2) [a] health care clearinghouse[;] [or] (3) [a] health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.”)


20. 45 C.F.R. § 164.501 (defining treatment as the “provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.”)

21. For example, the Medicare Program routinely provides reimbursement for health care services provided as part of clinical trials. See generally INSTITUTE OF MEDICINE, EXTENDING MEDICARE REIMBURSEMENT IN CLINICAL TRIALS 33-4 (2000), available at http://books.nap.edu/catalog/9742.html (last visited November 10, 2003). Indeed, the Centers for Medicare and Medicaid Services (the agency formerly known as the Health Care Financing Administration or “HCFA”) has been covering costs associated with 96% of the investigational medical devices in clinical research since 1995. Id. at 34. If a researcher electronically submits a claim for reimbursement for an investigational medical device to the Medicare Program (the electronic submission of which is required by another set of regulations that implement the Administrative Simplification provision of the HIPAA statute), the researcher would constitute a covered entity. Id.
her possession to carry out research. In the first situation, the Privacy Rule’s research provisions regulate the covered entity’s disclosure of PHI to the researcher. In the second situation, the research provisions regulate the covered researcher’s use of PHI.

To the extent a covered entity is involved neither in the use nor the disclosure of PHI for research purposes, the Privacy Rule’s research provisions (or, for that matter, any provision in the Privacy Rule) would not regulate the research activity. HHS explained in a recent guidance document that:

It is important to understand that many research organizations that handle individually identifiable health information will not have to comply with the Privacy Rule because they will not be covered entities. The Privacy Rule will not directly regulate researchers who are engaged in research within organizations that are not covered entities even though they may gather, generate, access, and share protected health information. For instance, entities that sponsor health research or create and/or maintain

---

22. The preamble to the 1999 Proposed Rule explains that:

Under HIPAAA, we do not have the authority to regulate researchers unless the researcher is also acting as a provider, as in a clinical trial. We can only directly regulate health care providers, health plans, and health care clearinghouses. This means that for most research-related disclosures of health information, we can directly regulate the entities that disclose the information, but not the recipients of the information.

Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,968 (Nov. 3, 1999). The same preamble further explains that:

We understand that this approach involves imposing burdens on covered entities rather than on researchers. However, our jurisdiction under this statute leaves us the choice of taking this approach, or failing to provide any protection for individuals whose information is made the subject of research, or requiring individual authorization whenever a covered entity wants to disclose protected health information for research. This is not the approach we advocate for new federal privacy legislation, where we would propose that standards be applied directly to researchers, but it would be a useful and appropriate approach under the HIPAA legislative authority.

Id. The preamble to the 2000 Final Rule further explains that:

We clarify that, in general, a researcher is also a health care provider if the researcher provides health care to subjects in a clinical research study and otherwise meets the definition of “health care provider” under the rule. However, a health care provider is only a covered entity if that provider conducts standard transactions. Therefore we cannot apply any restrictions or requirements on a researcher in that person’s role as a researcher. However, if a researcher is also a health care provider that conducts standard transactions, that researcher/provider is subject to the rule with regard to its provider activities.

Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,575. Note that the quoted language refers only to a researcher/provider who conducts standard transactions on his or her own behalf. Id. The preamble further explains, however, that if the provision of health care services and the resulting standard transactions are conducted on behalf of something the preamble refers to as a “home institution,” then the home institution is the covered entity for purposes of the HIPAA Privacy Rule, and the researcher/provider is a workforce member, not a covered entity. However, since the Privacy Rule applies to both internal uses of PHI by workforce members, as well as external disclosures by a covered entity to a non-workforce member, any use of PHI by a researcher employed by a “home institution” as a workforce member also would trigger the research provisions contained in the HIPAA Privacy Rule. For a further discussion of the application of the HIPAA Privacy Rule to researchers, see generally DEPT’ OF HEALTH & HUMAN SERVS., PROTECTING PERSONAL HEALTH INFORMATION IN RESEARCH: UNDERSTANDING THE HIPAA PRIVACY RULE, NIH Pub. No. 03-5388 (2003).

23. See, e.g., Jennifer Kulyvych & David Korn, The Effect of the New Federal Medical-Privacy Rule on Research, 346 NEW ENG. J. MED. 201 (Jan. 17, 2002) (noting that although the Privacy Rule does not directly apply to researchers who are not covered entities, “the effective reach of the rule is much greater, since it dictates not only how covered entities may use medical information, but also how they may disclose it to third parties, including researchers”).
health information databases may not themselves be covered entities, and thus may not directly be subject to the Privacy Rule. However, researchers may rely on covered entities for research support or as sources of individually identifiable health information to be included in research repositories or research databases. The Privacy Rule may affect such independent researchers, as it will affect their relationships with covered entities.\textsuperscript{24}

B. Application to Both Uses and Disclosures of PHI

The Privacy Rule’s regulation of both uses and disclosures of PHI for research purposes is important. The Privacy Rule’s research provisions specifically state that “[e]xcept as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section.”\textsuperscript{25} Although members of the public who submitted comments following the publication of the 1999 Proposed Rule recommended that covered entities have fewer requirements for internal uses of PHI for research compared to disclosures of PHI to an external person or organization, HHS disagreed:

[W]e disagree that an individual’s privacy interest is of less concern when covered entities use protected health information for research purposes than when covered entities disclose protected health information for research purposes. Therefore, in the final rule, the research-related requirements . . . apply to both uses and disclosures of protected health information . . . .\textsuperscript{26}

Thus, if a covered hospital or other covered health care provider discloses PHI to a researcher upon the researcher’s request, the disclosure by the covered entity must be made in accordance with the Privacy Rule’s research provisions. Likewise, if a researcher who is a covered entity (e.g., a researcher who is providing treatment as part of a clinical trial and who transmits health information in electronic form in connection with a claim for reimbursement for that treatment, or another standard transaction) wishes to use PHI in her possession to carry out research, that use of information by the covered researcher also must be conducted in accordance with the Privacy Rule’s research provisions. The Privacy Rule’s application to both uses and disclosures of health information is different than many state laws, which typically regulate health care providers’ disclosures of information to a third party, but not the providers’ internal uses of the information.\textsuperscript{27}

\textsuperscript{24} \textsc{Dep't of Health & Human Servs., Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule 1}, NIH Pub. No. 03-5388 (2003).

\textsuperscript{25} 45 C.F.R. § 164.508(a)(1) (emphasis added).

\textsuperscript{26} Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,702.

\textsuperscript{27} For example, the Texas Hospital Licensing Law, which regulates hospitals that operate in the State of Texas, only regulates the disclosure of health care information by a hospital, but not the hospital’s internal use of the information. Specifically, the Texas Hospital Licensing Law provides that “[e]xcept as authorized by Section 241.153, a hospital or an agent or employee of a hospital may not disclose health care information about a patient to any person . . . without the written authorization of the patient . . . .” \textsc{Tex. Health & Safety Code Ann.} § 241.152(a) (Vernon 2004) (emphasis added). Similarly, the Texas Medical Practice Act, which regulates physicians that practice medicine in the State of Texas, also only regulates the disclosure of information by physicians. For example, the Texas Medical
C. THE DEFINITION OF "RESEARCH"

Before addressing the rules to which a covered entity must adhere when using or disclosing PHI for research activities, those activities that constitute research activities must be identified. The Privacy Rule defines research as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge." Importantly, the Privacy Rule distinguishes between research activities and a set of activities called "health care operations." The Privacy Rule includes within the definition of health care operations:

Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination.

The distinction between a research activity and a health care operations activity appears to be whether the activity is designed to develop or contribute to generalizable knowledge. If the activity is designed to develop or contribute to generalizable knowledge, the activity is research. However, if the activity relates to conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines and the primary purpose of any studies resulting from such activities is not obtaining generalizable knowledge, then the activity constitutes a health care operation.

The ability to distinguish between a research activity and a health care operation is important. As discussed in more detail below, research activities require the covered entity to obtain from the patient (or her legal representative) a detailed written authorization form if the covered entity is unable to satisfy all of the required elements of an applicable exception to the authorization requirement. On the other hand, the Privacy Rule permits a covered entity to use and disclose PHI to carry out its own health care operations without any form of patient permission and without any other restrictions.

Practice Act provides:

A communication between a physician and a patient, relative to or in connection with any professional services as a physician to the patient, is confidential and privileged and may not be disclosed except as provided by this chapter. [¶] A record of the identity, diagnosis, evaluation, or treatment of a patient by a physician that is created or maintained by a physician is confidential and privileged and may not be disclosed except as provided by this chapter.

TEX. Occ. CODE ANN. § 159.002(a) & (b) (Vernon 2004) (emphasis added). (However, the Texas Medical Practice Act also provides an exception to the privilege of confidentiality, "allowing disclosure of confidential information by a physician" in certain situations including to "qualified personnel for research... but the personnel may not directly or indirectly identify a patient in any report of the research, audit, or evaluation or otherwise disclose identity in any manner..." Id. § 159.004(3). In summary, then, the HIPAA Privacy Rule is unique because it regulates a covered entity's internal use of health information in addition to the disclosure of such information to an external third party.

28. 45 C.F.R. § 164.501 (definition of research).
29. Id. (definition of health care operations).
30. See id. § 164.506(c)(1). "A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations [activities]." Id. Although the Privacy Rule gives
The preamble to the 2000 Final Rule acknowledges that the task of distinguishing between research activities and health care operations activities may be difficult. However, HHS believes that the difference between these activities is important from the patients' perspective. Specifically, HHS believes that individuals expect that "information about themselves will be used for health care operations activities [including] reviewing the competence or qualifications of healthcare professionals, evaluating provider and plan performance, and improving the quality of care." HHS further believes, however, that individuals do not expect that information about themselves will be used for research purposes without their prior authorization. Accordingly, HHS drafted the Privacy Rule in a manner that retains more stringent protections for the use and disclosure of PHI for research purposes than for health care operations activities.

D. Finally: The Research Provisions

The Privacy Rule establishes certain requirements that must be satisfied before a covered entity may use or disclose PHI for research activities. The Privacy Rule generally requires covered entities to obtain prior written authorization (hereinafter, "authorization") from each patient before using or disclosing her PHI for research activities. However, four exceptions to this rule exist. Specifically, covered entities may use and disclose PHI for research activities without prior authorization from the patient if: (1) the covered entity only uses or discloses a limited data set of information pursuant to a data use agreement; (2) the review of the PHI is preparatory to research; (3) the research is on decedents' information; or (4) an institutional review board (IRB) or privacy board has approved a waiver of or an alteration to the authorization. Each of these exceptions, as well as the criteria set forth therein, is discussed in Sections II(D)(2) through II(D)(5), below. In addition, covered entities always are free to use and disclose information that does not constitute PHI (i.e., information that is not individually identifiable) without regulation by the Privacy Rule. Stated another way, covered entities always are free to use and disclose information that has

---

32. Id.
33. Id.
34. See 45 C.F.R. § 164.508(c)(1) & (2) (identifying the elements and statements required to be included in an authorization form).
35. The health care industry refers to these situations as either "exceptions" (i.e., to the authorization requirement) or as "regulatory permissions" (i.e., permission to use and disclose PHI without authorization or any other form of patient permission). For the sake of brevity, I will refer to each as an "exception."
been sufficiently de-identified, as described in Section II(D)(1), immediately below.

1. Research Using De-Identified Health Information

The Privacy Rule only regulates a covered entity’s use or disclosure of protected health information; that is, **individually identifiable** health information. **Individually identifiable** health information specifically refers to health information that either identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.\(^{37}\) However, once information has been sufficiently de-identified,\(^{38}\) the Privacy Rule no longer applies to a covered entity’s use or disclosure of such de-identified information, and the covered entity may freely use and disclose the de-identified information without any form of prior patient permission or other regulation by the Privacy Rule.

The Privacy Rule establishes two methods for de-identifying health information. The most popular method, known as the “safe harbor” method, provides that a covered entity is considered to have de-identified information if the covered entity has removed all of a list of enumerated identifiers\(^{39}\) from the information and if the covered entity has no actual knowledge that the remaining information could be used alone or in combination with other information to identify the subject of the information.

The second method for de-identifying information requires a person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable to apply such principles and/or methods and determine “that the risk is very small that the information could be used, alone or in combination with

---

37. 45 C.F.R. § 164.501 (definition of individually identifiable health information).
38. For the HIPAA Privacy Rule’s provisions relating to de-identification, see 45 C.F.R. §§ 164.502(d) & 164.514(a)-(c).

The following identifiers of the individual, or of relatives, employers, or household members of the individual, must be removed from the information for the information to be sufficiently de-identified under the “safe harbor” method: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000; (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code . . . .

Id.
other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information."\(^{40}\) The person with knowledge of and experience with the statistical and scientific principles must document the methods and the results of her analysis that justify the determination that the risk of identification is small.\(^{41}\)

Because some forms of "records" research (also known as "retrospective," "archival," or "non-interventional" research) can be conducted using information that does not directly identify the individuals who are the subject of the information, the availability of a de-identification safe harbor, if appropriately structured, theoretically could encourage researchers to seek and use information that has been appropriately de-identified.\(^{42}\) However, following the publication of the de-identification safe harbor in the 2000 Final Rule, several articles appeared in medical journals arguing that the safe harbor, as written, is useless for many types of epidemiologic, health services, and other population-based research that require identification of each subject's geographical information, as well as certain dates and ages.\(^{43}\)

2. The First Exception: Using or Disclosing a Limited Data Set Pursuant to a Data Use Agreement

Because of the many complaints relating to the stringent criteria set forth in the de-identification safe harbor, the 2002 Final Modifications adopted a new provision that permits covered entities, without patient authorization, to use or disclose a "limited data set" of information for research purposes if the use or disclosure of the limited data set is made in accordance with a "data use agreement."\(^{44}\) "A limited data set is [PHI] that excludes" most, but not all, of the identifiers listed under the de-identification safe harbor including: "(i) names; (ii) postal address information other than town or city, state, and zip code; (iii) telephone numbers; (iv) fax numbers; (v) e-mail addresses; (vi) social security numbers; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) biometric identifiers, including finger and voice prints; and (xvi) full face photographic images and any comparable images."\(^{45}\)

Importantly, however, a limited data set permits a few identifiers to remain in the information including years relating to a patient (e.g., dates of service,
admission, or discharge; date of birth; date of death) and information relating to the town or city, state, and five-digit zip code of the patient, his or her employer, and the patient’s household members. Thus, information relating to the asthmatic condition of a child born on January 1, 2004, who lives in Houston, Texas, 77002, could be included within the limited data set, even though that same information would not constitute de-identified information under the de-identification safe harbor.

