The New HIPAA (Health Insurance Portability and Accountability Act of 1996) Medical Privacy Rule
Help or Hindrance for Clinical Research?
Jennifer Kulynych, JD, PhD; David Korn, MD

The Federal Policy for Protection of Human Research Subjects, adopted by 17 federal agencies as a common regulatory framework (the “Common Rule”) for most federally sponsored human subjects research, acknowledges the centrality of privacy and confidentiality to the ethical conduct of research by mandating, both implicitly and explicitly, that institutional review boards (IRBs) address these concerns. Regulations adopted by the US Food and Drug Administration (FDA) require IRBs to assess protections for privacy and confidentiality in a similar manner. Implicit in the requirement (of both the Common Rule and FDA regulations) that IRBs weigh the risks and benefits of proposed research is the expectation that risks to privacy and confidentiality will be among those the IRB considers. Moreover, both the Common Rule and FDA regulations require IRBs to make an explicit finding that a researcher has proposed adequate protections to minimize the possibility of a breach of privacy or confidentiality and the attendant risk that subjects could suffer embarrassment, stigmatization, or discrimination.

Despite these regulatory mandates, critics state that the existing system of IRB oversight does not ensure that subjects’ privacy rights are respected fully and their confidentiality protected adequately. It is argued that heavily burdened IRBs, particularly those in academic settings, may devote insufficient attention to, and may lack the expertise to evaluate, risks to privacy and confidentiality in an electronic age in which barriers to data transmission are low and in which data stripped of names and other facial identifiers may yet be re-identified for questionable purposes through the use of computer algorithms and diverse databases publicly available from private and governmental sources. Claims that some commercially sponsored research may be little more than thinly disguised marketing have further heightened anxiety about an erosion of health information privacy in an age of information technology, managed health care, and aggressive pharmaceutical direct-to-consumer promotion.

Touted as an answer to these and other health information privacy concerns is the new federal medical Privacy Rule, officially known as Standards for Privacy of Individually Identifiable Health Information. This regulation, authorized by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and drafted, due to congressional default,* by the Department of Health and Human Services (DHHS), was released in the final days of the Clinton administration and then re-issued with only minor modifications by the Bush administration. In response to a storm of unhappy comment letters from many affected parties, the Bush administration agreed to a further round of revision and released a substantially modified Final Rule in August 2002, with a compliance date of April 14, 2003. The Privacy Rule will be enforced by

*The HIPAA statute authorized the Secretary of DHHS to promulgate privacy regulations only if Congress failed to pass medical privacy legislation by a specified date. When this date passed, the Secretary issued a proposed rule titled Standards for Privacy of Individually Identifiable Health Information, commonly referred to as the Privacy Rule.
DHHS’ Office of Civil Rights (OCR), a regulatory body experienced in investigating discrimination claims but previously lacking familiarity with the regulation of either health-care delivery or research.

Given the nature of the privacy concerns to be addressed, the seemingly most logical and parsimonious approach to rule-making would have been to identify and regulate those uses of identifiable health information deemed to be problematic or impermissible. But DHHS chose instead to specify all permissible uses or disclosures of identifiable health information by those entities covered by HIPAA (eg, hospitals and providers). In doing so, despite their great investment of time in the Rule’s controverted gestation, the Rule’s drafters could not appreciate fully the intricacy and intensity of information exchange, either in the contemporary healthcare delivery system or in the conduct of biomedical and health sciences research. Furthermore, in choosing over strong objections to impose new regulatory burdens on research already subject to federal regulation, DHHS discounted the finding of its own statutorily created advisory group (the National Committee on Vital and Health Statistics), which in its 1997 report to the Secretary stated explicitly that it had uncovered no evidence that medical and health research in fact posed a threat to the privacy and confidentiality of medical information.

The Privacy Rule erects significant new barriers to the use or disclosure of identifiable health information by imposing an intricate series of organizational and procedural requirements on the entities it covers. Yet, the regulation does not implement a comprehensive statutory scheme for protecting medical information privacy, because by its own terms, HIPAA limits the Secretary to regulating the conduct of providers who are engaged in the electronic transmission of protected health information (PHI) to entities not covered by the Rule. This is to be accomplished through mandatory contractual conditions or highly specific data use agreements with third-party recipients of identifiable health information, or, when data are disclosed under a research waiver, unspecified “written assurances” proffered by the researcher.

