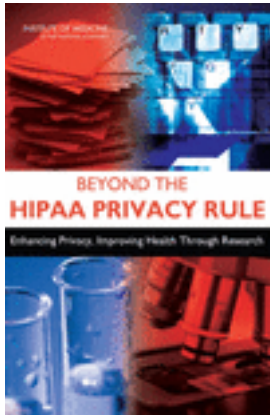


Free Executive Summary



Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research

Sharyl J. Nass, Laura A. Levit, and Lawrence O. Gostin, Editors; Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule; Institute of Medicine

ISBN: 978-0-309-12499-7, 330 pages, 6 x 9, paperback (2009)

This free executive summary is provided by the National Academies as part of our mission to educate the world on issues of science, engineering, and health. If you are interested in reading the full book, please visit us online at <http://www.nap.edu/catalog/12458.html>. You may browse and search the full, authoritative version for free; you may also purchase a print or electronic version of the book. If you have questions or just want more information about the books published by the National Academies Press, please contact our customer service department toll-free at 888-624-8373.

In the realm of health care, privacy protections are needed to preserve patients' dignity and prevent possible harms. Ten years ago, to address these concerns as well as set guidelines for ethical health research, Congress called for a set of federal standards now known as the HIPAA Privacy Rule. In its 2009 report, Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research, the Institute of Medicine's Committee on Health Research and the Privacy of Health Information concludes that the HIPAA Privacy Rule does not protect privacy as well as it should, and that it impedes important health research.

This executive summary plus thousands more available at www.nap.edu.

Copyright © National Academy of Sciences. All rights reserved. Unless otherwise indicated, all materials in this PDF file are copyrighted by the National Academy of Sciences. Distribution or copying is strictly prohibited without permission of the National Academies Press <http://www.nap.edu/permissions/>. Permission is granted for this material to be posted on a secure password-protected Web site. The content may not be posted on a public Web site.

Summary

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

Ethical health research and privacy protections both provide valuable benefits to society. Health research is vital to improving human health and health care—and protecting individuals involved in research from harm and preserving their rights is essential to the conduct of ethical research. The primary justification for protecting personal privacy is to protect the interests of individuals. In contrast, the primary justification for collecting personally identifiable health information for health research is to benefit society. But it is important to stress that privacy also has value at the societal level because it permits complex activities, including research and public health activities, to be carried out in ways that protect individuals' dignity. It is also important to note that health research can benefit individuals, for example, when it facilitates access to new vaccines, medicines, and other treatments.

The U.S. Department of Health and Human Services (HHS) developed a set of federal standards for protecting the privacy of personal health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).¹ The HIPAA Privacy Rule set forth detailed regulations

¹The HIPAA Privacy Rule (“Standards for Privacy of Individually Identifiable Health Information: Final Rule”) can be found at 45 Code of Federal Regulations (C.F.R.) parts 160 and 164. <http://www.hhs.gov/ocr/AdminSimpRegText.pdf> (accessed August 2, 2008). A summary of the HIPAA Privacy Rule, prepared by the HHS Office for Civil Rights, is available at <http://www.hhs.gov/ocr/privacysummary.pdf> (accessed August 2, 2008).

regarding the types of uses and disclosures of individuals' personally identifiable health information—called “protected health information”—permitted by “covered entities” (health plans, health care clearinghouses, and health care providers who transmit information in electronic form in connection with transactions for which HHS has adopted standards under HIPAA).² A major goal of the HIPAA Privacy Rule is to ensure that individuals' health information is properly protected while allowing the flow of information needed to promote high-quality health care. The HIPAA Privacy Rule also set out requirements for the conduct of health research.

The Institute of Medicine Committee on Health Research and the Privacy of Health Information (the committee) was charged with two principal tasks³: (1) to assess whether the HIPAA Privacy Rule is having an impact on the conduct of health research, defined broadly as “a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge”⁴; and (2) to propose recommendations to facilitate the efficient and effective conduct of important health research while maintaining or strengthening the privacy protections of personally identifiable health information.

