Annu. Rev. Med. 2006. 57:575–90
doi: 10.1146/annurev.med.57.121304.131257

First published online as a Review in Advance on Nov. 7, 2005

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) PRIVACY RULE: Implications for Clinical Research

Rachel Nosowsky[1] and Thomas J. Giordano[2]
[1]*Office of the Vice President and General Counsel, University of Michigan, Ann Arbor, Michigan 48109; email: nosowsky@umich.edu*
[2]*Department of Pathology, University of Michigan Health System, Ann Arbor, Michigan 48109; email: giordano@umich.edu*

Key Words health privacy, medical privacy, confidentiality, human subjects, patient rights

■ **Abstract** In the short time since it became effective for health care organizations, a privacy regulation issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) has had a significant adverse impact on the conduct of clinical research in the United States, without a substantial corresponding increase in privacy protection for research participants. Some of the problems associated with HIPAA have been resolved through revisions since the regulation's initial promulgation in December 2000, and other problems can be addressed by better educating health care providers and researchers about its requirements and available alternatives for compliance; however, considerable structural challenges remain. These constitute substantial barriers to research and resulting medical advances. Additional revisions to HIPAA based on the principles and trade-offs reflected in the Common Rule—which responsibly balances an individual's interest in privacy protection with the public interest in gaining knowledge through biomedical research—can go a long way to remedying remaining flaws in the system.

INTRODUCTION

Regulatory Framework

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996, principally to allow chronically or seriously ill individuals to change jobs without fear of losing health coverage because of "preexisting conditions" exclusions in their health benefits policies. The law included other health care reform provisions, among them measures intended to improve operation of the health care system and reduce administrative costs through "administrative simplification."

While the legislation was being drafted and its merits debated in Congress, privacy advocates voiced concerns that standardization mandates spelled out in the administrative simplification rules would create substantial risks to privacy. Congressional attempts to address these misgivings in the final HIPAA legislation and in subsequent years fell short, however. Lawmakers' efforts to reach consensus on an overall national privacy policy eventually broke down over central issues such as whether and to what extent federal law should pre-empt more restrictive state laws. As a result, it was finally left to the Secretary of the Department of Health and Human Services (HHS) to promulgate privacy regulations under HIPAA.

The final regulation (1), which is also known as the Privacy Rule, severely restricts the circumstances under which individually identifiable health information may be used and disclosed. It does not apply directly to research, but it does specify the limited circumstances under which health care providers and others may use or disclose patient information—the raw materials necessary to conduct much biomedical and health services research.

Privacy and Research

In developing the Privacy Rule, HHS declined to integrate or harmonize HIPAA with the existing regulatory framework for human subjects research, known as the Common Rule, on the theory that HIPAA was not intended to regulate research and that the two regulations could and should operate independently.

For more than two decades, the principles articulated in the report of The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (the Belmont Report) and reflected in the Common Rule—respect for persons, beneficence, and justice—have guided federally supported human-subjects research. These principles require, among other things, that prospective participants in research studies be provided with sufficient information to make an informed choice to participate in research or not, that the choice be voluntary and uncoerced, and that the risks and benefits of participation be reasonably shared through equitable recruitment and selection of subjects. The Common Rule specifies that before approving a proposed study, an Institutional Review Board (IRB) must determine that the protocol contains "adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data." Thus, researchers and IRBs operating under the Common Rule over these many years have gained extensive experience in identifying and addressing privacy concerns. Moreover, as alarmed as Americans remain about medical privacy and unauthorized use of their health information, they also overwhelmingly agree that the "United States should be a world leader in medical and health research" (2).

With these competing interests in mind, HHS's National Committee on Vital and Health Statistics (NCVHS) observed in a 1997 report on medical privacy that "[a]ny Administration position [on privacy] must properly balance the important and well-established interests of patients in the protection of their health information against the legitimate needs of the health care system to provide and pay for health care in an efficient, effective and fair manner and to support the responsible

use of health records for public health and health research" (3, 4). With respect to research in particular, NCVHS concluded: "Patient privacy interests are adequately protected by independent review of research protocols, the earliest possible removal of identifiers, prohibitions against use of research records for actions against patients, and strict penalties against researchers who violate the rules."

When it finally issued its regulation, HHS expressed its belief that HIPAA will facilitate, rather than burden, research: "The Privacy Rule both permits important research and, at the same time, encourages patients to participate in research by providing much needed assurances about the privacy of their health information" (5). Anecdotal reports suggest otherwise. For example, researchers regularly report that HIPAA-mandated authorization discourages prospective subjects from participating in clinical trials by including language to the effect that identifiable health information, once disclosed to researchers, will no longer be protected by the regulation. Recent published literature bears out this anecdotal evidence and more broadly indicts HHS for failing to strike a workable balance between competing individual and public interests. HIPAA, it is charged, imposes largely illusory privacy protections to the detriment of biomedical research and the medical advances that are supposed to flow from it.