Researchers accustomed to receiving data that have been rendered anonymous to the satisfaction of an IRB must understand that the Privacy Rule defines “identifiable” far more precisely and expansively than do federal research regulations (and well beyond the common understanding of the term). Under the Rule it becomes a daunting task for covered entities to create “de-identified” data sets that may be disclosed without patient authorization or further legal restriction. This problem of de-identification is particularly acute for health research, much of which requires data elements (eg, full zip code or date of birth) that must be removed to render the data de-identified to the strict standard of the Privacy Rule.

Otherwise, without written patient authorization of a highly prescriptive and purpose-specific form, covered entities may only make certain uses of their identifiable health information (PHI) and may only disclose it to third parties for sanctioned purposes. Subject to very limited exceptions, research (regrettably, and arguably unwisely) is not such a purpose. Thus, clinical research will require new, HIPAA-compliant authorizations, while disclosures of most health information for “secondary” health research will require new and additive IRB (or specifically constituted Privacy Board) review processes or, in limited cases, project-specific data use agreements, as well as possible review by the provider’s newly mandated compliance official, the Privacy Officer.

Achieving compliance with the Privacy Rule is not simply a matter of erecting the thicket of new policies, procedures, forms, and notices that the Rule requires: Providers must also make difficult decisions about when, how, and to whom to disclose health information in accordance with the Rule’s complicated restrictions. The burden of Privacy Rule compliance planning has been felt acutely within universities containing medical and other health professions schools and teaching hospitals (academic health centers [AHCs]), where clinical and other health sciences research requiring access to medical records may cross the Rule’s jurisdictional divide between covered and noncovered organizational components.

The Privacy Rule forces AHCs to navigate a confusing matrix of decisions and self-designations, confounded by the Rule’s ambiguous language, and with significant legal and operational consequences. AHCs and other covered entities may apply the Rule to all of their operations, or they may elect to bifurcate themselves into “hybrid entities” by isolating the components that perform “covered” functions such as treatment or billing, or administrative support for these functions. A hybrid entity must erect internal firewalls to prevent PHI from crossing between the covered and noncovered components (eg, between a covered hospital and a noncovered academic department or health profession school).

Research is especially problematic for the hybrid entity because, although research is not a covered function under the Privacy Rule, research involving treatment or requiring access to PHI does fall under the Rule’s provisions. Within a hybrid AHC, some of that research will be conducted in departments or schools (eg, genetics or epidemiology) that may lie outside the covered component, whereas other research (eg, clinical trials) will ordinarily be performed within it. Irrespective of location, any research that requires access to the covered entity’s medical archives will have to conform to the entity’s privacy policies and procedures—to
the extent that the entity is willing to consider providing such research access at all. To complicate matters further, the Rule is ambiguous about the status of IRBs, whether internal to the covered entity or external, and thus, it is uncertain whether the covered component of an institution may share PHI with an IRB for purposes of reviewing a research protocol. Similarly, it is unclear what terms a covered entity must reasonably impose when sharing PHI with commercial research sponsors or multisite collaborators. Other ambiguities include the interpretation of provisions in the Rule relating to “specificity of authorization,” “minimum necessary,” and “designated record set,” and the applicability of the Rule to international research.

Confused? That’s hardly surprising: Academic institutions, leading healthcare attorneys, and even DHHS itself seem uncertain about exactly how the Rule should be implemented in many research contexts. As a result, AHCs have spent hundreds of faculty hours on HIPAA implementation plans and committees and untold thousands of dollars on legal and consultant services to make sense of it all and to design forms, policies, and compliance plans that might withstand a compliance investigation or legal challenge. Noteworthy with regard to the potential for compliance investigations is the extent to which the Rule encourages “whistle-blowers” to report perceived violations of the privacy of any person’s medical information. Presently, OCR is soliciting comments on a proposal to automate such reporting through an online complaint system.