Under the Privacy Rule, a covered entity may use or disclose a limited data set for research purposes without patient authorization if the covered entity obtains satisfactory assurance, in the form of a data use agreement, that the limited data set recipient will only use or disclose the PHI for the limited research purposes. The preamble to the 2002 Final Modifications does not prescribe the form of the data use agreement, but does explain that the data use agreement may be a formal contract, an informal memorandum of understanding or, if the use of the limited data set is by the covered entity’s workforce members, the covered entity may choose to enter into a data use agreement with those workforce members similar to the manner in which a covered entity would enter into a confidentiality agreement with its workforce members.

3. The Second Exception: Reviews Preparatory to Research

The second exception allows covered entities to use and disclose PHI without patient authorization if a researcher will be reviewing the information for a purpose “preparatory to research.” This exception requires the covered entity to obtain from the researcher representations that:

(A) [The] use or disclosure is sought solely to review [PHI] as necessary to prepare a research protocol or for similar purposes preparatory to research;

46. 45 C.F.R. § 164.514(b)(2)(i)(C).
47. 45 C.F.R. § 164.514(e)(2). See also Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,235 (Aug. 14, 2002) (“Therefore, as part of a limited data set, researchers and others involved in public health studies will have access to dates of admission and discharge, as well as dates of birth and death for the individual . . . . [T]he limited data set may include the five-digit zip code or any other geographic subdivision, such as State, county, city, precinct and their equivalent geocodes, except for street address.”).
48. The data use agreement must:
(A) Establish the permitted uses and disclosures of such information . . . and may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the [Privacy Rule] if done by the covered entity; (B) Establish who is permitted to use or receive the limited data set; and (C) Provide that the limited data set recipient will: (1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law; (2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement; (3) Report to the Covered Entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware; (4) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and (5) Not identify the information or contact the individuals.
49. 45 C.F.R. § 164.514(e)(4)(ii).
(B) No [PHI will] be removed from the covered entity by the researcher in the course of [the] review; and
(C) The [PHI] for which the use or access is sought is necessary for the research purposes.\textsuperscript{51}

HHS has indicated that the covered entity may permit the researcher to make these representations in written or oral form.\textsuperscript{52}

4. The Third Exception: Research on Decedent’s Information

The third exception allows covered entities to use or disclose PHI about decedents for research purposes without obtaining patient authorization from a personal representative of the decedent if the covered entity obtains from the researcher:

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;
(B) Documentation, at the request of the covered entity, of the death of such individuals; and
(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.\textsuperscript{53}

The preamble to the Privacy Rule explains that this third exception is modeled after the Common Rule, which does not require IRB review of research on decedents’ information because the Common Rule “does not consider deceased persons to be ‘human subjects.’”\textsuperscript{54}

5. The Fourth Exception: IRB or Privacy Board Approval of a Waiver of or Alteration to Patient Authorization

The fourth exception permits covered entities to use and disclose PHI for research activities without patient authorization if an IRB or privacy board meeting certain requirements approves a waiver of the otherwise required patient authorization or an alteration to the required elements of the authorization. To satisfy this exception, the covered entity must obtain written documentation regarding the following:

a. The waiver of authorization has been approved by either an IRB or a privacy board meeting specified standards;\textsuperscript{55}
b. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;\textsuperscript{56}
c. The IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization, satisfies three criteria (discussed in

\textsuperscript{51} 45 C.F.R. § 164.512(i)(1)(ii).
\textsuperscript{52} Dep’t of Health & Human Servs., Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule 17, NIH Pub. No. 03-5388 (2003).
\textsuperscript{53} 45 C.F.R. § 164.512(i)(iii).
\textsuperscript{54} Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,701 (Dec. 28, 2000).
\textsuperscript{55} 45 C.F.R. § 164.512(i)(1)(i).
\textsuperscript{56} Id. § 164.512(i)(2)(i).
more detail in Section IV(A), below);\textsuperscript{57}
d. A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board;\textsuperscript{58}
e. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures;\textsuperscript{59} and
f. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.\textsuperscript{60}

6. \textit{Prior Written Authorization}

If a covered entity cannot or chooses not to de-identify the information or satisfy one of the four exceptions to the patient authorization requirement, then the covered entity must obtain the prior written authorization of the patient or the patient’s legal representative before using or disclosing the patient’s PHI for a research activity.\textsuperscript{61} The authorization form must contain certain elements and statements, which are identified and discussed in detail in Section III(A), below.

E. \textbf{The Privacy Rule’s “Individual Rights” Provisions}

In addition to establishing requirements that regulate how covered entities can use and disclose PHI,\textsuperscript{62} the Privacy Rule also gives certain rights to individuals who are the subject of PHI. These rights, referred to as the “individual rights,” include the right: (i) to notice of the covered entity’s privacy practices for PHI;\textsuperscript{63} (ii) to request additional privacy protections;\textsuperscript{64} (iii) to access (\textit{i.e.}, inspect and copy) PHI;\textsuperscript{65} (iv) to request amendment of incorrect or incomplete PHI;\textsuperscript{66} and (v) to receive an accounting of disclosures of PHI upon request.\textsuperscript{67} The notice of privacy practices and the accounting of disclosures provisions are discussed and analyzed in detail in Sections III(B) and III(C), below.

\begin{itemize}
\item \textsuperscript{57} Id. \textsection\textsection 164.512(i)(2)(ii).
\item \textsuperscript{58} Id. \textsection\textsection 164.512(i)(2)(iii).
\item \textsuperscript{59} Id. \textsection\textsection 164.512(i)(1)(iv).
\item \textsuperscript{60} Id. \textsection\textsection 164.512(i)(2)(v).
\item \textsuperscript{61} Please note that the Privacy Rule’s requirement for a written authorization, as described in the immediately preceding sentence, is different than, and in addition to, the Common Rule’s requirement to obtain the subject’s informed consent to participate in the research, as well as other applicable federal and/or state law requirements.
\item \textsuperscript{62} These “use and disclosure” requirements generally are set forth at 45 C.F.R. \textsection\textsection 164.502 – 164.514.
\item \textsuperscript{63} 45 C.F.R. \textsection\textsection 164.520.
\item \textsuperscript{64} Id. \textsection\textsection 164.522.
\item \textsuperscript{65} Id. \textsection\textsection 164.524.
\item \textsuperscript{66} Id. \textsection\textsection 164.526.
\item \textsuperscript{67} Id. \textsection\textsection 164.528.
\end{itemize}
III. ANALYSIS OF THE RIGHTS ATTRIBUTED TO INDIVIDUALS WHO ARE THE SUBJECT OF PROTECTED HEALTH INFORMATION

This Section III addresses whether the Privacy Rule promotes autonomy by analyzing certain of the legal rights attributed by the Privacy Rule to individuals who are the subjects of protected health information in light of the ethical principles set forth in the Belmont Report. Specifically, and as is discussed in more detail below, although the rights attributed to individuals under the Privacy Rule appear to promote respect for persons by giving patients additional information upon which to deliberate when making decisions regarding whether to participate in research, the realization of such autonomy is significantly limited by the following characteristics and features of the Privacy Rule: (1) the complex and confusing nature of most of the elements and statements required to be included in an authorization form (see Section III(A)(1)); (2) the covered entity’s ability to combine the research authorization form with other research-related documents (see Section III(A)(2)); (3) the covered entity’s ability to “condition” the provision of research-related treatment on the patient’s execution of the authorization form (see Section III(A)(3)); (4) the length of the notice of privacy practices and the number of required statements and/or the brevity of the discussion of research uses and disclosures therein (see Section III(B)); (5) covered entities’ reliance on law firms’ and/or professional organizations’ drafts of sample notices, and the failure of covered entities to develop their own institution-specific notices (see Section III(B)); and (6) the Privacy Rule’s “simplified” accounting provisions which provide little, if any, meaningful information to research subjects regarding the disclosure of their PHI for research activities (see Section III(C)).

A. THE RIGHT TO AUTHORIZE (OR REFUSE TO AUTHORIZE) USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION FOR RESEARCH ACTIVITIES

If a covered entity cannot or chooses not to de-identify the information to be used or disclosed, or cannot or chooses not to satisfy one of the four exceptions to the patient authorization requirement, then the covered entity must obtain the prior written authorization of the patient or the patient’s legal representative before using or disclosing the patient’s PHI for a research activity.

1. The Required Elements and Statements

The Privacy Rule requires the authorization form to contain several elements and statements including: (1) a description of the information to be used

68. Belmont Report, supra note 8.
69. Interestingly, the Privacy Rule distinguishes between required “elements” and “statements.” “Elements” are those items required to be included in the authorization form under 45 C.F.R. § 164.508(c)(1). “Statements” are those items required to be included in the authorization form under 45 C.F.R. § 164.508(c)(2). “Elements” appear to be items that require additional input from the covered entity (e.g., the name of the organization receiving the information, a specific expiration date or event),
or disclosed; (2) the identification of the persons or class of persons authorized to make the use or disclosure of the PHI; (3) the identification of the persons or class of persons to whom the covered entity is authorized to make the use or disclosure; \(^{70}\) (4) a description of each purpose of the use or disclosure; (5) an expiration date or event; (6) the individual's signature and date; (7) if signed by a personal representative, a description of his or her authority to act for the individual; (8) a statement that the individual may revoke the authorization in writing, and either a statement regarding the right to revoke and instructions on how to exercise such right or, to the extent this information is included in the covered entity's notice, a reference to the notice; (9) a statement that treatment, payment, enrollment, or eligibility for benefits may not be conditioned on obtaining the authorization if such conditioning is prohibited by the HIPAA Privacy Rule or, if conditioning is permitted by the HIPAA Privacy Rule, a statement about the consequences of refusing to sign the authorization; and (10) a statement about the potential for the PHI to be subject to re-disclosure by the recipient. \(^{71}\)

The first, second, third, sixth, seventh, and eighth required elements are not too controversial; indeed, many state laws required such information to be included in patient authorization forms even before HHS published its 1999 Proposed Rule. \(^{72}\) Accordingly, this article will not address these elements in detail.

a. The Statement of Purpose

The fourth element required by the Privacy Rule to be included in each authorization form is a "description of each purpose of the requested use or disclosure." \(^{73}\) Although the existence of this element, as stated, is not controversial, \(^{74}\)

while "statements" appear to be general statements designed to notify the patient of a particular fact (e.g., the fact that the recipient may not be a covered entity and, therefore, may re-disclose the information without risking sanctions under the Privacy Rule).

\(^{70}\) 45 C.F.R. § 164.508(c)(1). HHS specifically explains that the authorization must list:

ALL names or other identification, or ALL classes, of persons who will have access through the covered entity to the protected health information (PHI) for the research study (e.g., research collaborators, sponsors, and others who will have access to data that includes PHI). Examples may include, but are not limited to the following: [1] Data coordinating centers that will receive and process PHI; [2] Sponsors who want access to PHI or who will actually own the research data; and/or [3] Institutional Review Boards or Data Safety and Monitoring Boards.


\(^{71}\) 45 C.F.R. § 164.508(c)(1) - (2).

\(^{72}\) For example, the Texas Medical Practice Act has always required physicians to include in a "consent for the release of confidential information" the following information: (1) the billing records, medical records, or other information to be covered by the release; (2) the reasons or purposes for the release; and (3) the person to whom the information is to be released. See TEX. OCC. CODE ANN. § 159.005(b) (Vernon 2004). In addition, the Texas Medical Practice Act has always required the consent to be in writing and to be signed by: (1) the patient; (2) a parent or legal guardian of the patient if the patient is a minor; (3) a legal guardian of the patient if the patient has been adjudicated incapacitated to manage the patient's personal affairs; (4) an attorney ad litem appointed for the patient . . . ; or (5) a personal representative of the patient if the patient is deceased. Id. § 159.005(a).

\(^{73}\) 45 C.F.R. § 164.508(c)(1)(iv).

\(^{74}\) For example, the Texas Medical Practice Act also requires "the reasons or purpose for the release" to be stated in a "consent for the release of confidential information." See TEX. OCC. CODE ANN. § 159.005(b)(2) (Vernon 2004).
HHS has interpreted this element to mean that the statement of purpose must be "research study specific" when the authorization is for a use or disclosure of PHI for research activities. Moreover, HHS has specifically stated that an authorization form which only identifies a nonspecific research activity or a future, unspecified research activity is not a sufficient statement of purpose, and that an authorization form containing such a statement will be considered invalid and ineffective to authorize the covered entity to use or disclose the information.

Please note that the requirement for a research study-specific statement would effectively prohibit a covered entity, like a hospital, from using "blanket" research authorization forms that would authorize the use and disclosure of the patient’s information for general research purposes. For example, “all patients seen at the Olmstead Medical Center in Minnesota for two months in 1997 were asked to give general authorization to release their medical records for ‘research.’” Similarly, patients from the Mayo Clinic received forms sent with appointment notices requesting consent for “future research.” Under the Privacy Rule, the forms used by the Olmstead Medical Center and the Mayo Clinic simply stating the general purpose of the authorization as "research" or "future research," respectively, would be insufficient and would render the authorization forms invalid.

Of importance to the instant discussion, Part B of the Belmont Report identifies three basic ethical principles, including respect for persons. The Belmont Report specifically states that:

An autonomous person is an individual capable of deliberation about personal goals and of acting under the direction of such deliberation. To respect autonomy is to give weight to autonomous persons’ considered opinions and choices while refraining from obstructing their actions unless they are clearly detrimental to others. To show lack of respect for an autonomous agent is to repudiate that person’s considered judgments, to deny an individual the freedom to act on those considered judgments, or to withhold information necessary to make a considered judgment, when there are no compelling reasons to do so.

In addition, Part C of the Belmont Report discusses the topic of “information,” and further explains that disclosing specific pieces of information to patients with the intent of giving them sufficient information to make an informed deci-
sion promotes autonomy.80

Using the principles identified in the Belmont Report, the Privacy Rule’s requirement for a research study-specific statement of purpose arguably increases the likelihood that a particular patient will be able to make a quality decision regarding the use and disclosure of her PHI. Specifically, one could argue that a more specific statement of purpose will allow patients with particular feelings regarding particular types of research to select those research activities for which they feel their information might be useful, and to refuse to allow their PHI to be used or disclosed for research activities that may not be in their best interests. In view of the National Commission for the Protection of Human Subjects of Biomedical and Behavior Research’s position in the Belmont Report, by identifying the specific research study for which the patient’s information will be used or disclosed, the covered entity is giving the patient the freedom to act on her best judgment. On the other hand, withholding information regarding the particular study for which the patient’s information will be used or disclosed, when there is no compelling need to do so, could obstruct an informed decision and demonstrates a lack of respect for the potential research subjects.