UNDERSTANDING HIPAA AND ITS RELATIONSHIP TO THE COMMON RULE

A detailed description of the provisions of the Privacy Rule and its current interpretation is beyond the scope of this article. Such information is available through numerous sources, including the HHS Office for Civil Rights' *HIPAA: Medical Privacy-National Standards to Protect the Privacy of Personal Health Information*, at http://www.hhs.gov/ocr/hipaa/, and the National Institutes of Health's *HIPAA Privacy Rule: Information for Researchers*, at http://privacyruleandresearch.nih.gov.

Briefly, though, HIPAA applies to all "protected health information" (PHI), defined as information, including demographic information, (*a*) collected from an individual; (*b*) created or received by a health care provider, health plan, or a health care clearinghouse (collectively a "covered entity"); and (*c*) "relating to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." To be considered PHI, the information must directly identify an individual, or there must be a reasonable basis to believe the information could be used to identify the individual.

The Privacy Rule describes and classifies specific activities that require use or disclosure of PHI, assigning different levels of protection by category. Normally, HIPAA requires covered entities to obtain a person's written authorization before using or disclosing his PHI. PHI may be used or disclosed without authorization and with few restrictions for activities deemed by federal regulators to be central to the provision of and payment for health care and related services—"treatment,"

"payment," and "health care operations." (The terms in quotation marks are narrowly defined and specifically exclude research, defined, as in the Common Rule, as a "systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.") An earlier generation of health information privacy laws provided broad exceptions for additional important activities, including research. Although HIPAA likewise permits covered entities to use or disclose PHI without authorization for research, it does so only under very limited circumstances and subject to a complex set of restrictions, described in detail below. Moreover, uses and disclosures of PHI for these disfavored activities are subject to additional administrative requirements, including a difficult-to-implement requirement to track and account for disclosures not specifically authorized by patients. All uses and disclosures not explicitly permitted under the regulation are prohibited.

HIPAA IN PRACTICE: REPORTED IMPACT

Long before HHS first issued the Privacy Rule in December 2000, and during a reopened comment period leading to its revision in August 2002, individuals and organizations around the country raised concerns that the regulation would have a negative and lasting effect on clinical trials and other human research (1, 6–8). Some of these concerns were addressed before final implementation of the regulation in April 2003, but many were not. Today, the regulation remains ambiguous and complex, penalties for noncompliance are severe (9, 10), and implementation has resulted in both intended and unintended limitations on access to information and prospective research participants. And yet it is difficult to detect any significant gain for privacy protection in the area of human research.

Some advocates defending against criticism of HIPAA's impact on research have argued that many researchers are not covered entities, and therefore need not comply with the Privacy Rule. Yet this does not mean they are unaffected by HIPAA requirements. Covered entities who control the information that is necessary to perform research are regulated by HIPAA. And although many institutions and investigators arguably have been overly conservative in their interpretation of and efforts to comply with the Privacy Rule (11), even a very aggressive interpretation cannot adequately address all of the structural problems inherent in HIPAA that continuously have undermined important research efforts. According to surveys conducted by the American Association of Medical Colleges (AAMC) and the National Cancer Advisory Board (NCAB), these problems include "negative impact on informed consent process," "confusion of subjects," "negative impact on subject recruitment," "possible increase in selection bias," "alteration or abandonment of research direction," "inability or impaired ability to collaborate," "additional regulatory burdens on research process already struggling under the weight of extensive regulation," "increased costs," and "multiple inconsistent interpretations of HIPAA requirements across institutions, because of its inherent ambiguities" (12).

"In short," according to NCAB, "respondents reiterated their belief that HIPAA is severely derailing 'the progress of knowledge"' (13). These problems are unlikely to be addressed without material revisions to the regulations (14).

Subject Recruitment and Selection

Virtually every study measuring changes in participation rates pre- and post-HIPAA has found striking declines. Where these declines have been further examined, resulting bias in data sets can be clearly discerned. Some commentators have dubbed this an unintended consequence of the regulation, but these effects were easily foreseeable (15, 16) and stem from HHS's conscious policy decision to decisively tilt the scales in favor of individual privacy regardless of the detriment to communal progress.