Although research is not the sole source of HIPAA compliance costs, within AHCs the portion of the compliance effort devoted to research is both significant and costly, diverting resources from pursuits that any rational cost/benefit analysis might suggest merit greater priority, such as expanding IRB membership, increasing research staffing and technical capabilities, exerting greater institutional oversight of financial conflicts of interest, and enhancing informed consent procedures for research subjects.

And once implemented, the Privacy Rule will further encumber the research process for subjects, investigators, and IRBs. In a HIPAA-compliant research environment, subjects will encounter new and detailed notices of privacy practices and be required to authorize a laundry list of uses and disclosures of their health information. Researchers will be required to assemble the documentation necessary to secure authorization or waiver of authorization to use or disclose patients’ protected health information, in addition to seeking informed consent or waiver of consent. IRBs must master the new Privacy Rule and apply a new set of criteria to grant waivers of authorization, in addition to the criteria they must already apply under federal research regulations to waive informed consent. Research institutions and community providers must devise systems to capture over a 6-year period, and account in detail to patients on request, all disclosures of identifiable health information for nonexempt purposes that have not been specifically authorized; this includes disclosures to researchers pursuant to IRB waivers. These mandatory new systems and procedures will inevitably delay, impede—and possibly deter—the conduct of medical and other health sciences research that requires access to medical records or other provider-maintained repositories of health information.

In previous commentary urging modifications to the Privacy Rule, 6,7 and in our advocacy on behalf of the Association of American Medical Colleges, we questioned the wisdom of imposing a complex new federal privacy regime (and the attendant liability) on federally regulated research. In our view, the better and far more parsimonious approach to protecting privacy in human subjects research would have been to strengthen existing provisions of the federal Common Rule that govern an IRB’s review of privacy and confidentiality. The Office of Human Research Protections within DHHS is well situated to accomplish this through the normal administrative guidance-development process.

We regard the new Privacy Rule as a significant hindrance to health research. How serious that hindrance will be remains to be seen. We earlier expressed our fear that community providers for whom teaching and research are not primary missions will be especially reluctant to incur the substantial expense and liability exposure that attend compliance with the Rule’s research provisions. Archives maintained by such providers are essential for epidemiological, health services, and environmental and occupational health research, as well as for postmarketing studies of the safety and efficacy of drugs and medical devices—all of which require access to large, minimally biased population databases. Equally important, the health benefits inherent in the Human Genome project will only be realized through meticulous phenotyping of diverse populations, an undertaking that will generate enormous pressures for access to medical records. This is an especially unpromising time for the federal government to impose a convoluted and unnecessarily burdensome privacy regime on health research.

References
1. Criteria for IRB approval of research. 45 CFR §46.111 (DHHS regulations). The Common Rule has been adopted by many other federal agencies through various regulations.
5. 45 CFR, §160.102(a) (Privacy Rule: Applicability).
The New HIPAA (Health Insurance Portability and Accountability Act of 1996) Medical Privacy Rule: Help or Hindrance for Clinical Research?
Jennifer Kulynych and David Korn

_Circulation_. 2003;108:912-914
doi: 10.1161/01.CIR.0000080642.35380.50
_Circulation_ is published by the American Heart Association, 7272 Greenville Avenue, Dallas, TX 75231
Copyright © 2003 American Heart Association, Inc. All rights reserved.
Print ISSN: 0009-7322. Online ISSN: 1524-4539

The online version of this article, along with updated information and services, is located on the World Wide Web at:
http://circ.ahajournals.org/content/108/8/912

Permissions: Requests for permissions to reproduce figures, tables, or portions of articles originally published in _Circulation_ can be obtained via RightsLink, a service of the Copyright Clearance Center, not the Editorial Office. Once the online version of the published article for which permission is being requested is located, click Request Permissions in the middle column of the Web page under Services. Further information about this process is available in the Permissions and Rights Question and Answer document.

Reprints: Information about reprints can be found online at:
http://www.lww.com/reprints

Subscriptions: Information about subscribing to _Circulation_ is online at:
http://circ.ahajournals.org//subscriptions/