Indeed, providing a greater amount of information to the patient regarding the specific study for which the patient’s information will be used also may increase the chance that some individuals will authorize their information to be used and disclosed. In the article The Use of Medical Records in Research: What Do Patients Want?, authors Nancy Kass et al. discussed the results of a survey they conducted that involved “602 persons with a serious genetic or other chronic medical condition (or family history of such condition) concerning their experiences with and attitudes toward the privacy of their medical information.”81 The authors found that when patients with a particular disease were asked for permission to use their records for research by someone working on that same disease, such patients might be particularly likely to say ‘yes,’ given that the potential benefits of research may seem more directly relevant. The authors also concluded that researchers need to do a better job describing to patients why research is important, why it may be relevant to them and/or their family members, and why medical records often are essential to conducting such research.

In summary, an authorization form that specifically identifies the particular research study for which the patient’s information will be used or disclosed, compared to an authorization form that states a general purpose such as “research,” or “future research,” when there is no compelling need not to do so, would appear to promote patient autonomy and should be considered a positive development by the Privacy Rule. Unfortunately, the same cannot be said with respect to several of the other elements and statements the Privacy Rule requires to be included in an authorization form.

80. Id.
81. Kass et al., supra note 77, at 432.
b. An Expiration Date or Event

The fifth element generally required by the Privacy Rule to be included in an authorization form is an expiration date or event after which the covered entity is no longer permitted to use or disclose the PHI identified in the authorization form for the purpose identified in the authorization form. The preamble to the 2000 Final Rule explains, for example, that the statement may include a specific expiration date (e.g., January 1, 2004), or "a specific time period (e.g., one year from the date of signature)," or a specific expiration event that is "directly relevant to the individual or the purpose of the use or disclosure (e.g., for the duration of the individual's enrollment with the health plan that is authorized to make the use or disclosure)."

The 2002 Final Modifications clarified, however, that when an authorization form is for the use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository, then "the statement 'end of the research study,' "none," or similar language is sufficient." The clarification in the 2002 Final Modifications was, perhaps, a response to earlier comments submitted to HHS arguing that the general requirement for an expiration date or event "runs counter to the needs of research databases and repositories that are often retained indefinitely." HHS further explains its new position in the preamble to the 2002 Final Modifications:

*Comment:* One commenter argued that expiration dates should be included on authorizations and that extensions should be required for all research uses and disclosures made after the expiration date or event has passed.

*Response:* The Department disagrees. We have determined that an expiration date or event would not always be feasible or desirable for some research uses and disclosures of protected health information. By allowing for no expiration date, the final Rule permits without separate patient authorization important disclosures even after the "termination of the research project" that might otherwise be prohibited. However, the final Rule contains the requirement that the patient authorization specify if the authorization would not have an expiration date or event. Therefore, patients will have this information to make an informed decision about whether to sign the authorization.

Read together, the regulation and the interpretive preamble language would appear to require a research authorization to contain, at least, a statement to the following effect: "This authorization form will expire at the end of the research study" or "The expiration date for this authorization form is: None."

---

84. 45 C.F.R. § 164.508(c)(1)(v).
86. *Id.* at 53,225.
As discussed above, Part C of the Belmont Report explains that disclosing specific pieces of information to patients with the intent of giving them sufficient information to make an informed decision promotes autonomy. If the Privacy Rule is not going to require a specific expiration date in order to permit the completion of research studies that do not always have a specific “end” date, or to permit the creation of research databases, which are maintained indefinitely, then the authorization should explain to the patient why there is no expiration date. One of the Privacy Rule’s suggested statements (“at the end of the research study”) accomplishes this task. However, the other suggested statement (“none”) provides little additional information to the patient and may simply confuse the patient. The following statements may provide greater information to the patient and may be less confusing: “Because we are unsure of how long the research study will take, this authorization form will not expire on a particular date. However, we will not be permitted to use and disclose your information after the research study has ended.”

c. A Statement about the Potential for the PHI to be Subject to Re-Disclosure by the Recipient

The Privacy Rule requires authorization forms to include a statement regarding “[t]he potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.” In the preamble to the 2002 Final Modifications, HHS clarified that the statement “does not require an analysis of the risk for redisclosure, but may be a general statement that the health information may no longer be protected by the Privacy Rule once it is disclosed by the covered entity.” HHS further explains its belief that individuals need to know about the consequences of authorizing the disclosure of their PHI, and that the potential for redisclosure may, indeed, be an important factor in an individual’s decision to give or deny a requested authorization.

As discussed above, one portion of Part C of the Belmont Report focuses on the information that is given to the patient during the informed consent process, and explains that disclosing specific pieces of information to patients with the intent of giving them sufficient information to make an informed decision promotes autonomy. The Privacy Rule’s requirement for a statement regarding the possibility of redisclosure by the recipient would appear to promote patient autonomy by increasing the likelihood that a particular patient will be able to make a quality decision regarding the use and disclosure of their PHI. For example, if a patient was specifically concerned about the redisclosure of her information, she may choose not to authorize the disclosure. On the other hand, if

87. Belmont Report, supra note 8.
88. 45 C.F.R. § 164.508(c)(2)(iii).
90. Id.
91. Belmont Report, supra note 8.
a patient is unconcerned regarding future disclosures, she may elect to authorize the disclosure.

More specifically, if a particular patient knew that one recipient of her PHI would be Eli Lilly, the pharmaceutical giant, she might be more hesitant to authorize the disclosure of her information in light of the Eli Lilly’s recent “mistake” during the summer of 2002 when it sent an email to 669 persons who were then taking Eli Lilly’s drug Prozac, and all of the recipients’ email addresses were visible to all of the other email recipients, thus identifying to each Prozac-user the email address of 668 other Prozac-users.\footnote{See Crowell & Moring, L.L.P., Pharmaceutical Company Settles FTC Charges for Unintentional Disclosure of Email Addresses of Consumers, available at http://www.crowell.com/Content/Expertise/HealthCare/HealthCareLawNews/2002/Email.htm (last visited Nov. 11, 2003) (a law firm’s newsletter explaining that Eli Lilly settled Federal Trade Commission charges for unintentional disclosure of email addresses of consumers).} Similarly, if a particular patient knew that a recipient of her PHI would be Johnson & Johnson and that Johnson & Johnson was not a covered entity, she also might be hesitant to authorize the disclosure of her information if she knows that Johnson and Johnson inappropriately marketed a list of five million names and addresses of elderly incontinent women in 1998.\footnote{See, e.g., Sinai Health System’s Authorization to Use and Disclose Health Information for Research, available at http://www.sinai.org/review_board/authorizationform.pdf (last visited on Dec. 16, 2003).}

As stated above, HHS’ belief that individuals need to know about the consequences of authorizing the disclosure of their PHI, and the potential for the re-disclosure of their information, is on point. However, many covered entities’ authorization forms fumble when attempting to convey these ideas, and the patient reading the form may fail to understand that the recipient of her information is not required by the Privacy Rule to protect her information and may be able to re-disclose her information without being subject to sanctions under the Privacy Rule.

A review of authorization forms available on the Internet illustrates the difficulty covered entities convey when attempting to draft their authorizations. For example, one covered entity’s authorization form for the use and disclosure of research states the following: “Information disclosed to groups outside Sinai Health System may no longer be covered by this Authorization and federal privacy Regulations.”\footnote{Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,467 (Dec. 28, 2000).} The phrase “may no longer be covered by this Authorization” and the phrase “federal privacy regulations” may have little or no meaning to a person who is unsure of what the authorization “covers” in the first place, or to anyone besides a health care attorney who specializes in the Privacy Rule and, therefore, has a firm grasp on what the Privacy Rule protects.

Another covered entity’s “Authorization for the Use and Disclosure of Protected Health Information (PHI)” provides: “If neither federal nor Texas privacy law apply to the recipient of the information, I understand that the information disclosed pursuant to this authorization may be re-disclosed by the recipient and
no longer protected by federal or Texas privacy law.”

Again, this covered entity made a valiant attempt to capture the intent of the required statement, and probably conveys more of such intent than did the first authorization form discussed in the preceding paragraph. Unfortunately, if the patient who is signing the authorization form does not know the persons and organizations to whom federal and Texas privacy law apply, or the protections provided by such laws, the statement does not really provide the patient with information that will help the patient make a decision whether to authorize the disclosure of her information. For example, a patient may believe that federal privacy law does apply to pharmaceutical companies and would prohibit such companies from re-disclosing PHI when, in fact, the Privacy Rule generally does not apply to pharmaceutical companies because they do not fall within the definition of a covered entity.

As a final example, another covered entity’s “Authorization for Disclosure of Protected Health Information for Research” provides: “Your information that is disclosed to the researcher(s) may no longer be protected by Federal privacy regulations if the researcher(s) is not a health care provider covered by the regulations, however the researcher(s) agrees to protect your information as required by law.” This covered entity also attempted to capture the intent of the Privacy Rule’s required statement. However, it is likely that each patient’s PHI will be disclosed to persons and/or organizations beyond the “researcher(s)” identified in the form. For example, the pharmaceutical company who is sponsoring the research may receive PHI, or members of the researchers’ home institution also may receive PHI. In addition, this covered entity attempted to counteract the negative implications of the required statement by adding an additional statement that, “however the researcher(s) agrees to protect your information as required by law.” Unless the patient signing the authorization form understands that very little “law” protects information in the hands of a researcher who is not also a covered entity, the additional statement may indeed counteract the original required statement, which was intended to alert the patient that the researchers are not covered entities and, therefore, are subject to few if any prohibitions regarding their subsequent use and disclosure of patients information. Perhaps an individualized statement like the following would be more helpful: “The organizations that receive information under this authorization, including the researchers at Triangle Research and the Eli Lilly Pharmaceutical Company, may redisclose the information they receive under this authorization form without penalty under federal or state law.”

In summary, HHS’ belief that individuals need to know about the consequences of authorizing the disclosure of their PHI, and the potential for the re-


disclosure of their information, is on point. Unfortunately, patients who have little understanding of federal or state privacy law may have difficulty understanding the covered entities’ various attempts to put this idea on paper.

2. **Compound Authorizations: "I Signed What?"**

Part C of the Belmont Report also specifically discusses the topic of “comprehension,” and explains that the manner and context in which information is conveyed is as important as the information itself:

For example, presenting information in a disorganized and rapid fashion, allowing too little time for consideration or curtailing opportunities for questioning, all may adversely affect a subject’s ability to make an informed choice. 97

In addition, in The Law of Bioethics: Individual Autonomy and Social Regulation, the authors discuss whether patients understand and remember what they are told during the informed consent process. 98 The authors cite studies noting that patients could remember only small portions of the information that had been discussed during informed consent interviews, and that conclude that patients either forget what they are told or never really understood the information in the first place, and that the level of understanding in patients to whom informed consent disclosures have been made is not very high. 99 Importantly, the authors’ statements are made within the context of orally presented interviews, which may result in greater patient comprehension. Neither the Privacy Rule, its interpretive preamble language, nor any of the guidance documents allegedly interpreting the Rule require authorizations for the use or disclosure of PHI to be orally explained to the patient. The Privacy Rule simply requires covered entities to “obtain” or “receive” a valid authorization. 100

Although the statements in the Belmont Report were made with respect to researchers’ attempts to obtain a potential subject’s informed consent to participate in the research, the statements also are applicable to a covered entity’s attempt to obtain an authorization for the use or disclosure of PHI. Unfortunately, the Privacy Rule permits research authorizations to be presented to the patient in a disorganized fashion. Specifically, although the Privacy Rule contains a general prohibition against “compound” authorizations (i.e., an authorization for the use or disclosure of PHI generally may not be combined with any other document to create a compound authorization), 101 the Privacy Rule contains an exception to this prohibition for research authorizations pursuant to which an authorization for the use or disclosure of PHI can be combined in the same docu-

---

99. Id. at 112-13.
100. DHHS, Security and Privacy, 45 C.F.R. § 164,508(a) (2003).
101. 45 C.F.R. § 164,508(b)(3) “An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization . . . .” Id.
ment as any other type of written permission for the same research study, including a consent to participate in the research and any other documentation relating to the research.\textsuperscript{102}

Unfortunately, research consent documents, as well as other information provided to the prospective subject that relates to the research, can be very long. Many authorizations for the use and disclosure of PHI for research activities are either: (1) "floating" in the middle of other research-related documentation; or (2) "tacked on" to the end of existing informed consent and other documentation.\textsuperscript{103} One could argue that only a careful health care attorney who specializes in the Privacy Rule would notice a "floating" authorization placed in the middle of, or at the end of, another document.

In summary, the Privacy Rule provision permitting research authorizations to be combined with other research-related information can result in a situation in which information is presented to the patient in a disorganized fashion, which may adversely affect the patient's ability to understand the information presented and make an informed choice whether to authorize the use or disclosure of her PHI for research activities.

3. "Conditioning" Research-Related Treatment on the Patient's Execution of an Authorization Form

Part C of the Belmont Report also contains a discussion of the topic of "voluntariness." Specifically, the Belmont Report states:

An agreement to participate in research constitutes a valid consent only if voluntarily given. This element of informed consent requires conditions free of coercion and undue influence. Coercion occurs when an overt threat of harm is intentionally presented by one person to another in order to obtain compliance. Undue influence, by contrast, occurs through an offer of an excessive, unwarranted, inappropriate or improper reward or other overture in order to obtain compliance . . . .

[U]ndue influence would include actions such as manipulating a person's choice through the controlling influence of a close relative and threatening to withdraw health services to which an individual would otherwise be entitled [sic].\textsuperscript{104}

Along the same lines as the emphasized language in the immediately preceding

\textsuperscript{102} 45 C.F.R. § 164.508(b)(3)(i). This rule states in part that:

An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows: (i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research . . . .

\textit{Id.}

\textsuperscript{103} See, e.g., Kulychny & Korn, \textit{supra} note 22 (explaining that model authorization forms prepared by the American Hospital Association contain two pages of disclosures, not including pages of other standard disclosures required for research).