Researchers' experience in an ongoing preeclampsia study highlights problems both with the regulation itself and with its inconsistent and often overly conservative interpretation at different institutions (2). The study began in 1997. In 2002, it was shut down for four months while the maternity hospital where subjects were recruited determined how to implement HIPAA-mandated protections. Between April 2003 and September 2003, the institution refused to grant a waiver permitting review of medical records to identify patients who might be eligible for participation in the study; instead, only records of women who had enrolled in a research registry (constituting only 10% of female patients) were made available for review. In October 2003, the hospital's IRB began accepting waiver applications, but required permission from prospective subjects' providers before researchers approached the subjects. Finally, in June 2004, when the hospital merged with another institution, the waiver was again withdrawn. The study suffered a precipitous decline in recruitment during these periods: 12.4 women/week pre-HIPAA (95% CI 11.6–13.2), 2.5 women/week without a waiver (95% CI 2.0–3.0), 5.7 women/week with a waiver (95% CI 4.8–6.6), and 3.3 women/week after retraction of the waiver (95% CI 2.6–4.0).

Unfortunately, this narrative is not unique (17–20). More recently, researchers at the University of Michigan measured participation rates in two cohorts of patients eligible to participate in a local study of acute coronary syndrome (21). The first group included patients recruited through a telephonic consent process before HIPAA became effective; the second included patients recruited through a written informed-consent process administered by mail after HIPAA. In that study, consent for follow-up declined from 96.4% to 34.0% ($p < 0.01$). Moreover, the characteristics of those who agreed to participate in the registry through the written informed-consent process were markedly different from those of individuals who declined: Participants were older, more likely to be married, and had lower mortality rates at six months. The authors concluded that the privacy regulation "significantly decreases the number of patients available for outcomes research and introduces selection bias in the data collection for patient registries." Another researcher impacted by new "opt in" requirements adopted by many institutions in

the wake of HIPAA has observed that the regulation "is causing the death of many large epidemiologic and intervention studies" by seriously impeding recruitment and introducing bias (J. Piette, personal correspondence).

Informed-Consent Process

The Common Rule promotes "respect for persons" by generally requiring researchers to obtain voluntary, written informed consent from prospective subjects before enrolling them in studies. HIPAA similarly requires authorization before anyone's health information is used for research purposes. Common Rule consent requirements and HIPAA authorization requirements are summarized in Table 1. In brief, both regulations require that prospective subjects are informed of the purposes of the research and use or disclosure of their PHI; told who is conducting the research and is allowed to disclose or receive the PHI; and assured that their participation is voluntary.

The Common Rule mandates that the informed-consent document describe how confidentiality will be maintained. HIPAA has a similar requirement but demands a more detailed description, as well as a statement explaining that once PHI is disclosed to researchers, it may be redisclosed and is no longer protected by the federal regulation. In light of existing Common Rule, institutional, and ethical requirements for privacy protection, this language arguably implies a much greater risk to participant privacy than actually exists. Moreover, HIPAA's authorization requirements, together with clarifications published by the National Institutes of Health after implementation of the regulation, are complex and difficult to address. Most important, they undermine the careful balance struck by the Common Rule between a prospective subject's interest in privacy and the research community's need to identify and recruit subjects to participate in research projects.

Health care organizations have adopted different approaches to achieve compliance with Common Rule consent and HIPAA authorization requirements. Some use "stand-alone" HIPAA authorizations for studies that rely on information protected by HIPAA and do not require IRB approval for these documents. Others require integrated forms and IRB oversight of the consent and authorization process.

Not surprisingly, AAMC's 2003 survey found that use of an additional form tended to confuse more than inform participants, that authorization language (which often tracks the regulation) was difficult for subjects to understand, and that subjects were overwhelmed by the added length and repetitiveness of informed-consent forms. These anecdotal reports were borne out by researchers who examined forms from >100 institutions (23). They concluded that HIPAA on average appears to add ~ 2 pages to informed-consent documents that in many cases are already long and complex; readability hovers around a twelfth-grade level, which is far too difficult for many lay subjects to understand; and in general the forms seem to be designed more for institutional protection than for the provision of information prospective subjects need to make an informed choice about whether

TABLE 1 Comparison of Common Rule consent and HIPAA authorization requirements[a]

Common Rule consent	HIPAA authorization
Statement that study involves research; description of purposes of the research	Description of PHI[b] to be used or disclosed; description of each purpose of the disclosure (must be study-specific; "blanket" and "compound" authorizations generally prohibited)
Expected duration of subject's participation; approximate number of subjects involved	Expiration date or event ("at the end of the study" or "none" is acceptable for research projects)
Description of procedures to be followed; identification of any experimental procedures	Identification of persons/groups authorized to disclose PHI; identification of persons/groups (e.g., "researchers") authorized to receive PHI
Description of any foreseeable risks and statement that there may be unforeseeable risks; description of any reasonably expected benefits; disclosure of any appropriate alternatives that might be advantageous to the subject; statement describing confidentiality procedures; statement describing extra costs to subject	Statement that once disclosed to researchers, PHI may no longer be protected by HIPAA
If research involves more than minimal risk: description of compensation, treatment options, or statement of where more information can be obtained	—
Statement that participation is voluntary and withdrawal is permitted; statement that declining to participate or withdrawing will result in no loss of benefits; statement regarding involuntary removal of subject from study; consequences of early withdrawal and procedures for orderly withdrawal	Statement that use/disclosure of PHI is voluntary or, if applicable, that participation in study requires use/disclosure of PHI; statement that subject can revoke authorization and description of exceptions (e.g., data retained for regulatory purposes)
Statement that significant new findings will be shared with subject	—
Signature of subject or legally authorized representative (with description of person's authority) and date	Signature of subject or personal representative (with description of person's authority) and date