The committee's conclusion is that the HIPAA Privacy Rule does not protect privacy as well as it should, and that, as currently implemented, the HIPAA Privacy Rule impedes important health research. The committee found that personally identifiable information is often not protected by the HIPAA Privacy Rule; that important health research is unnecessarily constrained by the HIPAA Privacy Rule; and that security breaches are a growing problem for health care databases. In developing its recommendations to improve this situation, the committee was guided by three overarching goals: (1) improve the privacy and data security of health information; (2) improve the effectiveness of health research; and (3) improve the application of privacy protections for health research. A summary of the committee's recommendations is presented in Box S-1.

RECOMMENDATION I. DEVELOP A NEW APPROACH TO PROTECTING PRIVACY IN ALL HEALTH RESEARCH

The committee's first and foremost recommendation (Recommendation I) is that Congress should authorize HHS and other relevant federal

²45 C.F.R. § 160.103 (2006).

³The study was funded by the National Institutes of Health, the National Cancer Institute, the Robert Wood Johnson Foundation, the American Cancer Society, the American Heart Association/American Stroke Association, the American Society for Clinical Oncology, the Burroughs Wellcome Fund, and C-Change.

⁴45 C.F.R. § 164.510 (2006).

agencies to develop a new approach to protecting privacy in health research that would apply uniformly to all health research. When this new approach is implemented, HHS should exempt health research from the HIPAA Privacy Rule. The new approach should enhance privacy protections through improved data security, increased transparency of activities and policies, and greater accountability, while also allowing important health research to be undertaken with appropriate oversight. The new approach should do all of the following:

- Apply to any person, institution, or organization conducting health research in the United States, regardless of the source of data or funding.
- Entail clear, goal-oriented, rather than prescriptive, regulations.
- Require researchers, institutions, and organizations that store health data to establish strong data security safeguards.
- Make a clear distinction between the privacy considerations that apply to interventional research and research that is exclusively information based.
- Facilitate greater use of data with direct identifiers removed in health research, and implement legal sanctions to prohibit unauthorized reidentification of information that has had direct identifiers removed.
- Require ethical oversight of research when personally identifiable health information is used without informed consent. HHS should develop best practices for oversight that should consider:
 - o Measures taken to protect the privacy, security, and confidentiality of the data;
 - o Potential harms that could result from disclosure of the data; and
 - o Potential public benefits of the research.
- Certify institutions that have policies and practices in place to protect data privacy and security in order to facilitate important large-scale information-based research for clearly defined and approved purposes, without individual consent.
- Include federal oversight and enforcement to ensure regulatory compliance.

Informative examples for such an approach include Ontario's Personal Health Information Protection Act (PHIPA)⁵ and a similar model recently

⁵Personal Health Information Protection Act, Statutes of Ontario 2004, Ch. 3, Schedule A; Ontario Regulation 329/04.

BOX S-1

Summary of the Committee's Recommendations

The committee's foremost recommendation is the following:

I. Congress should authorize HHS and other relevant federal agencies to develop a new approach to protecting privacy that would apply uniformly to all health research. When this new approach is implemented, HHS should exempt health research from the HIPAA Privacy Rule.

→ Apply privacy, security, transparency, and accountability obligations to all health records used in research.

If national policy makers choose to continue to rely on the HIPAA Privacy Rule rather than adopt a new federal approach (Recommendation I), the committee recommends the following:

II. HHS should revise the HIPAA Privacy Rule and associated guidance.

A. HHS should reduce variability in interpretations of the HIPAA Privacy Rule in health research by covered entities, Institutional Review Boards (IRBs) and Privacy Boards through revised and expanded guidance and harmonization.

1. HHS should develop a dynamic, ongoing process to increase empirical knowledge about current "best practices" for privacy protection in responsible research using protected health information (PHI), and promote use of those best practices.
2. HHS should encourage greater use of partially deidentified data called "limited datasets" and develop clear guidance on how to set up and comply with the associated data use agreements more efficiently and effectively, in order to enhance privacy in research by expanding use and usability of data with direct identifiers removed.
3. HHS should clarify the distinctions between "research" and "practice" to ensure appropriate IRB and Privacy Board oversight of PHI disclosures for these activities.
4. HHS guidance documents should simplify the HIPAA Privacy Rule's provisions regarding the use of PHI in activities preparatory to research and harmonize those provisions with the Common Rule, in order to facilitate appropriate IRB and Privacy Board oversight of identification and recruitment of potential research participants.