\textsuperscript{104} Belmont Report, \textit{supra} note 8 (emphasis added).
quotation, the Privacy Rule contains a general prohibition on "conditioning" of authorizations. Specifically, the Privacy Rule generally prohibits a covered entity from "condition[ing] the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization . . . ." The purpose of this general rule is to prevent covered entities from coercing individuals into signing an authorization for a use or disclosure that is not necessary to carry out the primary services that the covered entity provides to the individual. HHS explains in the preamble to the 2000 Final Rule:

For example, a health care provider could not refuse to treat an individual because the individual refused to authorize a disclosure to a pharmaceutical manufacturer for the purpose of marketing a new product. 106

Important to the instant discussion, however, the Privacy Rule contains a specific exception to the general prohibition against "conditioning" for research-related treatment. Specifically, the Privacy Rule permits a "covered health care provider [to] condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research . . . ." HHS explains that permitting the use and disclosure of PHI is part of the patient’s decision to receive care through the clinical trial and, therefore, that the conditioning is necessary to ensure that the researchers have access to the information for which they are providing valuable treatment:

Covered entities seeking authorization . . . to use or disclose protected health information created for the purpose of research that includes treatment of the individual, including clinical trials, may condition the research-related treatment on the individual’s authorization. Permitting use of protected health information is part of the decision to receive care through a clinical trial, and health care providers conducting such trials should be able to condition research-related treatment on the individual’s willingness to authorize the use or disclosure of his or her protected health information for research associated with the trial. 108

In addition to these requirements, the Privacy Rule also requires authorization forms for research to contain a statement placing the patient on notice of the covered entities’ . . . :

[A]bility or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either: (A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when [the prohibition on same applies]; or (B) The consequences to the individual of a refusal to sign the authorization when . . . the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization. 109

Again, HHS’ belief that a patient needs to know about the consequences of her

---

105. 45 C.F.R. § 164.508(b)(4).
107. 45 C.F.R. § 164.508(b)(4)(iii).
refusal to sign an authorization is on point. Unfortunately, as with other required authorization elements discussed above, the complexity of the Privacy Rule’s provisions regarding “conditioning” of authorizations has resulted in confusing statements by covered entities as they attempt to put the “conditioning” concept on paper.

For example, one covered entity made the following relevant statement in its research authorization: “You may refuse to sign this authorization and your refusal will not affect your ability to obtain treatment, however, it may affect your ability to participate in this research study.” It appears that this covered entity is attempting to explain that the failure to execute the form would not affect the patient’s ability to receive other treatment from the covered entity (e.g., a routine physical that is not associated with any research protocol), but that the patient may not be able to receive research-related treatment unless she signs the authorization form. However, an unsophisticated patient could read the second clause in the covered entity’s statement (“your refusal will not affect your ability to obtain treatment”) and think that she will be able to receive research-related treatment, but that the refusal to sign the authorization will simply affect some other part of her participation in the research study.

However, some covered entities were able to convey the intended notice to patients. For example, one hospital’s authorization form explains: “[I]f you do not sign this authorization for the use and disclosure of your PHI, you will not be able to participate in this research study. Your failure to sign this authorization will not otherwise affect your regular treatment, payment for healthcare, eligibility (or enrollment) for benefits.” The only problem is that the eligibility and enrollment language was included in the Privacy Rule for use by covered entities who are health plans seeking to use PHI to determine whether to enroll a patient in the health plan, not health care providers. Accordingly, patients of this hospital may think that the hospital is capable of enrolling patients in a health plan.

However, some covered entities are capable of both conveying the intended notice to patients and eliminating the inapplicable language relating to eligibility and enrollment in their research authorization form. For example, one covered entity’s authorization form provides:

While your health care outside the study, the payment for your health care, and your health care benefits will not be affected if you do not sign this form, you will not be able to participate in the research described in this authorization and will not receive treatment as a study participant if you do not sign this form.

---


4. Summary Regarding Authorizations under the Privacy Rule

The Institute of Medicine’s recent report, *Responsible Research: A Systems Approach to Protecting Research Participants*, recommends the following with respect to the informed consent process required by the Common Rule:

Informed consent should be an ongoing process that focuses not on a written form or a static disclosure event, but rather on a series of dynamic and appropriately targeted conversations between the participant and the research staff that should begin before enrollment and be reinforced during each encounter or intervention. The informed consent conversation(s), as well as the written consent document, should not be obscured by language designed mainly to insulate the institution from liability. Rather, the process should ensure that participants clearly understand the nature of the proposed research and its potential risks and benefits to them and society.\textsuperscript{112}

Although the IOM’s statement was made with respect to obtaining the research participant’s informed consent to participate in the research under the Common Rule (not the individual’s authorization to use and disclose PHI under the Privacy Rule), the IOM’s recommendations are equally applicable to obtaining patient authorization under the Privacy Rule. For example, if the individuals responsible for obtaining each patient’s authorization could “follow-up” on the static statements set forth in the authorization form, by further (orally) explaining the concepts in the authorization form, the patients who are being asked to authorize the disclosure of their information may have a better understanding of what they are signing. One idea is for the researchers, or someone on their behalf, to prepare a PowerPoint presentation or other presentation or video that specifically: (1) identifies and describes the organizations who will receive each individual’s protected health information; (2) identifies each information recipient’s location on a map to help the individual understand where her information will be sent; (3) specifically explaining that no federal or state privacy law applies to certain recipients of the information; and (4) discussing other information interpreting the required statements and elements included in the authorization form. If, before the individuals are asked to authorize the use and disclosure of their information for research purposes, the individuals are shown the presentation and are encouraged to discuss their concerns and ask questions, the individuals’ comprehension of the confusing concepts described in the authorization form may increase.

In summary, by focusing on the required elements of the authorization form, the regulatory permission for “compound” authorizations, and the regulatory permission for the “conditioning” of research-related treatment on the patient’s execution of the authorization form, this Section III(A) attempts to address whether the Privacy Rule’s authorization provisions promote individual autonomy by giving the individual who is the subject of the PHI sufficient in-

formation to choose whether a particular research use or disclosure is in her best interests. Although none of the authorization requirements necessarily impede research, especially since the authorization can be integrated into the informed consent document required by the Common Rule, sole reliance on authorization forms by covered entities and researchers appears to add to the administrative and bureaucratic cloud surrounding research without increasing patient understanding or protection of information. Obtaining authorization for the use and disclosure of PHI for research activities under the Privacy Rule, like obtaining a patient’s informed consent to participate in research under the Common Rule, should be an ongoing process that focuses not on the written authorization form, which is a static disclosure event, but rather on a series of dynamic and appropriately targeted conversations between the patient and the covered entity and/or researcher. Neither the discussion with the patient nor the authorization document should be obscured by complicated language intended to protect the covered entity from liability. Instead, the authorization process should focus on making patients clearly understand how their information will be used for research activities, the risk that their information could be redisclosed by researchers and other recipients, and the potential benefits of the research.

B. THE RIGHT TO RECEIVE A NOTICE OF PRIVACY PRACTICES

In addition to giving individuals the right to authorize (or refuse to authorize) a covered entity’s use or disclosure of PHI for research, the Privacy Rule also provides that individuals (including prospective patients) have the “right to adequate notice of the uses and disclosures of [their PHI] that may be made by [their] covered entity, and of [their] rights and the covered entities’ legal duties with respect to [PHI].”113 Covered entities satisfy this right by developing and distributing a document called a “notice of privacy practices,” which must contains certain required elements and statements.114

113. 45 C.F.R. § 164.520(a)(1).
114. The elements required to be included in each covered entity’s notice of privacy practices include: (i) Header language. A header stating:
   ‘THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY’; (ii) [a description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations; (iii) [a description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual’s written authorization . . . ; (iv) [for each purpose described in [(ii) and (iii)], the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law; (v) [a statement that other uses and disclosures will be made only with the individual’s written authorization and that the individual may revoke such authorization as provided by 45 C.F.R. § 164.508(b)(5) . . . ; (vi) Optional activities. If the covered entity intends to engage in any of the following activities, the description must include a separate statement, as applicable, that: (A) [the covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual, (B) [the covered entity may contact the individual to raise funds for the covered entity; or (C) A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan; (vii) Individual rights. The notice must con-
The Privacy Rule requires each covered entity’s notice of privacy practices to include “a description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual’s written authorization”\textsuperscript{115} and “for each [such] purpose . . . the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by [the Privacy Rule] other applicable law.”\textsuperscript{116} Because research is an activity for which a covered entity may use or disclose PHI without written authorization (in some circumstances), each covered entity that will use or disclose PHI for research without written authorization must include in its notice a “description” of research as one such purpose, as well as “sufficient detail” regarding the type of research activities that will take place.

The preamble to the 2000 Final Rule reasons that “individuals who do not wish for [PHI] about themselves to be [used or] disclosed for research purposes without their authorization [can] select a health care provider” that will not use or disclose PHI for research purposes without individual authorization as set

tain a statement of the individual’s rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows: (A) [t]he right to request restrictions on certain uses and disclosures of protected health information as provided by 45 C.F.R. § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction; (b) [t]he right to receive confidential communications of protected health information as provided by 45 C.F.R. § 164.522(b), as applicable; (c) [t]he right to inspect and copy protected health information as provided by 45 C.F.R. § 164.524; (d) [t]he right to amend protected health information as provided by 45 C.F.R. § 164.526; (e) [t]he right to receive an accounting of disclosures of protected health information as provided by 45 C.F.R. § 164.528; and (f) [t]he right of an individual . . . to obtain a paper copy of the notice from the covered entity upon request; (viii) Covered entity’s duties. The notice must contain: (A) [a] statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information; (B) [a] statement that the covered entity is required to abide by the terms of the notice currently in effect; and (C) [f]or the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, . . . a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice; (ix) Complaints. The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint; (x) Contact information. The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by 45 C.F.R. § 164.530(a)(1)(ii); (xi) Effective date. The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published; (xii) Optional elements. (A) In addition to the information required [above], if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by 45 C.F.R. § 164.512(j)(1)(i); (B) [f]or the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with [45 C.F.R.] § 164.530(i)(2)(ii), the notice must include the statements required by [45 C.F.R. § 164.520] (b)(1)(v)(C).

See 45 C.F.R. 164.520(b)(1).

115. 45 C.F.R. § 164.520(b)(1)(ii)(B).

116. Id. § 164.520(b)(1)(ii)(D).
forth in the provider's notice of privacy practices. The preamble to the 2000 Final Rule further explains that the Privacy Standards also permit covered entities "to agree not to disclose [PHI] for research purposes, even if research disclosures would otherwise be permitted under their notice of" privacy practices.

Unfortunately, most covered entities' notices are either so long, or the discussion of research disclosures is so abbreviated, that patients likely would have difficulty shopping for a health care provider based on whether the provider's notice states that the provider will use a patient's PHI for research activities without authorization. For example, the third paragraph of one covered entity's sixteen-paragraph Notice of Privacy Practices simply states the following with respect its use of patient information for research activities:

We may use or disclose medical and billing information about you without your prior authorization for several other reasons. Subject to certain requirements, we may give out protected health information about you without prior authorization for public health purposes, abuse or neglect reporting, health oversight audits or inspections, research studies, funeral arrangements, organ donation, workers' compensation purposes, or during emergencies. We may also disclose protected health information when required by law, such as in response to a request from law enforcement officials in specific circumstances, or in response to valid judicial or administrative orders.

One could argue that this hospital did not take note of the Belmont Report's statement that presenting information in a "disorganized and rapid fashion . . . all may adversely affect a subject's ability to make an informed choice" when it placed the phrase "research studies" in the middle of a laundry list of other public policy activities identified in the Privacy Rule at 45 C.F.R. § 164.512 for which no authorization is required. In addition, the simple phrase "research studies," without other detail, arguably does not satisfy the Privacy Rule's requirement that the description of each activity "must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by" the Privacy Rule. From reading this hospital's notice, a patient would have no idea whether the hospital uses or discloses PHI for research activities pursuant to an IRB approval of the waiver of the authorization, or for research involving decedents, or for activities preparatory to research, or whether the hospital only uses a limited data set of information pursuant to a data use agreement.

118. Id.
119. See, e.g., Kulynych & Korn, supra note 23 (noting that some notice of privacy practices run to ten pages of single-spaced text).
121. 45 C.F.R. § 164.520(b)(1)(ii)(D).
122. Please note, however, that other health care providers' notices do contain more descriptive statements regarding their research activities. For example, the Houston Women's Care Associates' Notice of Privacy contains a separate paragraph describing its research activities.
The Privacy Rule also requires covered health care providers to "[p]rovide the notice . . . [n]o later than the date of the first service delivery . . . to [patients] after the compliance date for the covered health care provider," and to make a good faith attempt to obtain each patient's written acknowledgement that they have received a copy of the entity's notice of privacy practices, except in emergency situations. Many patients who visited their covered providers following the Privacy Rule's compliance date were handed forms to sign that would document the patient's receipt of the entity's notice of privacy practices when, in fact, the covered entity had not provided the patient with a copy of the notice. In many cases, it was only when the patient asked for a copy of the notice did the patient receive one. In many cases, patients receive a copy of the notice only after waiting a considerable amount of time for registration and benefits verification and, when they finally are promised treatment, they are unwilling to leave that provider and choose another provider who will demonstrate a greater understanding of the Privacy Rule or whose notices provided a better explanation of whether and how they used patient information for research purposes. In summary, covered providers tend to emphasize the importance of obtaining the documentation they are required to obtain under the Privacy Rule (i.e., the patient's written acknowledgement that she has received a copy of the notice), but the same providers do not attempt to notify patients of their privacy practices, as is also required by the Privacy Rule.

Finally, because the Privacy Rule requires so many statements to be included in each covered entity's notice of privacy practices, many covered entities hire sophisticated law firms to draft their notices. Law firms typically draft thorough sample notices that prompt their clients to include client-specific information. However, many providers fail to include institution-specific informa-

---

Research: We may disclose information to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your health information.

See Houston Women's Care Associates Notice of Privacy, available at http://www.hwca.net/HIPAA.htm (last visited Dec. 30, 2003). By further example, North Dallas Plastic Surgery's Notice of Privacy Practices also thoroughly explains:

Research. Our practice may use and disclose your PHI for research purposes in certain limited circumstances. We will obtain your written authorization to use your PHI for research purposes except when an Institutional Review Board or Privacy Board has determined that the waiver of your authorization satisfies the following: (i) the use or disclosure involves no more than a minimal risk to your privacy based on the following: (A) an adequate plan to protect the identifiers from improper use and disclosure; (B) an adequate plan to destroy the identifiers at the earliest opportunity consistent with the research (unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law); and (C) adequate written assurances that the PHI will not be re-used 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 would otherwise be permitted; (ii) the research could not practically be conducted without the waiver; and (iii) the research could not practically be conducted without the waiver; and (iii) [sic] the research could not practically be conducted without access to and use of the PHI.


123. 45 C.F.R. § 164.520(c)(2)(i).
124. Id. § 164.520(c)(2)(ii).
tion, with the result that one provider notice may be the same as every other provider notice.

Providers who do not have the financial resources to hire law firms to draft their notices may copy notices provided by professional organizations including the American Hospital Association, the American Medical Association, or other similar associations. These associations have created for their members generic notices that do not describe a particular entity’s privacy practices and that would require substantial editing to make a notice provider-specific, as is contemplated by HHS. For example, the New Jersey Hospital Association Information Services (NJHAIS) provides model notices of privacy practices, including pocket-sized brochures, 8.5” x 14” patient handouts, and 25.5” x 33” laminated foamboard posters that providers can purchase. To “simplify” the provider’s compliance efforts, the NJHAIS includes the covered provider’s logo and contact information on the notice. The provider’s only responsibility is to “[r]eview the verbiage – make changes, additions and deletions in the highlighted areas and return your customized Notice of Privacy Practices via email,” and then the NJHAIS will produce and mail the order directly to the provider. 125 Unfortunately, most providers appear not to be making many changes to the suggested language.