[a]Sources: Office for Human Research Protections, *Informed Consent Checklist*, at http://www.hhs.gov/ohrp/humansubjects/assurance/consentckls.htm and National Institutes of Health, *HIPAA Authorization for Research*, at http://privacyruleandresearch.nih.gov/authorization.asp.

[b]PHI, protected health information.

to participate. These findings are entirely predictable; even the National Institutes of Health's model language (24) scores at a twelfth-grade level using Microsoft Word's Flesch-Kincaid scale. The result, according to one researcher, is a reduction in active engagement by prospective participants in the informed-consent process (M. Burmeister, personal correspondence). This outcome is particularly disturbing in light of research indicating that, at least in some clinical trials, confidentiality ranks among the least important considerations for deciding whether to participate (26). As much as HIPAA may technically increase privacy protection, there appears to be at least as significant a loss to substantive informed consent.

Inconsistent Interpretation and Other Institutional Problems

Countless efforts have been made by private industry, trade groups, and even HHS itself to facilitate industry compliance with HIPAA's complex web of "standards" and "implementation specifications." Yet interpretations of the Privacy Rule remain numerous, perhaps partly because of differing levels of risk tolerance in the face of possible administrative, civil, and even criminal penalties. Instead, covered entities and others affected by HIPAA have conducted largely independent analyses of the regulation's requirements and impact and have reached different and sometimes affirmatively inconsistent conclusions. Indeed, even within institutions, initial determinations made in the rush to achieve compliance before the April 2003 deadline are subject to continuing reexamination as additional guidance becomes available from HHS and other agencies, reports are circulated about alternative approaches adopted at peer institutions, and local experience suggests the need to explore new paths.

This volatility within institutions and inconsistent application among institutions has a particularly deleterious impact on multicenter research. At a time when multicenter collaborations are increasingly important in clinical, outcomes, and epidemiologic research, HIPAA has caused many providers to stop participating altogether (27, 28).

Research Quality

HIPAA promotes reduced dependence on identifiable data sets by eliminating authorization or waiver requirements for use of masked or deidentified data through one of two methods summarized in Table 2.

Yet identifiable data are indispensable to many research endeavors, including studies designed to identify the natural history, cause, and development of disease; measure the costs and benefits of alternative interventions; analyze disparities in the health delivery system; identify trends in health care; and validate the results of original trials (29). Prior to HIPAA, most records research involving use of anonymized data was eligible for an exemption from IRB review. Since the regulation became effective, however, researchers have experienced reduced access to the information necessary to create anonymized data sets.

TABLE 2 Rules for anonymizing data: comparison of deidentified data sets and limited data sets

Data element[a]	Deidentified data set[b]	Limited data set[c]
Names	Remove	Remove
Address, city and other geographic information smaller than state. Three-digit zip code may be included in a deidentified data set for an area where >20,000 people live; use "000" if <20,000 people live there	Remove[d]	Remove street address (city, state, zip may remain)
All elements of dates (except year), plus age and any date (including year) if age is over 89. Examples: date of birth, date of death, date of admission, date of discharge, date of service	Remove	May be included
Telephone and fax numbers, email addresses, web URL addresses, IP addresses	Remove	Remove
Social security number, medical record number, health plan beneficiary number, any account number, certificate or license number	Remove	Remove
Vehicle identifiers and serial numbers, including license plate numbers	Remove	Remove
Device identifiers and serial numbers	Remove	Remove
Biometric identifiers (e.g., fingerprints, voice prints). DNA is not considered a biometric identifier for purposes of HIPAA	Remove	Remove
Full-face photographs and any comparable images	Remove	Remove
Any other unique identifying number, characteristic or code	Remove	May be included

[a]For each listed data element, the information must be removed from the dataset with respect to the patient and to any of the patient's employers, relatives, or household members.

[b]Even if all the information listed in this column is removed, if the researcher knows that any remaining information in the data set could be used to reidentify a patient (e.g., a diagnosis code where the disease is very rare), then the data set is not considered deidentified.

[c]Use of a limited data set requires a "data use agreement" with detailed provisions designated by HHS, including provisions limiting use to a specified purpose and provisions prohibiting reidentification by recipients.

[d]If links must be maintained in the data set for potential later reidentification, they must be completely unrelated to any of the above elements. For example, a patient's initials or a scrambled social security number are not permitted in a deidentified data set. A subject code that reflects the order in which subjects were enrolled into a trial would be permitted.

