

REPORT BRIEF • FEBRUARY 2009

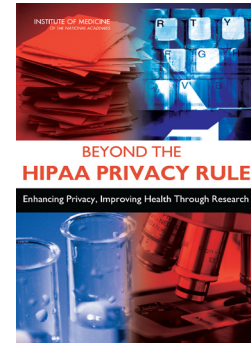
BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH

Our modern electronic world has many benefits and conveniences; emails can be checked from a mobile device and patients provide their medical histories online. But this free flow of information also creates privacy concerns; the risks of data security breaches, identity theft, and discrimination are real. Privacy protections are needed, but they can also impede the flow of information, with negative consequences. In health research, access to patient health information is vital for making medical advances such as new therapies, improved diagnostics, and more effective ways to prevent illness and deliver care. At the same time, effective privacy protections permit health care and research activities to be carried out in ways that preserve patients' dignity, and help protect individuals from harms like discrimination. Thus, privacy protections and ethically-conducted health research provide valuable, interrelated benefits to society and society should strive to support both.

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), which called for a set of federal standards, now known as the HIPAA Privacy Rule, for protecting the privacy of personally identifiable health information. One major goal of the Privacy Rule is to ensure that individuals' privacy is properly protected while allowing the flow of information needed to promote high-quality health care. In 2007, the Institute of Medicine charged the Committee on Health Research and the Privacy of Health Information with two major tasks: 1) to assess whether the HIPAA Privacy Rule is having an impact on the conduct of health research, and 2) to propose recommendations to facilitate health research while maintaining or strengthening the privacy protections of personally identifiable health information. In its report, the committee concludes that the HIPAA Privacy Rule does not protect privacy as well as it should, and that, as currently implemented, it impedes important health research.

A NEW APPROACH FOR PROTECTING PRIVACY IN HEALTH RESEARCH

The committee determined that the Privacy Rule's research provisions have many serious limitations, and therefore, it recommends first and foremost that Congress authorize the Department of Health and Human Services (HHS) and other relevant federal agencies to develop a new approach to ensuring privacy in health research. This new framework, which should be applicable to all health research in the United States regardless of the source of funding or the holder of the data, would improve the privacy and confidentiality of personal health data used in research by reducing variability in the ethical oversight of research and by placing a high priority on strong security protections. It would also enable responsible research and enhance trust in the research enterprise.



In its report, the committee concludes that the HIPAA Privacy Rule does not protect privacy as well as it should, and that, as currently implemented, it impedes health research.



INSTITUTE OF MEDICINE
OF THE NATIONAL ACADEMIES

For more information visit www.iom.edu/hipaa.

Advising the Nation. Improving Health.

HHS and other federal agencies should implement new goal-oriented, federal oversight of all information-based research in the U.S., with a focus on best practices in privacy, security, and transparency.

The committee found it important to distinguish between the unique needs of information-based research, which uses medical records or stored biological samples, and interventional clinical research, which involves people who participate in experimental treatment. Applying the same protections in these two fundamentally different scenarios is neither appropriate nor justifiable. The committee recommends extending the Common Rule (another set of federal regulations that generally applies to federally funded research conducted on human beings) to apply to all interventional research, regardless of funding source.

In addition, HHS and other federal agencies should implement new goal-oriented, federal oversight of all information-based health research in the U.S., with a focus on best practices in privacy, security, and transparency. The new framework aims to facilitate greater use of data in which the information that identifies the individual has been removed and includes legal sanctions to prohibit unauthorized reidentification. For situations in which personally identifiable information is used in research without individual consent, the new framework provides two methods for ethical oversight:

- 1) Oversight by a local ethical review board in which the measures to protect the confidentiality of the data, the potential harms that could result from disclosure, and the potential public benefits of the research are considered in determining whether to allow the research to go forward without consent.
- 2) Federal certification of institutions that have policies and practices in place to protect data privacy and security for clearly defined research purposes.