B. HHS should develop guidance materials to facilitate more effective use of existing data and materials for health research and public health purposes.

1. HHS should develop guidance that clearly states that individuals can authorize use of PHI stored in databases or associated with biospecimen banks for specified future research under the HIPAA Privacy Rule with IRB/Privacy

Board oversight, as is allowed under the Common Rule, in order to facilitate use of repositories for health research.

2. HHS should develop clear guidance for use of a single form that permits individuals to authorize use and disclosure of health information in a clinical trial and to authorize the storage of their biospecimens collected in conjunction with the clinical trial, in order to simplify authorization for interrelated research activities.
3. HHS should clarify the circumstances under which DNA samples or sequences are considered PHI, in order to facilitate appropriate use of DNA in health research.
4. HHS should develop a mechanism for linking data from multiple sources so that more useful datasets can be made available for research in a manner that protects privacy, confidentiality, and security.

C. HHS should revise provisions of the HIPAA Privacy Rule that entail heavy burdens for covered entities and impede research without providing substantive improvements in patient privacy.

1. HHS should reform the requirements for the accounting of disclosures of PHI for research.
2. HHS should simplify the criteria that IRBs and Privacy Boards use in making determinations for when they can waive the requirements to obtain authorization from each patient whose PHI will be used for a research study, in order to facilitate appropriate authorization requirements for responsible research.

Regardless of whether Recommendation I or II is implemented, the following recommendations, which are independent of the Privacy Rule, should be adopted:

III. Implement changes necessary for both policy options above (Recommendations I and II).

A. All institutions (both covered entities and non-covered entities) in the health research community should take strong measures to safeguard the security of health data.

→ HHS should also support the development and use of new security technologies and self-evaluation standards.

B. HHS—or, as necessary, Congress—should provide reasonable protection against civil suits for members of Institutional Review Boards and Privacy Boards who serve in good faith to encourage service on IRBs and Privacy Boards.

→ But no protection for willful or wanton misconduct.

C. HHS and researchers should take steps to provide the public with more information about health research by:

1. Disseminating research results to study participants and the public.
2. Educating the public about how research is done and what value it provides.

proposed in the United Kingdom.⁶ Ontario's PHIPA shares a number of similarities with the HIPAA Privacy Rule. In general, both rules require the holder of personally identifiable health data to get informed consent (referred to as authorization in the Privacy Rule) before using those data for a purpose other than providing services directly related to the health care of the patient. If a researcher wishes to use personally identifiable health data without getting informed consent, both rules require the researcher to obtain a waiver of informed consent approved by an independent ethics board before the study begins.

However, the HIPAA Privacy Rule and PHIPA do have some key differences. One major difference is that unlike the HIPAA Privacy Rule, which applies privacy obligations unevenly across the health care sector, PHIPA applies to health information custodians (HICs, e.g., providers, hospitals, and pharmacies) that collect, use, and disclose personally identifiable health information, as well as to non-HICs that receive personally identifiable health information from a HIC. Thus, the privacy protections follow the data.

Another important difference is that PHIPA permits HICs to disclose personally identifiable health information without consent to "prescribed persons or entities" that have in place privacy practices, policies, and procedures approved by Ontario's Information and Privacy Commissioner. The prescribed persons or entities may then disclose information to researchers either in deidentified form, or in identifiable form with approval of a Research Ethics Board (Canadian equivalent of an Institutional Review Board [IRB] or Privacy Board). Consistent with the principle of transparency, a prescribed entity must also make public a description of its functions and a summary of its practices, policies, and procedures. A similar approach was recommended in a report commissioned by the United Kingdom's Prime Minister on secondary uses of personal information. This report suggested the creation of "safe harbors," which have three defining characteristics: (1) they provide a secure environment for processing personally identifiable health data, (2) they are restricted to "approved researchers" who meet relevant criteria, and (3) they implement penalties and allow for criminal sanctions against researchers who abuse their access to personally identifiable data. The committee believes that such an approach, combined with strong security measures, offers adequate privacy protections for personally identifiable health information in information-based health research, while greatly expanding research opportunities.