Moreover, in its 2003 survey of academic researchers, AAMC noted that by encouraging use of deidentified data and prohibiting authorization for unspecified future uses, HIPAA also had increased error rates and forced researchers to limit their focus or change the direction of their inquiry. Researchers have examined the relative utility of pre-HIPAA data sets incorporating patient identifiers, limited

data sets, and deidentified data; their results support these concerns, finding that substantial data were lost in the effort to strip data sources of identifiers (30). Many researchers are "forced to make decisions about current need for data items when research is open ended and has unforeseen questions that will later arise" (28).

Formal agency interpretation of HIPAA's authorization requirements also has resulted in reduced reporting of data necessary to validate study results. International researchers serving as a coordinating center for a multicenter traumatic brain injury trial, for example, observed significant changes in screening log reporting after HIPAA implementation (31). In that study, most of the American sites significantly restricted the data made available to the coordinating center. Ten of 15 American sites do not report actual age; 10 provide date but not time of injury; many omit information on the occurrence of hypoxic or hypotensive episodes; and an admission Glasgow Coma Scale is often omitted. These omissions directly affect the quality of research by rendering impossible detailed comparison of participating and nonparticipating screened patients and comparison of basic population characteristics between countries and regions.

Yet HIPAA provides no obvious vehicle to facilitate such reporting. Screening log data ordinarily include links to prospective subject records (to facilitate reidentification if necessary for external validation), unique identifiers, ages, genders, screening dates, service dates, and other related health information. Thus, the information may be accessed by a researcher only (*a*) with patient authorization, (*b*) under a waiver of authorization, or (*c*) in the form of a limited data set or deidentified data set. Patient authorization, however, is unlikely to be obtained, at least in instances of patient refusal to participate. A waiver of authorization is not likely to be granted by an IRB or Privacy Board under circumstances where patients are directly approached because in that instance it is difficult to demonstrate that it is "impracticable" to obtain consent or authorization. Finally, limited data or deidentified data sets often exclude information relevant to, and indeed necessary for, external validation. Some covered entities have addressed these problems by interpreting HIPAA to permit researchers to collect the necessary data and deidentify it or create a limited data set before passing it on to coordinating centers or sponsors. Many others, though, as is clear from the above example, have not.

Administrative Costs

When HHS issued the original final Privacy Rule in December 2000, it estimated a total cost of more than $17 billion to the health care industry for implementation. This represented nearly 0.25% of total estimated health care expenditures in 2003, expected to decrease to 0.07% of total expenditures by 2008. The Department argued at the time that the cost would be more than offset by projected savings resulting from implementation of other "administrative simplification" regulations and that the value of increased privacy protection for individuals could not be

quantified. Of the total projected cost of implementation, more than $40 million in the first year and nearly $600 million over 10 years were attributed to the regulation's "requirements on research" (32).

Health care organizations, researchers, IRBs, and others involved in clinical research in fact have experienced these costs—attributed primarily to increased paperwork, increased staff time, and significant slow-downs in recruitment and enrollment—and cited them as reasons for reformulating research plans or abandoning research efforts altogether (4, 12, 18, 27, 28, 32–34). It is conceivable that these costs may have the less direct, but still important, effect of increasing the need for external commercial funding, discouraging investigator-initiated research, and reducing training opportunities for young researchers. Anecdotal observations confirm that while large research projects can absorb these costs (18), smaller ones cannot.

Enhanced Privacy Protection?

For all the added regulatory burden created by HIPAA, it is difficult to discern concrete gains for subject privacy. The regulation's prescriptive requirements for valid authorization forms generally may provide subjects with a bit more detail than they otherwise might receive about the intended uses and disclosures of their information, but prohibitions on compound and blanket authorizations often have the strange effect of actually misleading subjects by omission.

For example, a National Action Plan on Breast Cancer working group consisting of patient advocates, ethicists, lawyers, pathologists, clinicians, and researchers developed a special consent form that gave prospective subjects the following choice. They could agree (*a*) to the use of their specimens (and related information) for research related to their condition or for any research at all; and/or (*b*) to be contacted in the future about other research opportunities (35, 36). Although the form has its critics, ethics committees throughout the United States subsequently agreed it struck an appropriate balance between the need to inform prospective subjects of their rights and the need to facilitate future research without having to anticipate specific research questions. In fact, NIH continues to post a version of the form on its website, at http://www.cancerdiagnosis.nci.nih.gov/specimens/legal.html#3b. HHS, however, declined explicit requests to allow this practice under the Privacy Rule, arguing that "blanket authorizations" for unspecified future research would deprive patients of the necessary information to make an informed choice about participation in the activity. HHS further argued that covered entities were not in a position to evaluate the adequacy of such authorizations, and added that the requirement for authorization could be waived when necessary to facilitate future research (1). Given the difficulties of contacting subjects months or even years after initial collection, this means that most future studies will proceed under a waiver of authorization (if they are regulated by HIPAA at all). Thus, rather than giving subjects a greater say in the future use of their information, HIPAA may effectively deprive them of that control.