While people's expectations regarding privacy vary, public opinion polls suggest that many Americans would like to control all access to their medical records via a consent mechanism. However, in some cases, obtaining individual consent is not feasible, and a requirement for consent can lead to invalid results. For example, identifying adverse side effects from a treatment may entail the review of thousands of patient records, and patients with certain conditions or characteristics may be underrepresented if they are more likely to deny access to their records. Consequently, the results may not be applicable to their condition or circumstances.

REVISING HHS GUIDANCE ON PRIVACY PROTECTION IN RESEARCH

If national policy makers choose to continue to rely on the HIPAA Privacy Rule to protect patient privacy in health research rather than adopt the new approach, the committee recommends that HHS revise the HIPAA Privacy Rule and issue expanded and revised guidance on the Privacy Rule's research provisions. The committee's specific recommendations are intended to reduce variability in interpretation among Institutional Review Boards (IRBs) and Privacy Boards in order that all research is conducted under the same set of requirements. The committee suggests that HHS

- promote "best practices" for privacy protection in responsible research;
- facilitate greater use of data in which the information that identifies the individual has been removed;
- clarify the distinctions between health "research" and health "practice" (such as quality improvement or public health practices) to ensure appropriate ethical oversight of protected health information (PHI), as defined by the Privacy Rule, since "research" and "practice" activities are regulated differently under the Privacy Rule; and
- require the same restrictions for activities conducted in preparation for research (such as identifying potential research participants) under both the Privacy Rule and the Common Rule.

Because interpretation of the HIPAA Privacy Rule is not uniform, existing databases and stored patient biospecimens are often used ineffectively for health research and public health purposes. Therefore, the committee makes four recommendations to facilitate health research by maximizing the usefulness of these data sources. In particular, the committee suggests that HHS:

- Develop guidance that clearly states that individuals can authorize use of PHI stored in databases or biospecimen repositories for specified future research under the HIPAA Privacy Rule with ethical oversight.
- Develop clear guidance for use of a single form that permits individuals to authorize use and disclosure of PHI in a clinical trial and to authorize the storage of their biospecimens collected in conjunction with the clinical trial.
- Clarify the circumstances under which DNA samples are considered PHI.
- Create a mechanism for linking an individual's data from multiple sources such as databases so that more useful datasets can be made available for research in a manner that protects privacy, confidentiality, and security.

IMPROVING DATA SECURITY AND MAKING RESEARCH RESULTS ACCESSIBLE TO ALL AMERICANS

Whether the Privacy Rule is revised or a new framework is adopted, the committee stresses the need for three additional changes. The committee recommends that all health research institutions take strong measures to safeguard the security of personally identifiable health information. It recommends that HHS support the development and use of new security technologies and self-evaluation standards. In addition, to encourage people to volunteer to serve on IRBs or Privacy Boards, the committee recommends that HHS or Congress, as necessary, provide reasonable protection against civil suits for IRB and Privacy Board members. The protection should be reserved for good-faith decisions made within the scope of the Boards' responsibilities and backed by minutes or other evidence; there should be no protections for misconduct in reviewing the research.

Because studies show that the majority of Americans are interested in the findings of health research, the committee recommends that HHS and researchers take steps to inform the public further about health research—how research is conducted, the results it produces, and what value it provides to society.

CONCLUSION

As electronic health records are adopted more widely, the potential consequences of security breaches in health care make the protection of health information in research imperative. Today's protections, as provided in the HIPAA Privacy Rule, are not as effective as they should be. Not only are they frequently misinterpreted and generally lacking in clarity, but often they fail to protect patient privacy and impede important health research. Although expanded guidance from HHS could address some of the problems identified in this report, the committee strongly recommends that federal policy makers develop a new approach to ensuring privacy in health research that would apply to all health researchers and would provide more effective ethical oversight and stronger security protections. To ensure continued progress in improving our nation's health and health care, effective privacy protections must be implemented in a way that does not hinder health research or inhibit medical advances.

The committee recommends that all health research institutions take strong measures to safeguard the security of personally identifiable health information.