The committee's new framework entails a two-part practical approach to protecting health information privacy because there are fundamental

⁶In a report commissioned by the United Kingdom's Prime Minister on secondary uses of personal information.

differences between information-based research (e.g., using medical records or stored biological samples) and direct, interventional human subjects research. Applying the same human subjects protections in these two different scenarios is neither appropriate nor justifiable. Promoting individual autonomy is essential when a person's health care or participation in clinical research is considered. The purpose of informed consent in this type of research is mainly to protect research participants from physical harm by providing a description of the potential risks and benefits of the study. In contrast, in information-based research that relies solely on medical records and stored biospecimens, the research participant faces no risk of direct physical harm. In this context, informed consent (authorization) is intended to ensure that individuals are able to exercise control over their personal information that is held by third parties, and to give individuals the right to determine whether their personal information can be used in a particular research project (or a series of such projects, if consent for future research is permitted). Because of these fundamental differences between information-based research and direct, interventional human subjects research, the committee makes a clear distinction between the privacy considerations that apply to interventional research and research that is exclusively information based.

First, the committee recommends that all interventional research, regardless of funding source and support, should be required to comply with the Common Rule,⁷ and all researchers who gain access to personally identifiable health information as part of the interventional research should be required to protect that information with strong security measures. Research participants should be allowed to provide consent for future research uses of data and biological materials collected as part of the interventional study as long as an IRB reviews and approves the future uses, ensuring that the new study is not incompatible with the original consent.

Second, the committee recommends that HHS and other relevant federal agencies develop a new approach to uniform, goal-oriented oversight of information-based research, with a focus on best practices in privacy, security, and transparency as in PHIPA and the proposed United Kingdom model. This new approach should include a mechanism by which some programs or institutions could be certified by HHS or another accrediting body, similar to a prescribed entity as in PHIPA or a safe harbor as in the United Kingdom model. Such entities could then collect and analyze personally identifiable health information for clearly defined and approved purposes, without individual consent. Because of the administrative requirements in becoming certified, this option is most appropriate for disease

⁷The "Common Rule" is the term used by 18 federal agencies who have adopted the same regulations governing the protection of human subjects of research.

registries and other very large scale research databases. Certified entities could also aggregate personally identifiable data from multiple sources, and then provide data to researchers with direct identifiers removed, under strict security requirements. This would facilitate greater use of data with direct identifiers removed in research because the aggregated datasets would be more complete and thus would lead to more accurate conclusions. To further protect privacy, unauthorized reidentification of information that has had direct identifiers removed should be prohibited by law, and violators should face legal sanctions.

In cases where researchers cannot use data with direct identifiers removed, and personally identifiable health information is needed for research, approval and oversight by an ethics oversight board should be required, partially analogous to what is now done under the HIPAA Privacy Rule and PHIPA. This board could perhaps entail a new body specifically formulated to review medical records research, rather than relying on traditional IRBs that were created to review interventional research. If researchers seek a waiver of patient consent, an ethics oversight board should consider the measures the researchers propose to take to protect the privacy and confidentiality of the data, the potential harms that could result from disclosure of the data, and the potential public benefits of the proposed research study. In order to facilitate consistent application of this option, HHS will need to develop clear guidance and best practices on how to assess the potential harm, the proposed measures to protect privacy and confidentiality, and the potential public benefits of a research study, as has been done under PHIPA.

Although expectations regarding privacy vary among different demographic groups, public opinion polls suggest that a significant portion of the American public would like to control all access to their medical records for research via an individual consent mechanism. However, obligations to implement comprehensive privacy protections—such as security, transparency, and accountability—are independent of patient consent. Moreover, the committee concluded, based on considerable testimony and other evidence, that a universal requirement for informed consent can lead to invalid results because of significant differences between patients who do or do not grant consent, and missed opportunities to advance medical science because it can be prohibitively costly and difficult to obtain consent for studies that require analysis of very large datasets. As a result, the committee's new framework includes two alternatives to consent that can be used in certain circumstances (e.g., disclosure to a certified entity and waiver of informed consent by an ethics review board), which are intended to facilitate research that is socially beneficial and to protect privacy through increased security, transparency, and accountability.