Several exceptions to the Privacy Rule's authorization requirements were adopted in part to address the concern that HIPAA would negatively impact research. In truth, however, those exceptions undermine the promise that patients will have more control over their information and impose on covered entities and researchers administrative obstacles that are difficult and often costly to overcome. In addition, HIPAA may actually result in decreased privacy protection by introducing new risks. For example, one technique many researchers have adopted to ensure their access to PHI is the creation of research registries (18). Researchers ask individuals to allow demographic and health information to be recorded in a registry that is then used for records research proceeding under a waiver or for contacting prospective subjects for future studies. Before HIPAA, researchers accessed this information directly or through data stewards from medical records. Within large health care organizations, such records typically are managed by sophisticated information technology staff and are protected by rigorous access and security protections. Research registries, however, often are managed by much less experienced researchers and staff, and to the extent that they are maintained outside covered entities, they are not regulated by HIPAA at all. With reports of hacking incidents involving data repositories of all sorts on the rise, it is easy to anticipate new security risks, at least for individuals who choose to participate in registries. Moreover, an individual's refusal to participate in a particular registry does not guarantee that the person will never be contacted about participating in a future project. It may, however, bias studies (and render the "equitable selection" demanded by the Common Rule meaningless) by limiting the populations researchers initially approach to participate in studies.

CONCLUSION AND RECOMMENDATIONS

In 2004, the President's Cancer Panel observed, "Government cannot provide zero-risk privacy protection to individuals and at the same time promote a national agenda of collaborative cancer research. Making progress against cancer means making use of medical information, some of which may be considered private" (37). This fact is no less applicable to other medical specialties. The question, then, is how much individual risk citizens should be asked to assume collectively in the name of a public agenda of research and advances in medical knowledge.

The negative impact of HIPAA on research can best be addressed by reconsidering the role of research in the provision of health care and benefits in the United States. Medical research is no less a core element of health care operations than other quality-improvement and disease-management activities. It should be explicitly recognized as such, consistent with government-funded initiatives to promote evidence-based medicine and more efficient translation of research discoveries to everyday practice. To address concerns about the conduct of researchers who operate outside the jurisdiction of the Common Rule, this recognition could be

conditioned on a requirement that the research be subject to the oversight of an IRB operating under a Federalwide Assurance (6).

Numerous individuals (6, 33, 38, 39) and organizations (12, 14, 27, 28) have offered more specific recommendations to address the many challenges posed by HIPAA. These include explicitly defining human subjects research, or at least recruitment, as part of "health care operations" (and thus eliminating many of HIPAA's administrative requirements and complications); permitting the use of blanket and compound authorizations subject to IRB approval, or eliminating the authorization and waiver rules altogether for research conducted under the Common Rule; relaxing the deidentification standards and focusing instead on the safeguards researchers use in maintaining data; excluding research from HIPAA's accounting requirements; eliminating the authorization requirement for exempt research; improving guidance on the application of HIPAA to international research; and, more generally, harmonizing HIPAA, as it relates to research, with the Common Rule. It is conceivable that adoption of all of these recommended changes may positively impact research, but if implemented piecemeal, they are unlikely to fully address the problems we have discussed.

Concerns about HIPAA's impact on research are not universal. In fact, some advocates charge that HIPAA does not go far enough in protecting privacy and, in particular, in ensuring patients' rights to control their health information—not only in connection with research (40, 41) but even when used for "routine purposes" (42, 43). Some commentators who acknowledge an early impact on research argue that identified problems will recede as researchers gain a better understanding of the regulatory requirements and familiarity with new procedures designed to facilitate compliance (13, 44, 45). The fact that researchers are more likely to identify significant problems than are administrators, who are more directly engaged in regulatory compliance efforts (28), may bear out this theory by pointing to a gap in training that is easily addressable.

Moreover, even after implementation of the new Privacy Rule, public anxiety about privacy—and particularly about medical privacy and the right to control health records—persists. As Kulynych & Korn (6) have observed, "Medical information differs in important ways from other personal data: it is more private, intimate, and sensitive and therefore merits greater protection. Misuse of medical information may cause serious harm: discrimination, stigmatization, or loss of insurance or employment." Recent incidents involving security breaches at large data-warehousing organizations and at research institutions, including the University of California at Berkeley and universities participating in the National Science Foundation's TeraGrid network, as well as anecdotal reports of intentional breaches and inadvertent disclosures resulting from human and computer error, have only heightened these concerns and intensified the call for ever more restrictive privacy and security regulation at the federal and state levels. One can assume that if it were more widely appreciated that publication of even small amounts of data can lead to identification of individuals, demand for such measures would become even more urgent.