In summary, HHS contemplates patients using notices of privacy practices as a form of consumer report that provides information about each covered entity’s privacy practices. In theory, patients will read various entities’ notices and shop for a provider who uses and discloses PHI for research activities in a manner that is consistent with the patient’s beliefs. Unfortunately, many patients receive the notice when they are about to receive treatment and either have little time to read the lengthy notice or are unwilling to leave and find another provider who pays greater attention to privacy issues after waiting for a substantial period of time in the waiting room. In addition, many managed care organizations (MCO’s) restrict patients’ choice of physicians and hospitals to those that participate in the MCO’s network, thus further limiting the ability of a patient to choose her provider based on the provider’s notice.

Even if patients were sufficiently educated to use notices of privacy practices as a form of consumer report, covered entities would be required to develop entity-specific notices that describe each entity’s particular privacy practices in order for patients to realize the benefits of their shopping. However, when covered entities copy law firms’ or professional organizations’ sample notices, without customizing them to reflect their own privacy practices, patients are not provided with sufficient institution-specific information from which they can distinguish one provider’s practices from another.

C. THE RIGHT TO RECEIVE AN ACCOUNTING OF DISCLOSURES

In addition to giving patients the right to authorize uses and disclosure of PHI for research and the right to receive a notice of privacy practices, the Privacy Rule also provides individuals with the right to receive an accounting, or a list, of disclosures of PHI made by a covered entity in the six years prior to the date on which the accounting is requested. 126 Unfortunately, the numerous exceptions to the accounting requirement almost swallow the rule. Covered entities are not required to include the following disclosures in an accounting requested by an individual: (a) disclosures to carry out treatment, payment, or health care operations; (b) disclosures to individuals of protected health information about them; (c) disclosures for the covered entity’s facility directory or to persons involved in the individual’s care or other notification purposes; (d) disclosures for national security or intelligence purposes; (e) disclosures to correctional institutions or law enforcement officials; (f) disclosures that occurred prior to the compliance date for the covered entity (i.e., generally, April 14, 2003); (g) disclosures authorized by the individual pursuant to an authorization form that contains all of the required elements set forth at 45 C.F.R. § 164.508(c)(1) and (2); (h) disclosures that are incidental to a permitted use or disclosure; and (i) disclosures of a limited data set pursuant to a data use agreement. 127

In light of the exceptions listed above, if a covered entity uses or discloses PHI for research purposes and such use or disclosure is made pursuant to an authorization form or is of a limited data set and pursuant to a data use agreement, then the covered entity need not track these disclosures in case an accounting is requested by an individual. On the other hand, if a covered entity uses or discloses PHI for research purposes and such use or disclosure is pursuant to one of the other exceptions to the authorization requirement (reviews preparatory to research; research on decedents’ information; or an IRB or privacy board waiver of or alteration to the otherwise required authorization), which are not excepted from the accounting requirement, then the covered entity must track such disclosures and identify them in any accounting that is requested by and provided to a patient.

Accountings generally must include, for each disclosure: (a) the date of the disclosure; (b) the name of the entity or person who received the PHI and, if known, the address of such entity or person; (c) a brief description of the PHI disclosed; and (d) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure. 128 In theory, the purpose of the accounting requirement is to allow patients to request and receive a document identifying all of the situations in which the covered entity has disclosed their information without their knowledge. In theory, patients who obtain such information will be able to identify recipients of their information and/or

126. 45 C.F.R. § 164.528.
127. Id. § 164.528(a)(1).
128. Id. § 164.528(b)(2); § 164.528(b)(2)(iv).
determine whether their covered entities are inappropriately disclosing information.

Importantly, however, the 2002 Final Modifications established a simplified accounting process for disclosures for research purposes involving PHI relating to fifty or more individuals. If, during the period covered by the accounting, a covered entity has made disclosures of PHI for a particular research purpose relating to fifty or more individuals, the accounting may, with respect to such disclosures for which the PHI about the individual may have been included, provide:

a. The name of the protocol or other research activity;
b. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
c. A brief description of the type of protected health information that was disclosed;
d. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
e. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
f. A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity. 129

Both the regular and the simplified accounting processes suffer from several practical problems including: (1) the difficulty of making patients aware of their right to request and receive an accounting; and (2) the burden of producing an accounting that actually complies with the Privacy Rule.

The only way patients are informed of their right to receive an accounting is through the covered entity’s notice of privacy practices. The Privacy Rule requires notices of privacy practices to include:

a statement of the individual’s rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows: . . . [t]he right to receive an accounting of disclosures of protected health information as provided by § 164.528 . . . . 130

Thus, to the extent a covered entity’s notice of privacy practices is poorly organized, or does not clearly identify the individual’s right to request an accounting, or does not specifically explain what the patient needs to do to request an accounting, the patient will have difficulty exercising her right to request and receive an accounting of disclosures. Although many notices clearly explain patients’ rights to receive an accounting, 131 other notices simply state that patients

129. 45 C.F.R. § 164.528(b)(4)(i).
130. 45 C.F.R. § 164.520(b)(1)(iv).
131. For example, the Orthopedic Institute, P.C., clearly explains in its notice the accounting requirement (although the discussion tends towards the legalistic), and specifically describes how patients can request an accounting. Specifically, the Orthopedic Institute’s notice explains that patients have the
have "the right to receive an accounting of how and to whom your protected health information has been disclosed." To the extent the patient does not understand the definition of the term "accounting," or the patient simply overlooks the placement of the statement in the multi-page notice of privacy practices, the patient may miss her introduction to that particular right.

If a covered entity has developed a well-organized notice of privacy practices, and a patient does identify and exercise her right to request an accounting of disclosures, the covered entity actually must produce an accounting in accordance with the Privacy Rule. Thus, covered entities must be capable of tracking and documenting, in either written or electronic form: (1) information that is disclosed to third parties electronically; as well as (2) information that is physically disclosed to third parties by paper or other non-electronic means. Although many covered entities are capable of tracking information that is disclosed electronically via electronic audit trails, tracking physical disclosures of paper records may be more difficult. Moreover, when a particular patient actually requests an accounting, the covered entity must be able to search the tracking documentation and produce a list of all of the situations in which the patient's information has been disclosed, except for those disclosures not required to be included in the accounting under 45 C.F.R. § 164.528(1)(i) – (viii). Although the 2002 Final Modifications simplify the research accounting process somewhat by requiring the covered entity to identify only "[t]he date or period of time during which such disclosures . . . may have occurred," as well as a statement that individual's PHI "may or may not have been disclosed for a particular research protocol or other research activity," the research accounting process likely requires more careful attention to disclosures than is currently paid by covered entities. Indeed, covered entities and researchers have pointed to the accounting of disclosures requirement as, perhaps, the most onerous requirement set forth in

right:

To an Accounting of Disclosures. You have the right to an accounting of any disclosures of your Protected Health Information made during the six-year period preceding the date of your request beginning from April 14, 2003. However, the following disclosures will not be accounted for: (i) disclosures make [sic] for the purpose of carrying out treatment, payment or health care operations, (ii) disclosures make [sic] to you, (iii) disclosures of information maintained in our patient directory, or disclosures make [sic] to persons involved in your care, or for the purpose of notifying your family for friends about your whereabouts, (iv) disclosures for national security for intelligence purposes, (v) disclosures to correctional institutions or law enforcement officials who had you in custody at the time of disclosure, (vi) disclosure that occurred prior to April 14, 2003, (vii) disclosures made pursuant to an authorization signed by you, (viii) disclosures that are part of a limited data set, (ix) disclosures that are incidental to another permissible use or disclosure, or (x) disclosures made to a health oversight agency or law enforcement official, but only if the agency or official asks us not to account for you for such disclosure and only for the limited period of time covered by that request. The accounting will include the date of each disclosure, the name of the entity or person who receive [sic] the information and the person's address (if known), and a brief description of the information disclosed and the purpose of the disclosure. To request an accounting of disclosures, submit a written request to the Privacy Officer on the final page of this Notice.


133 45 C.F.R. § 164.528(b)(4)(i)(D).
the Privacy Rule. 134

Finally, one must ask, in light of the Belmont Report’s emphasis on respect for persons, whether the accounting requirement promotes patient autonomy by providing information to the patient that she can actually use or whether the accounting requirement withholds information necessary for the patient to make a considered judgment when there is no compelling reason to do so. 135 Remember, the 2002 Final Modifications simplified the accounting process for covered entities with respect to the tracking of research disclosures. In addition to the name and description of the protocol or research activity, the contact information of the entity that sponsored the research and the researcher to whom the information was disclosed, the Privacy Rule only requires disclosure of: (a) a brief description of the type of PHI that was disclosed; (b) the date or period of time during which such disclosures occurred, or may have occurred; and (c) a statement that the PHI of the individual may or may not have been disclosed for the particular protocol or other research activity. 136 Thus, a patient whose information has been disclosed for research activities and who requests an accounting of disclosures may not be notified of the particular information that has been disclosed, or the specific date her information was disclosed or, more importantly, whether her information actually was disclosed for a particular protocol. Without knowing whether her information actually was disclosed for a particular research protocol, one could argue that the patient’s right to receive an accounting does not empower the patient to identify recipients of her information or to determine whether the covered entity is inappropriately disclosing information. Indeed, one could argue that the patient’s right to receive an accounting, at least in the research context in which the Privacy Rule only requires the simplified accounting, only raises additional questions, not answers.

IV. ANALYSIS OF THE USE AND DISCLOSURE OF PHI FOR RESEARCH ACTIVITIES WITHOUT PATIENT AUTHORIZATION: ARE PATIENTS’ CONFIDENTIALITY INTERESTS SUFFICIENTLY PROTECTED?

Section III, above, addressed whether the Privacy Rule promotes autonomy by analyzing certain of the rights attributed to individuals who are the subject of protected health information including: (1) the general right of an individual to authorize (or refuse to authorize) a covered entity’s use or disclosure of health information for research activities; (2) the right of an individual to receive a notice of privacy practices; and (3) the right of an individual to receive an accounting of disclosures made by the covered entity. This Section IV focuses not on the rights the Privacy Rule attributes to patients but, instead, the situations in

134. See, e.g., Mary L. Durham, How Research Will Adapt to HIPAA: A View from Within the Healthcare Delivery System, 28 Am. J.L. & MED. 491, 497 (2002) (noting that some healthcare organizations will choose to deny researchers access to information instead of attempting to track information disclosures to researchers in accordance with the Privacy Rule’s accounting requirement).
135. See Belmont Report, supra note 8, at 4.
136. 45 C.F.R. § 164.528(b)(4)(i).
which the Privacy Rule permits covered entities to use and disclose PHI without patient authorization. Whereas in Section III this article asked whether the Privacy Rule sufficiently respects patients who are potential research subjects, this Section IV asks whether covered entities and institutional review boards have sufficient expertise to make decisions without patient involvement or authorization.

A. IRB OR PRIVACY BOARD APPROVAL OF A WAIVER OF OR ALTERATION TO THE OTHERWISE REQUIRED PATIENT AUTHORIZATION

HHS recognizes that "[f]or some types of research, it is impracticable for researchers to obtain written [a]uthorization from research participants."\(^\text{137}\) Accordingly, the Privacy Rule permits covered entities to use and disclose PHI for research activities without patient authorization if an IRB or an appropriately formed "privacy board" has approved a waiver of, or alteration to, the otherwise required authorization. The privacy board is a new board that is substantially similar in composition\(^\text{138}\) to an IRB but only has the authority to review requests for waivers of authorization under the Privacy Rule, not the approval of research under the Common Rule.

The Privacy Rule requires IRBs and privacy boards that review requests for waivers of, or alterations to, authorizations to determine that the following three criteria are satisfied: (1) "the use or disclosure of PHI must involve no more than a minimal risk to the privacy of individuals;" (2) "the research [cannot] practicably be conducted without the waiver or alteration; and (3) the research [cannot] practicably be conducted without access to and use of the [PHI]."\(^\text{139}\)

Interestingly, many members of the public who commented on the 2000 Final Rule argued that neither IRBs nor privacy boards should have the right to waive an individual’s right to authorize uses and disclosures of PHI for research activities. Instead, these commenters argued "that individuals always should have the right to authorize all uses and disclosures of [PHI] about themselves."\(^\text{140}\) HHS disagreed, stating that it:

> [C]arefully weighed individuals’ privacy interests with the need for identifiable health information for certain public policy and national priority


\(^{138}\) The privacy board must: (1) 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; (2) [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 such entities [(the purpose of which is to prohibit a covered entity from creating a privacy board comprised entirely of its own employees)]; and (3) . . . not have any member participating in a review of any project in which the member has a conflict of interest. 45 C.F.R. § 164.512(i)(1)(B); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,535-36 (Dec. 28, 2000). See Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,695-96.

\(^{139}\) 45 C.F.R. § 164.512(i)(2)(ii)(A)-(C).

\(^{140}\) E.g., Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,231.
purposes. The Department believes that the Privacy Rule reflects an appropriate balance . . . . However, we do believe that researchers’ ability to use protected health information without a patient’s authorization is a privilege that requires strong confidentiality protections to ensure that the information is not misused. The Department believes that the safeguards required by the final Rule achieve the appropriate balance between protecting individuals’ privacy interests, while permitting researchers to access protected health information for important, and potentially lifesaving, studies.\footnote{141}

In the above quotation, HHS does acknowledge that a researcher’s ability to use PHI without patient “authorization is a privilege that requires strong confidentiality protections to ensure that the [PHI] is not misused.”\footnote{142} The remainder of this Section IV(A) addresses the particular waiver criteria HHS selected, as well as recent findings relating to the effectiveness of IRBs, to argue that allowing an IRB to approve a waiver of, or alteration to, the authorization may not result in the application of strong confidentiality protections to research subjects’ health information.

1. The First Waiver Criterion

The first waiver criterion requires the IRB or privacy board to determine that the use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals. In analyzing the first criterion, the IRB or privacy board is asked to determine whether there exists: (a) an adequate plan to protect the identifiers from improper use and disclosure; (b) an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and (c) 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 project, or for other research in which the use or disclosure of PHI is permitted by the HIPAA Privacy Rule.\footnote{143} The Privacy Rule neither defines the ambiguous category of “pri-
vacy rights” nor the level of risk that would exceed “minimal” risk.  