FOR MORE INFORMATION . . .

Copies of *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research* are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, www.nap.edu. The full text of this report is available at www.nap.edu.

This study was supported by funds from the Department of Health and Human Services, American Cancer Society, American Heart Association/American Stroke Association, American Society for Clinical Oncology, Burroughs Wellcome Fund, C-Change, and the Robert Wood Johnson Foundation. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for this project.

The Institute of Medicine serves as adviser to the nation to improve health. Established in 1970 under the charter of the National Academy of Sciences, the Institute of Medicine provides independent, objective, evidence-based advice to policymakers, health professionals, the private sector, and the public. For more information about the Institute of Medicine, visit the IOM web site at www.iom.edu.

Permission is granted to reproduce this document in its entirety, with no additions or alterations. Copyright © 2009 by the National Academy of Sciences. All rights reserved.

COMMITTEE ON HEALTH RESEARCH AND THE PRIVACY OF HEALTH INFORMATION: THE HIPAA PRIVACY RULE

LAWRENCE O. GOSTIN (Chair), Professor of Law, Georgetown University Law Center, Washington, DC; **PAUL APPELBAUM**, Columbia University Medical Center/New York Psychiatric Institute; **ELIZABETH BEATTIE**, Professor, School of Nursing, Faculty of Health Sciences, The Queensland University of Technology, Queensland, Australia; **MARC BOUTIN**, Vice President of Policy, Development, and Advocacy, National Health Council, Washington, DC; **THOMAS W. CROGHAN**, Senior Fellow, Mathematica Policy Research, Inc., Washington, DC; **STANLEY W. CROSLEY**, Chief Privacy Officer, Eli Lilly and Company, Law Division, Indianapolis, IN; **SANDRA HORNING**, Professor of Medicine/Oncology, Stanford School of Medicine; **JAMES S. JACKSON**, Director, Institute for Social Research, University of Michigan—Ann Arbor; **MARY BETH JOUBLANC**, Chief Privacy Officer, State of Arizona, Arizona Government Technology Agency; **BERNARD LO**, Professor of Medicine, Director, Program in Medical Ethics, University of California—San Francisco; **ANDREW F. NELSON**, Executive Director, HealthPartners Research Foundation, Minneapolis, MN; **MARC ROTENBERG**, President, Electronic Privacy Information Center, Washington, DC; **WENDY VISSCHER**, Director, Office of Research Protection, RTI International, Research Triangle Park, NC; **FRED WRIGHT**, Associate Chief of Staff for Research, VA Connecticut Healthcare System; **CLYDE W. YANCY**, Medical Director, Baylor Heart and Vascular Institute, Baylor University Medical Center, Dallas, TX

CONSULTANTS

SARAH M. GREENE, Group Health Center for Health Studies, Seattle, WA; **DAVID HELMS**, President and CEO, AcademyHealth, Washington, DC; **ROBERTA NESS**, University of Pittsburgh, Pittsburgh, PA; **JOY PRITTS**, Health Policy Institute, Georgetown University, Washington, DC; **ED WAGNER**, Director of the W.A. MacColl Institute for Healthcare; Innovation, Center for Health Studies, Group Health Cooperative of Puget Sound, Seattle, WA; **ALAN WESTIN**, Privacy Consulting Group, Teaneck, NJ

STUDY STAFF

SHARYL NASS, Study Director and Senior Program Officer; **LAURA LEVIT**, Associate Program Officer (Christine Mirzayan Science and Technology Policy Graduate Fellow, December 2006 to March 2007); **CATHERINE REYES**, Christine Mirzayan Science and Technology Policy Graduate Fellow (September 2006 to November 2006); **MARY ANN PRYOR**, Senior Program Assistant (until August 2007); **MICHAEL PARK**, Senior Program Assistant (from September 2007); **ANDREW POPE**, Director, Board on Health Sciences Policy; **ROGER HERDMAN**, Director, Board on Health Care Services