It is not surprising, then, that the most important challenge for those advocating change is to present policy makers and the public with an accurate and clear description of the choices to be made and their consequences. Patients overwhelmingly support medical research (2) but also want to control the use of their own information in research—even when it is anonymized (40, 46). It is therefore critical to communicate that these goals inherently conflict, at least at the margins: that research, to have any meaning, requires (at a minimum) access to adequate information to recruit subjects and validate results; that individual control over all uses of medical information can and does undermine research; and that research can be conducted in a manner that is respectful of privacy and appropriately addresses the need for confidentiality. Advocates for eliminating most barriers to the use of data for research with appropriate safeguards are not enemies of patients' privacy. After all, we are patients ourselves. Instead, we believe that individual privacy interests must be balanced against the community interest in medical advances and that existing legal and ethical requirements for conducting human-subjects research adequately protect participant information from inappropriate use and disclosure.

ACKNOWLEDGMENTS

The authors thank Matthew Mann for his assistance in researching this article and James W. Govert and Ethan Nosowsky for their editorial contributions.

The *Annual Review of Medicine* is online at http://med.annualreviews.org

LITERATURE CITED

1. 2002. Standards for privacy of individually identifiable health information. U.S. Dep. Health Hum. Serv. 67 Fed. Reg. 157, pp. 53181–273
2. Ness RB. 2005. A year is a terrible thing to waste: early experience with HIPAA. *Ann. Epidemiol.* 15:85–86
3. 1997. *Health privacy and confidentiality recommendations.* http://www.ncvhs.hhs.gov/privrecs.htm. U.S. Dep. Health Hum. Serv., Nat. Comm. Vital and Health Stat.
4. Kulynych J, Korn D. 2003. The new HIPAA (Health Insurance Portability and Accountability Act of 1996) Medical Privacy Rule: help or hindrance for clinical research? *Circulation* 108:912–14
5. 2003. HIPAA frequently asked questions (#302): Will the Privacy Rule make covered entities unable or reluctant to share information for research? U.S. Dep. Health Hum. Serv., Off. Civil Rights
6. Kulynych J, Korn D. 2002. The effect of the new federal medical-privacy rule on research. *N. Engl. J. Med.* 346:201–4
7. Marshall MF. 2002. *Comments to Notice of Proposed Rulemaking.* http://www.hhs.gov/ohrp/nhrpac/documents/rschltr.pdf Nat. Hum. Res. Prot. Advis. Comm.
8. *HIPAA testimony and correspondence*. http://www.aamc.org/advocacy/library/listing_hipaa.htm. Am. Assoc. Med. Coll.
9. 1996. Health Insurance Portability and Accountability Act. *P.L. 104–191, 42 U.S.C. 1320d*
10. 2005. HIPAA administrative simplification: enforcement. U.S. Dep. Health Hum. Serv., 70 Fed. Reg. 73, pp. 20224–58
11. Kaiser J. 2004. Patient records. Privacy