Accordingly, IRBs must have sufficient time, sufficient information and sufficient analytical skills to decide, with respect to each particular research proposal, whether: (1) the researchers’ stated plan to protect identifiers is “adequate”; (2) the time proposed by the researchers for the destruction of the identifiers is sufficiently “early” (or that there is a “sufficient” health or research justification for retaining the identifiers); and (3) that the researchers have “adequately” assured that the PHI will not be reused or will not be redisclosed to any other person (or that such assurances are not required because there exists either a particular applicable law that contains an exception to this rule, or there exists sufficient oversight of the research project, or the HIPAA Privacy Rule otherwise permits a future use or disclosure of the information).

2. The Second Waiver Criterion

The second waiver criterion requires the IRB or privacy board to determine that “[t]he research could not practicably be conducted without the waiver or alteration.” Interestingly, the Privacy Rule itself does not provide any guidance regarding how IRBs or privacy boards are supposed to interpret this criterion. Buried in the depths of the preamble to the 2000 Final Rule, however, HHS explains that that “[i]nterventional research, such as most clinical trials, could not meet the waiver” criterion because a researcher who would “have direct contact with research subjects [ ] should in virtually all cases be able to seek and obtain patients’ authorization for the use and disclosure of [PHI] about themselves for the research study.” The preamble further explains that “[i]f research could practicably be conducted with authorization, then authorization must be sought. Authorization may not be waived simply for convenience.”

Unfortunately, many covered entities, researchers, and IRBs are unaware of HHS’ interpretation of the second criterion. Despite HHS’ statement of intent that IRBs and privacy boards should determine that most clinical trials (as opposed to research classified as “non-interventional,” “records”, “restrospective,” or “archival”) will not meet this criterion, many researchers are requesting IRB

144. Jennifer Kulyanych & David Korn, Use and Disclosure of Health Information in Genetic Research: Weighing the Impact of the New Federal Medical Privacy Rule, 28 A.L.J. & Med. 309, 320 (2002) (explaining that the waiver criteria "are problematic because they ask reviewers to attempt a perplexing task" including deciding "that the research presents no more than a minimal risk to the undefined and disturbingly ambiguous category of individual 'privacy rights' and [ ] to assess whether the minimal risks . . . outweigh the anticipated benefits of the research").

145. 45 C.F.R. § 164.512(i)(2)(ii)(B).

146. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,693.

147. Id. The second waiver criterion’s requirement that authorization not be waived simply for convenience is similar to an American Medical Association Code of Ethics provision which permits the waiver of informed consent for research in emergency situations only when the subject lacks capacity “to give informed consent for participation” and “the window of opportunity for intervention [is] so narrow as to make obtaining surrogate consent infeasible.” See AMERICAN MEDICAL ASSOCIATION, CODE OF ETHICS E-8.085 (1997). Again, the theory behind both the Privacy Rule’s waiver criterion and the Code of Ethics’ waiver of informed consent provision is that neither authorization nor consent can be waived for convenience.
approval for the waiver of authorization in clinical trials. Accordingly, IRBs must be trained by someone with knowledge of HHS' interpretation of the waiver criteria regarding the proper application of the waiver criteria. Alternatively, IRBs must be given sufficient time to review the hundreds of pages of preamble language to the 1999 Proposed Rule, the 2000 Final Rule, the 2002 Proposed Modifications, and the 2002 Final Modifications in order to learn how to correctly apply the various waiver criteria.

3. The Third Waiver Criterion

The third waiver criterion provides that the IRB or privacy board must determine that "[t]he research could not practicably be conducted without access to and use of the protected health information." Again, the Privacy Rule itself does not provide any guidance regarding how IRBs or privacy boards are supposed to interpret this criterion. Buried in the depths of the preamble to the 2000 Final Rule, however, HHS explains that "[i]f a researcher could practicably use de-identified health information for the research study, protected health information should not be used or disclosed for the study without . . . authorization." Accordingly, IRBs must have sufficient time, sufficient information and sufficient analytical skills to: (1) understand the information identified by the researchers as necessary to conduct the research; (2) to determine whether the research could be carried out using fewer patient identifiers; and (3) whether using fewer patient identifiers is a "practicable" solution.

4. IRBs and Privacy Boards May Not Have Sufficient Time, Information, or Analytical Skills to Perform the Tasks Delegated to Them Under the Privacy Rule

The Privacy Rule assumes that IRBs and privacy boards have sufficient time, information, and analytical skills to apply the waiver criteria and to appropriately balance research subjects' privacy interests with society's need to use and disclose PHI to carry out research. Although the HHS and FDA regulations do regulate many procedural aspects of the approval of research under the Common Rule, recent evidence suggests that IRBs may not have the ability to shoulder the additional responsibilities delegated to them under the Privacy Rule.

For example, in testimony before the United States House of Representatives on June 11, 1998, George Grob, the Deputy Inspector General for Evaluation and Inspections of HHS' Office of Inspector General, identified significant limitations relating to the ability of IRBs to review research under the Common

148. However, HHS does explain that if a particular study only 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," then an IRB could determine that this particular waiver criterion had been satisfied. See DEPT OF HEALTH & HUMAN SERVS., INSTITUTIONAL REVIEW BOARDS AND THE HIPAA PRIVACY RULE, NIH PUB. NO. 03-5428 (2003), available at http://privacyruleandresearch.nih.gov/irbandprivacyrule.asp (last visited on Nov. 16, 2003).
149. 45 C.F.R. § 164.512(i)(2)(C).
Rule. Grob specifically explained, among other things, that: (1) IRBs review too much, too quickly, with too little expertise; (2) HHS has not evaluated the effectiveness of IRBs; (3) IRBs face conflicts that threaten their independence; and (4) IRBs and their institutions provide little training for investigators and board members.

Importantly, Grob explained the threats to the adequacy of IRB review of research protocols:

IRBs across the country are inundated with protocols. We found average increases of 42 percent in initial reviews during the past 5 years at the sites we visited. Some of them are now reviewing more than 2,000 protocols annually. These IRBs are also being flooded with adverse-event reports from the multi-center trials they oversee. One IRB reported receiving an average of 200 such reports a month. These problems are not found only in large IRBs; even smaller IRBs are suffering. Several small IRB representatives told us that while the number of proposals they review is substantially fewer than at the large institutions, they often have only one staff member who is responsible for coordinating all IRB activities.

The increased workload, coupled with resource constraints, causes problems for IRBs and threatens the adequacy of their reviews. In an effort to cope, many are forced to rely on a pre-assigned reviewer to examine and summarize research plans. In some IRBs, unless one of the assigned reviewers raises a question or concern about the research, the board engages in little or no discussion at its meeting. Some IRBs have been able to increase the length of their meeting, but many others are forced to squeeze more reviews into a fixed block of time.

Science is becoming increasingly complex and many IRBs find that they lack sufficient scientific expertise on their boards or staffs to adequately assess protocols. . . . From time to time, IRBs will use consultants to fill the gap, but this can be costly and can bog down an already overburdened review process.

With respect to conflicts that threaten IRBs' independence, Grob further noted that:

In fulfilling their mission of protecting human subjects, IRBs must keep the interests of its subjects central. But, we found that many IRBs we spoke with face conflicts that could less their objectivity.

Clinical research, particularly from commercial sponsors, is an important source of revenue and/or prestige for most institutions. . . . [But] [w]e found several examples of hospital IRBs that were housed in offices of grants and contracts or of clinical research programs, the very offices

152. Id. at 4-12.
153. Id. at 7-8.
geared to bring in research dollars. Independent IRBs, which review primarily commercial research, are subject to similar pressures as several are owned by contract research organizations. Others may have equity-owners as board members reviewing protocols. Such organizational placements, while not necessarily representing a conflict, certainly can accentuate pressures on IRBs to accommodate financial interests.\textsuperscript{154}

Finally, with respect to the training provided to investigators and board members, Grob noted that:

The review process can involve complicated ethical issues and scientific questions. Because of this, the education of board members, [particularly “outside” members,] is important . . . . Nationally, in the context of the numbers of research investigators and the complexity of the ethical issues, such efforts are minimal. IRBs face significant obstacles which include not only insufficient resources, but reluctance of investigators to participate in training sessions. For new IRB members, their orientation to the role is seldom much more than a stack of materials to read and on-the-job learning.\textsuperscript{155}

Please note that the Grob’s testimony relates only to an IRB’s responsibility to review research under the Common Rule, and that Grob testified over one year before HHS published its 1999 Proposed Privacy Rule, and over four years before HHS published its 2002 Final Modifications to the Privacy Rule. However, as discussed in more detail below, to the extent IRBs shoulder additional responsibility under the Privacy Rule to approve the waiver of authorizations for the use and disclosure of information, such IRBs will still, if not to a greater extent, be asked to review too much, too quickly, with too little expertise and not enough training, and will still face conflicts that threaten their independence.\textsuperscript{156}

Grob’s testimony emphasized that IRBs are inundated with protocols, and that the increased workload, coupled with resource constraints, causes problems for IRBs and threatens the adequacy of their reviews. To the extent the same overworked IRBs now are responsible for reviewing researchers’ requests to waive authorizations for the use and disclosure of PHI under the Privacy Rule, the IRBs will face an even greater workload, and may continue to rely on pre-assigned reviewers to examine and summarize research plans. One question is whether the assigned reviewer will have sufficient time, information, and analytical skills to decide, with respect to each particular research proposal, whether: (1) the researchers’ stated plan to protect identifiers is “adequate”; (2) the time proposed by the researchers for the destruction of the identifiers is sufficiently “early” (or that there is a “sufficient” health or research justification for

\textsuperscript{154} Id. at 10-11.

\textsuperscript{155} Id. at 11-12.

\textsuperscript{156} On May 3, 2000, Grob updated his testimony and provided a status of his earlier recommendations. See Protecting Human Subjects: Status of Recommendations. Testimony before the Comm. on Gov’t Reform and Oversight, Subcomm. on Criminal Justice, Drug Policy and Human Resources (May 3, 2000) (statement of George Grob, Deputy General for Evaluation and Inspections). Grob noted that, since 1998, HHS has taken action and initiated several promising steps but, overall, few of Grob’s recommendations have been enacted. Recommendations not acted on including recommendations relating to flexibility and accountability, oversight of ongoing research, education and training of IRB members, conflicts of interest, workload pressures, and reengineering federal oversight, among other things. Id.
retaining the identifiers); (3) that the researchers have "adequately" assured that the PHI will not be reused or will not be redisclosed to any other person (or that such assurances are not required because there exists either a particular applicable law that contains an exception to this rule, or there exists sufficient oversight of the research project, or the HIPAA Privacy Rule otherwise permits a future use or disclosure of the information); (4) the information identified by the researchers is, indeed, "necessary" to conduct the research; (5) the research could be carried out using fewer patient identifiers; and (6) using fewer patient identifiers is a "practicable" solution?

A second question is whether the assigned reviewer will be appropriately trained by someone with knowledge of HHS’ interpretation of the waiver criteria regarding the proper application of the waiver criteria, or whether the assigned reviewer will be given sufficient time to review the hundreds of pages of preamble language to the 1999 Proposed Rule, the 2000 Final Rule, the 2002 Proposed Modifications, and the 2002 Final Modifications, in order to learn how to correctly apply the various waiver criteria? Or, will IRB members be given a copy of the Privacy Rule to read and told to apply what they learn when they receive their first request to waive an authorization for the use or disclosure of PHI under the Privacy Rule?

If the assigned reviewer is not capable of applying the Privacy Rule’s waiver criteria herself, will the assigned reviewer be bold enough to raise a question regarding one of these issues, thus forcing the full IRB to consider the questioned issue? Even if the full IRB considers the questioned issue, does the full IRB have the information and analytical skills to correctly apply the waiver criteria established by the Privacy Rule? In light of Grob’s testimony, and subsequent reports published by HHS’ Office of Inspector General (OIG), one could argue that the additional responsibility to review researchers’ requests for waivers of authorizations under the Privacy Rule will suffer from the same inadequate review as do current requests for review of the participation of human subjects in research under the Common Rule. In addition, to the extent that the IRBs considering requests for waivers of authorization also are housed in offices of grants and contracts, or have a large number of conflicted members, such IRBs may feel pressured to accommodate the financial pressures faced by institutions who would like to receive the revenue associated with clinical research.

5. Specific Privacy Board Problems and Possible Solutions

As discussed above, the Privacy Rule permits either an IRB or a new body, called a “privacy board,” to approve a waiver of authorization. Despite the pub-

lic’s apparent ignorance of, or infrequently noted distaste for,\textsuperscript{158} the privacy board, one possible solution is re-work the Privacy Rule’s provisions relating to privacy boards\textsuperscript{159} by increasing the number of outside members, requiring a significantly greater training of members, and routing all requests for waivers of authorizations to be reviewed by the privacy board (not the already overwhelmed IRB).

Unfortunately, the Privacy Rule’s current provisions relating to the constitution of privacy boards suffer from many of the same problems as do the Common Rule’s current provisions relating to the constitution of IRBs, including potential conflicts of interests and institutional alliances. For example, the Privacy Rule currently requires privacy boards to: (1) 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”; (2) 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 such entities”; and (3) prohibit a privacy board member from participating “in a review of any project in which the member has a conflict of interest.”\textsuperscript{160}

With respect to the second clause relating to unaffiliated members, some commenters to the 1999 Proposed Rule recommended, arguably correctly, that privacy boards be required to include more than one unaffiliated member to address concerns regarding conflicts of interest.\textsuperscript{161} However, HHS disagreed:

We disagree that privacy boards should be required to include more than one unaffiliated member. We believe that the revised membership criterion for the unaffiliated member of the privacy board, and the criterion

\textsuperscript{158} See, e.g., Stewart A. Laidlaw, et al. \textit{Genetic Testing and Human Subjects in Research}, 24 WHITTIER L. REV. 429, 438 (2002) ("[I]t is disingenuous to believe that more than a handful of institutions will choose to create a separate privacy board; most will opt to use the IRB. Therefore, the IRB will become involved in reviewing requests for release of private medical information.").

\textsuperscript{159} As currently written, the Privacy Rule requires covered entities that will disclose PHI pursuant to a waiver of authorization to obtain written documentation that an IRB or a privacy board has reviewed the research protocol. If the reviewing body is an IRB, the IRB must be established in accordance with HHS regulations set forth at 45 C.F.R. § 46.107 or equivalent regulations of another federal agency. Privacy boards, however, are new, alternative review boards authorized by the Privacy Rule to review requests for waivers of authorizations that meet the following requirements: (1) the privacy board must 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; (2) the privacy board must 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 such entities; and (3) the privacy board must not have any member participating in a review of any project in which the member has a conflict of interest. DHHS Security and Privacy Rule, 45 C.F.R. 164.512(i)(2) (2003). With respect to the third requirement, individuals who commented on the 2000 Final Rule requested clarification whether employment by the covered entity would constitute a conflict of interest, particularly if the covered entity is receiving a financial gain from the conduct of the research. HHS responded that employees of covered entities or employees of the research institution requesting PHI for research purposes are not necessarily conflicted, even if those employees may benefit financially from the research. HHS further explained, however, that there are many factors that should be considered in assessing whether a member of an IRB has a conflict of interest, including financial and intellectual conflicts. Standards for Privacy of Individually Identifiable Health Information, Final Rule, 65 Fed. Reg. 82,462, 82,696 (Dec. 28, 2000).