Rule creates bottleneck for U.S. biomedical researchers. *Science* 305:168–69
12. Ehringhaus S. 2003. *Testimony on behalf of the Association of American Medical Colleges before the National Committee on Vital and Health Statistics Subcommittee on Privacy*. http://www.aamc.org/advocacy/library/research/testimony/2003/111903.pdf
13. Bankhead C. 2004. Privacy regulations have mixed impact on cancer research community. *J. Natl. Cancer Inst.* 96:1738–40
14. Prentice ED. 2004. *SACHRP recommendations: letter to the Secretary*. U.S. Dep. Health Hum. Serv., Secretary's Advis. Comm. Hum. Res. Prot. http://www.hhs.gov/ohrp/sachrp/hipaalettertosecy090104.html
15. Melton LJ 3rd. 1997. The threat to medical-records research. *N. Engl. J. Med.* 337:1466–70
16. Woolf SH, Rothemich SF, Johnson RE, et al. 2000. Selection bias from requiring patients to give consent to examine data for health services research. *Arch. Fam. Med.* 9:1111–18
17. Gorby NS, Wolf MS, Bennett CL. 2004. Introducing HIPAA: triple the cost and triple the time for patient recruitment to the SELECT study. *2004 ASCO Annu. Meet. Proc., J. Clin. Oncol.* 22(14S):6009
18. Vates JR, Hetrick JL, Lavin KL, et al. 2005. Protecting medical record information: start your research registries today. *Laryngoscope* 115:441–44
19. Phipps E, Harris D, Brown N, et al. 2004. Investigation of ethnic differences in willingness to enroll in a rehabilitation research registry: a study of the Northeast Cognitive Rehabilitation Research Network. *Am. J. Phys. Med. Rehabil.* 83:875–83
20. Tu JV, Willison DJ, Silver FL, et al. 2004. Impracticability of informed consent in the Registry of the Canadian Stroke Network. *N. Engl. J. Med.* 350:1414–21
21. Armstrong D, Kline-Rogers E, Jani SM, et al. 2005. Potential impact of the HIPAA Privacy Rule on data collection in a registry of patients with acute coronary syndrome. *Arch. Intern. Med.* 165:1125–29
22. Deleted in proof
23. Breese P, Burman W, Rietmeijer C, et al. 2004. The Health Insurance Portability and Accountability Act and the informed consent process. *Ann. Intern. Med.* 141:897–98
24. 2004. *HIPAA authorization for research*. U.S. Dep. Health Hum. Serv., Nat. Inst. Health. http://privacyruleandresearch.nih.gov/pdf/authorization.pdf
25. Deleted in proof
26. Tait AR, Voepel-Lewis T, Robinson A, et al. 2002. Priorities for disclosure of the elements of informed consent for research: a comparison between parents and investigators. *Paediatr. Anaesth.* 12:332–36
27. Government Accountability Office. 2004. *Health information: first-year experiences under the federal Privacy Rule*. Washington, DC: Gov. Account. Off. http://www.gao.gov/new.items/d04965.pdf
28. Ehringhaus SH. 2004. *AAMC project to document the effects of HIPAA on research*. Am. Assoc. Med. Coll.–SACHRP Presentation. http://www.aamc.org/advocacy/library/research/testimony/2004/033004.pdf
29. Black N. 2003. Secondary use of personal data for health and health services research: why identifiable data are essential. *J. Health Serv. Res. Policy* 8(Suppl. 1):36–40
30. Clause SL, Triller DM, Bornhorst CP, et al. 2004. Conforming to HIPAA regulations and compilation of research data. *Am. J. Health Syst. Pharm.* 61:1025–31
31. Maas AI, Kompanje EJ, Slieker FJ, et al. 2005. Differences in completion of screening logs between Europe and the United States in an emergency phase III trial resulting from HIPAA requirements. *Ann. Surg.* 241:382–83
32. 2000. *Standards for privacy of individually identifiable health information*. U.S.

Dep. Health Hum. Serv. 65 Fed. Reg., pp. 82462–29. http://www.hhs.gov/ocr/hipaa/finalreg.html
33. Califf RM, Muhlbaier LH. 2003. Health Insurance Portability and Accountability Act (HIPAA): Must there be a trade-off between privacy and quality of health care, or can we advance both? *Circulation* 108:915–18
34. Mull J. 2004. *Consent form and IRB challenges that arise with specimen banking in a multicenter trial setting*. Presented at Conflicts of Interest, Privacy/Confidentiality, and Tissue Prepositories: Protections, Policies, and Practical Strategies, Boston, MA
35. Taube SE, Barr P, LiVolsi V, et al. 1998. Ensuring the availability of specimens for research. *Breast J.* 4:391–95
36. Ryan KJ, Brady JV, Cooke RE, et al. 1979. *Ethical principles and guidelines for the protection of human subjects*. The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.htm
37. 2004. *President's Cancer Panel: translating research to reduce the burden of cancer*. http://deainfo.nci.nih.gov/advisory/pcp/30aug04.htm
38. Ingelfinger JR, Drazen JM. 2004. Registry research and medical privacy. *N. Engl. J. Med.* 350:1452–53
39. Rothstein MA. 2005. Research privacy under HIPAA and the Common Rule. *J. Law Med. Ethics* 33:154–59
40. Cayton H, Denegri S. 2003. Is what's mine my own? *J. Health. Serv. Res. Policy* 8(Suppl. 1): S1:33–35
41. 2002. *Declaration on ethical considerations regarding health databases*. World Med. Assoc. http://www.wma.net/e/policy/d1.htm
42. Markey EJ. 2004. Commerce with a conscience: balancing privacy and profit in a digital world. *Harvard J. Legis.* 41:377–88
43. Roche PA. 2005. Protecting privacy of human subjects. *Science* 307:1200–1
44. Barnard J, Fine D. 2003. The HIPAA Privacy Rule and its impact on pediatric research. *J. Pediatr. Gastroenterol. Nutr.* 37:527
45. O'Rourke P, Barefoot B, Johnson O, et al. 2004. *Privacy Panel II: Privacy/confidentiality challenges in the HIPAA era*. Presented at Conflicts of Interest, Privacy/Confidentiality, and Tissue Repositories: Protections, Policies, and Practical Strategies, Boston, MA
46. 2005. Lewis Harris & Associates. *Health Information Privacy (HIPAA) notices have improved public's confidence that their medical information is being handled properly*. http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=894