\textsuperscript{160} 45 C.F.R. § 164.512(i)(1)(ii)(B).

\textsuperscript{161} Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,595.
that requires that the board have no member participating in a review of any project in which the member has a conflict of interest, are sufficient to ensure that no member of the board has a conflict of interest in a research proposal under their review.\textsuperscript{162}

Thus, HHS believes that the third clause (which prohibits a member from participating in the review of any request for waiver of authorization if the member has a conflict of interest) combined with the second clause (which only requires one unaffiliated member) is sufficient to avoid situations in which privacy board members will feel forced to accommodate the financial pressures faced by institutions who would like to receive the revenue associated with clinical research. However, it is important to note that HHS interprets the third clause (which prohibits a member from participating in the review of any request for waiver of authorization if the member has a conflict of interest) \textit{not} to apply to employees of the institution:

\textit{Comment:} . . . One commenter specifically requested clarification about whether employment by the covered entity constituted a conflict of interest, particularly if the covered entity is receiving a financial gain from the conduct of the research.

Response: We understand that determining what constitutes conflict of interest can be complex. We do not believe that employees of covered entities or employees of the research institution requesting protected health information for research purposes are necessarily conflicted, even if those employees may benefit financially from the research. However, there are many factors that should be considered in assessing whether a member of an IRB has a conflict of interest, including financial and intellectual conflicts.\textsuperscript{163}

In summary, employees of covered entities or research institutions are not considered “necessarily conflicted” under the Privacy Rule, even if they benefit financially from the research. Thus, one may argue that the concerns raised by George Grob in his 1998 testimony as well as the subsequent and recent OIG reports (that IRB members reviewing research under the Common Rule may feel forced to accommodate financial pressures faced by institutions who would like to receive the revenue associated with clinical research) are equally applicable to privacy board members reviewing requests for waivers of authorization under the Privacy Rule.

In addition, although HHS believes it has addressed concerns regarding the training of privacy board members, the Privacy Rule does not specifically require even one member of the privacy board to demonstrate even a basic level of competency in privacy or security matters:

\textit{Comment:} . . . A few of these commenters also recommended that IRBs be required to have at least one member trained in privacy or security matters.

\begin{itemize}
\item \textsuperscript{162} \textit{Id.} at 82,695.
\item \textsuperscript{163} \textit{Id.} at 82,696.
\end{itemize}
Response: ... We agree, however, that the proposed rule may not have ensured that the privacy board had the necessary expertise to protect adequately individuals' privacy rights and interests. Therefore, in the final rule, we have modified one of the membership criteria for privacy board to require that the board has 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. 164

HHS' phrase "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" 165 is typically interpreted to require the inclusion of individuals with various backgrounds (e.g., scientific backgrounds, non-scientific backgrounds, legal backgrounds) as is required under the Common Rule, 166 but not individuals who have received specific training in privacy and confidentiality matters.

One additional idea is to require privacy boards to be accredited by something called a "Protected Health Information Use and Disclosure Accreditation Program," which would accredit only those privacy boards that could demonstrate their ability to: (1) understand the HIPAA Privacy Rule's provisions regarding the waiver of authorization; (2) understand and apply the Rule's standards for protecting PHI from inappropriate use and disclosure; (3) determine whether a researchers' stated plan to protect identifiers is "adequate"; (4) determine whether the time proposed by the researchers for the destruction of the identifiers is sufficiently "early" (or that there is a "sufficient" health or research justification for retaining the identifiers); (5) determine whether a researcher has "adequately" assured that the PHI will not be reused or will not be redisclosed to any other person (or that such assurances are not required because there exists

164. Id. at 82,695 (emphasis added).
165. Id.
166. For example, the Common Rule, as set forth in HHS' regulations at 45 C.F.R. Part 46, specifically require members with varying backgrounds:

(a) Each IRB shall have at least five members, with varying backgrounds to promote complete and adequate review of research activities commonly conducted by the institution. The IRB shall be sufficiently qualified through the experience and expertise of its members, and the diversity of the 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. In addition to possessing the professional competence necessary to review specific research activities, the IRB shall be able to ascertain the acceptability of proposed research in terms of institutional commitments and regulations, applicable law, and standards of professional conduct and practice. The IRB shall therefore include persons knowledgeable in these areas. If an IRB regularly reviews research that involves a vulnerable category of subjects, such as children, prisoners, pregnant women, or handicapped or mentally disabled persons, consideration shall be given to the inclusion of one or more individuals who are knowledgeable about and experienced in working with these subjects.

(b) Every nondiscriminatory effort will be made to ensure that no IRB consists entirely of men or entirely of women, including the institution's consideration of qualified persons of both sexes, so long as no selection is made to the IRB on the basis of gender. No IRB may consist entirely of members of one profession.

(c) Each IRB shall include at least one member whose primary concerns are in scientific areas and at least one member whose primary concerns are in non-scientific areas.

either a particular applicable law that contains an exception to this rule, or there exists sufficient oversight of the research project, or the HIPAA Privacy Rule otherwise permits a future use or disclosure of the information; (6) determine whether the information identified by the researcher is, indeed, "necessary" to conduct the research; (7) determine whether the research could be carried out using fewer patient identifiers; and (8) determine whether using fewer patient identifiers would be a "practicable" solution.

The idea for a "Protected Health Information Use and Disclosure Accreditation Program" is supported by recent findings published by the Institute of Medicine (IOM). Specifically, following the death of 18-year-old Jesse Gelsinger during a 1999 clinical study at the University of Pennsylvania and other similar incidents at other research centers that highlighted growing problems such as conflicts of interest, inadequate safety monitoring and oversight, and insufficient communication with research subjects, HHS commissioned the IOM to develop a report addressing whether research subjects' health and well-being are protected. "To accomplish its purpose, the IOM assembled the Committee on Assessing the System for Protecting Human Research Participants" (Committee), and asked the Committee "to conduct the study in two phases:" (1) "an immediate study of the possible value of accrediting human research protection programs;" and (2) "a comprehensive review of the present system for protecting human research participants," as well as recommendations for strengthening the system.167

On April 17, 2001, the IOM reported its findings relating to the first phase in Preserving Public Trust: Accreditation and Human Research Participant Protection Programs.168 In this initial report, the Committee explained how it "reviewed and considered available draft standards developed independently by Public Responsibility in Medicine and Research (PRIM&R)," as well as the National Committee for Quality Assurance (NCQA), which is under contract to the U.S. Department of Veterans Affairs (VA).169 The Committee then provided "a series of findings and recommendations for using performance standards to improve the system for protection of human research participants."170 Specifically, the Committee found that "the standards proposed by the NCQA for VA facilities" appeared "promising for use in the accreditation of VA facilities," and that "pilot accreditation programs should start from the accreditation standards and processes proposed by NCQA for VA facilities and be adapted for use in other organizational contexts by NCQA or other accreditation bodies."171 The Committee further recommended that:

(1) the organizations formulating accreditation standards and carrying out


169. Id. at 1.

170. Id.

171. Id. at 2.
the accreditation process be independent, nongovernmental organizations; (2) the formulation of accreditation standards, the accreditation process, and human research participant protection program operations directly involve research participants; and (3) the accreditation process accommodate organizations involved in research beyond the traditional models of academic health centers and VA facilities and be appropriate for research methods other than clinical research.\footnote{172}

The Committee ultimately concluded that "[o]nly by experience gained through pilot testing can the value that accreditation adds to the current regulatory system, in terms of enhanced protection of human research participants, be adequately assessed."\footnote{173} Interestingly, one of the Committee’s specific recommendations, to articulate sound goals within accreditation standards, states that one goal of accreditation standards should be "independent review of research by a board knowledgeable about protection standards and the fields of research being reviewed."\footnote{174}

The following year, on October 3, 2002, the IOM reported its findings relating to the second phase in a document entitled \textit{Responsible Research: A Systems Approach to Protecting Research Participants}, which contains a series of recommendations including protecting all research participants, refocusing the mission of institutional review boards, recognizing participant contributions and providing access to information including revitalizing informed consent, and continuously improving performance.\footnote{175} A theme central to the IOM’s report was the concept of the “Human Research Participant Protection Program,” or HRPPP, a term adopted by the IOM to embrace a set of complementary elements and activities necessary to ensure that comprehensive protection is afforded to every research participant. Importantly, the IOM’s report explains that:

As the demands on the research oversight system have grown, so has the reliance on IRBs to accomplish all protection tasks. This is a disservice to research participants, because IRBs... find it exceedingly difficult to both manage the increasing volume of protocol actions and ensure the safety of research volunteers... \footnote{176}

The Director of the Office for Human Research Protections (OHRP) also has endorsed voluntary accreditation of IRBs as a helpful means of assuring quality and regulatory compliance with respect to the review of research under the Common Rule.\footnote{177} IRB accreditation programs have been further endorsed by the General Accounting Office, HHS’ Office of Inspector General, and the National Bioethics Advisory Commission.\footnote{178}

\begin{itemize}
\item \footnote{172} \textit{Id.}
\item \footnote{173} \textit{Id. at 2.}
\item \footnote{174} \textit{Id. at 12.}
\item \footnote{175} \textit{INSTITUTE OF MEDICINE, RESPONSIBLE RESEARCH: A SYSTEMS APPROACH TO PROTECTING RESEARCH PARTICIPANTS} 1-5 (2003), available at http://www.nap.edu/books/0309084881/html/.
\item \footnote{176} \textit{Id. at 8-9.}
\item \footnote{177} \textit{See Robert J. Kenney, Jr. et al., FEDERAL RESEARCH COMPLIANCE: BIOMEDICAL & RESEARCH INTEGRITY ISSUES, 02-04 BRIEFING PAPERS} 1, 6 (March 2002) (citing \textit{IRB Accreditation, Certification Advised by OHRP Director Koski, THE BLUE SHEET} 9 (Sept. 20, 2000)).
\item \footnote{178} \textit{See id. at 6 \& n.44.}
\end{itemize}
Important to the instant discussion, the new Association for Accreditation of Human Research Protection Programs (AAHRPP) offers voluntary accreditation (similar to JCAHO’s accreditation of hospitals and other types of health care facilities) for IRBs that review research under the Common Rule. Indeed, the AAHRPP has adopted nine principles for accreditation of IRBs\(^\text{179}\) and five domains\(^\text{180}\) of accreditation standards\(^\text{181}\) that could be revised to include a greater or additional focus on the use and disclosure of PHI for research activities under the Privacy Rule. One of the accreditation standards, Standard II-6, requires IRBs to systematically evaluate “the protection of privacy and confidentiality in [the] proposed research.”\(^\text{182}\) However, this standard is very general and only requires: (1) “written policies and procedures to evaluate the proposed arrangements for protecting the privacy of research participants during and after their involvement in the research; (2) the following of “written policies and procedures to evaluate proposed arrangements for protecting the confidentiality of identifiable data, when appropriate, during and after the conclusion of the investigation.”\(^\text{183}\) This standard could be substantially revised to include more specific criteria relating to the composition of the privacy board, to require substantial initial and continuing education of the board’s members with respect to the Privacy Rule’s waiver criteria and the application of such criteria to various research proposals.

In conclusion, one possible solution is re-work the Privacy Rule’s provisions relating to privacy boards by increasing the number of outside members, requiring significantly greater training of members, and routing all requests for waivers of authorizations to the privacy board, not the already overwhelmed IRB. Increasing the number of outside members arguably may minimize members’ desire to accommodate financial pressures faced by institutions who would like to receive the revenue associated with clinical research. An additional idea is to amend the privacy board membership requirements to include a patient advocate who may help focus the privacy board’s attention to matters of patient privacy.\(^\text{184}\) Requiring greater training of privacy board members would privacy board members to correctly apply each of HHS’ waiver criteria to individual requests for authorization waivers. Finally, requiring privacy boards to be accredited arguably would help ensure that privacy board members have received proper training and are sufficiently capable of focusing on matters of privacy and


\(^{180}\) Id. The AARPP’s five domains include the organization, research review unit, investigator, sponsor, and participant. Id.


\(^{182}\) Id.

\(^{183}\) Id.

\(^{184}\) Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,696 (Dec. 28, 2000). The Privacy Rule currently does not require patient advocates to be included as members of a privacy board. However, the Privacy Rule does permit patient advocates to be included if they meet the membership criteria set forth at 45 C.F.R. § 164.512(i).
confidentiality.

B. RESEARCH ON DECEDENT’S INFORMATION

As discussed in Section II, the “research on decedents’ information” exception allows covered entities to use or disclose PHI about decedents for research purposes without obtaining patient authorization from a personal representative of the decedent if the covered entity obtains from the researcher:

(1) a representation that the use or disclosure is sought solely for research on the protected health information of decedents; (2) documentation, at the request of the covered entity, of the death of such individuals; and (3) a representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.\(^\text{185}\)

The preamble to the Privacy Rule explains that this exception is modeled after the Common Rule, which does not require IRB review of research on decedents’ information because the Common Rule does not consider deceased persons “human subjects.”\(^\text{186}\)

Interestingly, the American Medical Association’s (AMA’s) Code of Ethics explains, with respect to the confidentiality afforded to medical information postmortem, that “[a]ll their strongest, confidentiality protections after death would be equal to those in force during a patient’s life.”\(^\text{187}\) However, the AMA does recognize that “[d]isclosure of medical information postmortem for research and educational purposes is appropriate as long as confidentiality is maintained to the greatest possible degree by removing any individual identifiers.”\(^\text{188}\)

Thus, even though the AMA contemplates using decedents’ information for research without prior authorization of the decedent or, now, the decedent’s legal representative, the AMA requires the removal of individual identifiers, whereas the relevant exception under the Privacy Rule only requires satisfaction of the three representations identified in the preceding paragraph, but not the removal of identifiers.

Thus, using the records of deceased persons for research activities is not without controversy. For example, one individual who commented on the 1999 Proposed Rule stated that she extensively used information relating to decedents for research, and that any restrictions were likely to impede her research efforts.\(^\text{189}\)

On the other hand, concerns regarding the use and disclosure of genetic and other hereditary information are raised even when research is conducted on the information of decedents. Although PHI relating to a decedent does not necessarily identify living relatives who have the same name of the decedent, living


\(^{186}\) Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. at 82,701.


\(^{188}\) Id.

\(^{189}\) Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. at 82,701.
relatives could be identified and suffer the same harm as if their own medical records were used or disclosed for research purposes.

The following example, although not involving a decedent, highlights the problem: a woman requested DNA testing for Huntington’s Disease (HD), which is a neurodegenerative disorder characterized by involuntary movement, progressive dementia, and mood disturbance. Over time, HD patients typically lose their ability to speak, and synchronized breathing and swallowing become progressively more difficult. The woman wanted to undergo testing so that she could plan for her future and make career decisions. Although the woman normally would be eligible for testing, she had an identical twin, who did not want to be tested because she felt that she would not be able to face a positive test result. The twin who wanted to be tested stated that she would keep her results confidential. Accordingly, the physician allowed the first twin to be tested. Unfortunately,

\[\text{[o]nce [the tested twin] was informed of the results -- that there was a high probability that she would have Huntington’s disease—the information spread quickly throughout the entire family. This meant that the twin who did not want to know her genetic status was now faced with the unwelcome knowledge that she too would probably have the disease . . . . When information was given to one twin, the other irretrievably lost the freedom to decide.}\]

In summary, at least in the context of PHI that contains genetic information, the twin who did not want to be tested suffered a loss of autonomy because although she stated her decision that she did not want to be tested, her choice was, ultimately, unrealized. Although the twin who did want to be tested was not deceased, a similar situation could occur in which PHI of a decedent is used or disclosed for research or other purposes and the PHI becomes known by a family member who carries the same genetic trait.

C. Reviews Preparatory to Research

The “reviews preparatory to research” exception allows covered entities to use and disclose PHI without patient authorization if a researcher will be reviewing the information for a purpose “preparatory to research.” This exception requires the covered entity to obtain from the researcher representations that:

- (A) Use or disclosure is sought solely to review [PHI] as necessary to prepare a research protocol or for similar purposes preparatory to research;
- (B) No [PHI] is to be removed from the covered entity by the researcher in the course of her review; and
- (C) The [PHI] for which use or access is sought is necessary for the re-

191. Id. at 673.
192. Id. at 674 (citing Catherine A. Hayes, Genetic Testing for Huntington’s Disease—A Family Issue, 327 NEW ENG. J. MED. 1449, 1450 (1992)).
search purposes.\footnote{DHHS, Security and Privacy, 45 C.F.R. § 164.512(i)(1)(ii) (2003).}

HHS also explains that this exception is modeled after the Common Rule provision which exempts from coverage:

research involving the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publicly available, or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or indirectly through identifiers linked to the subjects.\footnote{Id.}

HHS stated its intent that this exception would be used to permit covered entities to use and disclose PHI to assist in the development of a research hypothesis and to aid in the recruitment of research participants. Apparently, industry groups had expressed concern that the 1999 Proposed Rule would prohibit physicians from using patient information to recruit subjects into clinical trials and recommended that researchers continue to have access to hospitals’ and clinics’ patient information in order to recruit patients for studies.\footnote{Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. at 82,537.} HHS agreed:

[T]his provision permits covered entities to use and disclose protected health information for these preliminary research activities without individual authorization and without documentation that an IRB or privacy board has altered or waived individual authorization.\footnote{Id.}

To satisfy this exception, please note that: (i) the review of the PHI must be conducted in such a manner that only de-identified protected health information is recorded by the researcher; and (ii) no PHI can be removed from the physical premises of the covered entity.\footnote{Id.} HHS interprets these provisions as allowing a covered entity to permit a researcher who is an employee or a member of the covered entity’s workforce to use protected health information to contact prospective research subjects while on the physical premises of the covered entity.\footnote{Id.} However, the inability to remove PHI from the premises of the covered entity would appear to prohibit a covered entity from disclosing PHI to a researcher who is not an employee or a member of the covered entity’s workforce for purposes of recruiting research subjects unless the covered entity itself contacts the potential research subjects from the covered entity’s premises. Stated another way, this exception would not permit a researcher who is not employed by the covered entity or who is not a member of the workforce of the covered entity to copy patients’ names and addresses, take such contact information back to the researcher’s office, clinic, or home institution, and later prepare written communications (or contact such individuals by telephone) and request the patients’ participation in research.

\footnote{DEP’T OF HEALTH & HUMAN SERVS., PROTECTING PERSONAL HEALTH INFORMATION IN RESEARCH: UNDERSTANDING THE HIPAA PRIVACY RULE 17, NIH PUB. NO. 03-5388 (2003) (emphasis in original).}
D. USING AND DISCLOSING LIMITED DATA SETS PURSUANT TO DATA USE AGREEMENTS

Finally, an additional option is to encourage researchers to use limited data sets of information for their research activities, which is permitted once the researcher enters into a simple data use agreement with the covered entity. As discussed in Section II, a limited data set is PHI that excludes most, but not all, of the identifiers listed under the de-identification safe harbor including, but certainly permits the use of any health information including information relating to the patient’s diagnosis, condition, and treatment, as well as identifiers including dates relating to a patient (e.g., dates of service, admission, or discharge; date of birth; date of death) and information relating to the town or city, state, and five-digit zip code of the patient, his or her employer, and the patient’s household members. Thus, information relating to the asthmatic condition of a child born on January 1, 2004, who lives in Houston, Texas, 77002, could be included within the limited data set, even though that same information would not constitute de-identified information under the de-identification safe harbor.

HHS adopted the limited data set exception in the 2002 Final Modifications. Accordingly, much of the medical literature addressing the topic that was published before August of 2002 simply berates the stringent de-identification safe harbor because that safe harbor would not allow the use of information identifying a patient’s age or date of birth, as well as the area in which the patient lived. These medical articles argued that the de-identification standard would prohibit most epidemiologic, health services, and other population-based research, which requires identification of each subject’s geographical information, as well as certain dates and ages.

Thus, the 2002 Final Modifications’ limited data set option appears to be a nice compromise between the stringent de-identification safe harbor and the authorization requirement. In addition, because most direct identifiers must be removed from the limited data set that will be used and disclosed by the researcher, patient concerns regarding re-identification should be minimized.

V. CONCLUSION

One of the ethical principles set forth in the Belmont Report requires the

---

199. Remember, the preamble to the 2002 Final Modifications does not prescribe the form of the data use agreement, and permits the agreement to be a formal contract, an informal memorandum of understanding or, a confidentiality-type agreement.

200. DHHS, Security and Privacy, 45 C.F.R. § 164.514(e)(2) (2003). See also Standards for Privacy of Individually Identifiable Health Information, Final Rule, 67 Fed. Reg. at 53,235 (“Therefore, as part of a limited data set, researchers and others involved in public health studies will have access to dates of admission and discharge, as well as dates of birth and death for the individual. . . .” and “[T]he limited data set may include the five-digit zip code or any other geographic subdivision, such as State, county, city, precinct, and their equivalent geocodes, except for street address.”).

201. See e.g., Kulychny and Korn, supra note 23 (noting that “[e]ven the American Medical Association, which generally supports the Privacy Rule, views this standard as a disincentive for researchers to seek and covered entities to provide de-identified data and urges that the list of identifiers be pared dramatically”).
maximization of possible benefits and the minimization of possible harms. Similarly, this conclusion focuses on whether the Privacy Rule’s research provisions strike a balance between increasing patient autonomy and confidentiality and imposing administrative burdens on covered entities.

Many commentators have generally noted that the Privacy Rule is so complex that its costs in terms of compliance outweigh any possible benefit. For example, an article published in The New England Journal of Medicine the week before the general compliance date for the Privacy Rule stated the following:

I believe the new regulations are excessively and unnecessarily complex and often more attuned to making sure that businesses and government agencies get access to medical records than to the protection of patients’ privacy... The implementation of the new HIPAA privacy regulations is likely to be costly, inconsistent, and frustrating to both physicians and patients.

Critics of the Privacy Rule’s research provisions continue to argue that the provisions will discourage entities from making medical records available for research and will diminish the pace and volume of research. Others argue that such critics are “overly alarmist,” but point out that it is “strange” to see the federal government focusing so much attention on protecting the medical records and privacy of human subjects when the autonomy, health, and safety of human subjects is what needs and deserves greater protection in the research setting. Still others argue that “[w]e are unaware of any documented evidence that research conducted under the supervision of an IRB constitutes a serious threat to privacy or confidentiality,” and argue that HHS should modify the Privacy Rule to permit the use and disclosure of PHI without patient authorization if the research is conducted under the supervision of an IRB in satisfaction of the Common Rule. Indeed, the HIPAA statute, enacted in 1996, required HHS to consult with the National Committee on Vital and Health Statistics (NCVHS) when developing recommendations to Congress for what was supposed to be privacy legislation. In response, the NCVHS issued a report approved on June 25, 1997, which stated that “testimony identified no instances of breaches of confidentiality resulting from researcher use of records.”

A review of Section III of this article results in the conclusion that although the HIPAA Privacy Rule appears to promote autonomy by attributing a number of important rights to individuals who are the subject of health information, the overwhelming number and complex nature of the regulations significantly limits the ability of many covered entities to understand exactly what the Rule requires.

204. id. at 1489 (citing Jennifer Kulynych and David Korn, The New Federal Medical-Privacy Rule, 347 NEW ENG. J. MED. 1133-34 (2002)).
205. id.
206. See, e.g., Kulynych & Korn, supra note 23, at 203.
207. NAT’L COMMITTEE ON VITAL & HEALTH STATS., HEALTH PRIVACY AND CONFIDENTIAL RECOMMENDATIONS OF THE NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS 8 (1997).
In addition, although neither the authorization requirement, the notice of privacy practices requirement, nor the accounting requirement impede research (especially since the authorization can be integrated into the informed consent document required by the Common Rule), the Privacy Rule exacerbates covered entities’ and researchers’ reliance on authorizations, notices, and accountings—which are just forms. These forms simply add to the administrative and bureaucratic cloud surrounding research, without also increasing patients’ understanding of their rights or the protection of their information. Obtaining authorization for the use and disclosure of PHI for research activities, or distributing a notice of privacy practices, or providing a list of an accounting of disclosures, like obtaining a patient’s informed consent to participate in research under the Common Rule, should be an ongoing process that focuses not on the written form, notice, or list, which are static disclosure events, but rather on a series of dynamic and appropriately targeted conversations between the patient and the covered entity and/or researcher. Neither the discussion with the patient, nor the form, notice, or accounting should be obscured by complicated language intended to protect the covered entity and researchers from liability. Instead, the entire process should focus on making patients clearly understand how their information will be used for research activities, the risk that their information could be redisclosed by researchers and other recipients of their information, and the potential benefits of the research. In summary, obtaining signed authorization forms, distributing written notices, and providing accountings under the Privacy Rule does not appear to improve a patient’s ability to make an informed decision regarding the use and disclosure of her information for a particular research activity.

A review of Section IV of this article further demonstrates that IRBs are asked to review too much, too quickly, with too little expertise and not enough training, and that IRBs face conflicts that threaten their independence. If the Privacy Rule is going to ask IRBs to shoulder the additional burden of reviewing and approving requests for waivers of authorizations, arguably such reviews will suffer from the same inadequacy that is characteristic of reviews of research under the Common Rule. Accordingly, one solution is for covered entities to create separate bodies called privacy boards, provide sufficient training to board members regarding the correct application of the Privacy Rule’s waiver criteria, and route all requests for authorization waivers through the privacy board (not the institution’s overwhelmed IRB). An additional solution is to require accreditation of privacy boards. Existing accreditation standards that apply to IRBs that review research under the Common Rule could be revised to include more specific criteria relating to the composition of the privacy board and initial and continuing education of the board’s members.

Looking beyond IRB or privacy board approval, the Privacy Rule does permits the use and disclosure of PHI for research without authorization in situations involving research on decedents’ information and in situations involving a review of information in preparation for research. However, these exceptions raise their own privacy issues and, generally, are of limited applicability. One additional solution, however, may be to encourage researchers to use limited
data sets of information for their research activities, which the Privacy Rule permits once the researcher has entered into a simple data use agreement with the covered entity. Because any health information, including information relating to the patient’s diagnosis, condition, and treatment, as well as identifiers including dates relating to a patient (e.g., dates of service, admission, or discharge; date of birth; date of death) and information relating to the town or city, state, and five-digit zip code of the patient, his or her employer, and the patient’s household members can remain in the information used and disclosed by the researchers, researchers will be able to continue to engage in some epidemiologic, health services, and other population-based research without prior patient authorization or satisfaction of another exception.\textsuperscript{208} On the other hand, because direct identifiers like the patient’s name, social security number, and street address are removed from the information, patient concerns regarding re-identification are minimized.

Finally, looking beyond the Privacy Rule, it is important to note that physicians who engage in research have an independent ethical obligation to avoid mere reliance on IRB or privacy board approval or another exception to the authorization requirement under the Privacy Rule if such reliance would not be in the best interests of their patients.\textsuperscript{209} The existence of an independent obligation bearing on the conduct of individual physicians is recognized in American professional ethics guidelines. For example, the American Medical Association’s (AMA’s) Principles of Medical Ethics provides that physicians shall “regard responsibility to the patient as paramount.”\textsuperscript{210} The AMA’s Code of Ethics further provides that “a physician is ethically required to . . . hold[] the best interests of the patient as paramount,”\textsuperscript{211} and that the “[a]voidance of real or perceived conflicts of interest in clinical research is imperative if the medical community is to ensure objectivity and maintain individual and institutional integrity.”\textsuperscript{212} Because the Privacy Rule’s research provisions are so onerous and do rely so heavily on static disclosure events, a physician who complies with her own independent ethical obligations may best be able to balance protecting patient confidentiality, promoting individual autonomy, and encouraging medical research.

\textsuperscript{208} See id. (noting that “[e]ven the American Medical Association, which generally supports the [Privacy Rule], views this standard as a disincentive for researchers to seek and covered entities to provide de-identified data and urges that the list of identifiers be pared dramatically”).

\textsuperscript{209} See, e.g., Trudo Lemmens and Paul B. Miller, The Human Subjects Trade: Ethical and Legal Issues Surrounding Recruitment Incentives, 31 J.L. MED. & ETHICS 398, 406-07 (Fall 2003) (explaining that researchers, physicians, and others involved in research are obliged to familiarize themselves with research ethics guidelines and to treat these as binding professional standards governing their personal involvement in all research-related activities).

\textsuperscript{210} AMERICAN MEDICAL ASSOCIATION, PRINCIPLES OF MEDICAL ETHICS VIII (June 2001).

\textsuperscript{211} AMERICAN MEDICAL ASSOCIATION, CODE OF ETHICS E-10.015 (2001).

\textsuperscript{212} Id. at E-8.031 (2002).