If society seeks to derive the benefits of medical research in the form of

improved health and health care, information should be shared to achieve that greater good, and governing regulations should support the use of such information, with appropriate oversight. In the committee's proposed new framework, the greater emphasis on ensuring the security protections of personally identifiable health information (as in the Committee's Recommendation III.A), facilitating research using data with direct identifiers removed, and ensuring the scientific merits of any proposed research in the new framework should help to foster its acceptability. Nonetheless, effective communication with the public about how health research is done and the value it provides (the committee's Recommendation III.C) will be important to address concerns and gain acceptance.

RECOMMENDATION II. REVISE THE PRIVACY RULE AND ASSOCIATED GUIDANCE

If this comprehensive new approach is not implemented (or, for the interim while the new framework is being developed), the committee proposes as an alternative that HHS revise the current HIPAA Privacy Rule and the associated guidance. These revisions would address some of the problems uncovered during the course of this study.

Recommendation II.A. The committee recommends that HHS develop guidance materials to reduce variability among IRBs and Privacy Boards in their interpretation of the HIPAA Privacy Rule as applied to research. One of the weaknesses in the current privacy protection system is that there is extreme variability in the regulatory interpretations and approval decisions among IRBs and Privacy Boards. Regulatory language often is not easily understandable and is subject to wide interpretation. Thus local IRBs and Privacy Boards interpret state and federal regulations independently, resulting in a great deal of variation in how the regulations are implemented. To address this problem, the committee developed four specific recommendations.

First, HHS should develop a dynamic, ongoing process to increase empirical knowledge about current "best practices" for privacy protection in responsible research using protected health information (PHI), and promote use of those best practices. To accomplish this, HHS should regularly convene consensus development conferences in collaboration with health research stakeholders to collect and evaluate current practices in privacy protection.

Second, HHS should encourage greater use of partially deidentified data called "limited datasets" and develop clear guidance on how to set up and comply with the associated data use agreements (DUAs) more efficiently and effectively. Currently, there is pervasive confusion regarding the conditions of DUAs and how recipients may meet those conditions. As

a result, in some health care settings, the burden of establishing a DUA prevents research from going forward. At the other extreme, some covered entities sign DUAs as a matter of course, providing little meaningful privacy protection to the patient.

Third, HHS should clarify the somewhat artificial distinction it has made between “research” and “practice” to ensure appropriate IRB and Privacy Board oversight of PHI disclosures for these closely related activities. This will require HHS to consult with relevant stakeholders to develop standard criteria for IRBs and Privacy Boards to use when making distinctions between health research and related endeavors, such as public health practice and quality improvement practices. These criteria should be evaluated regularly by HHS to ensure that the criteria are helpful and producing the desired outcomes.

Fourth, HHS should simplify the guidance regarding the use of PHI in activities preparatory to research and harmonize these provisions with the Common Rule. The committee recommends that all researchers (including those internal to a covered entity) be required to obtain IRB approval (as required under the Common Rule) prior to contacting potential research participants. When making a decision about whether to approve research projects, the IRB should review and consider the investigator’s plans for contacting patients, and ensure that the information will be used only for research projects approved by the IRB and will not be disclosed elsewhere.

Recommendation II.B. The committee recommends that HHS develop guidance materials to facilitate more effective use of existing data and materials for health research and public health purposes. Many institutions create and maintain databases with patient health information or repositories with biological materials collected from patients. These databases and biospecimen banks are used for many types of health research, including studies to understand diseases or to compare patient outcomes following different treatments. Current interpretations of provisions of the HIPAA Privacy Rule sometimes make it difficult to effectively use these valuable resources for health research. The committee developed four specific recommendations to facilitate important health research by maximizing the usefulness of patient data associated with biospecimen banks and in research databases, thereby allowing novel hypotheses to be tested with existing data and materials as knowledge and technology improve. The recommendations would align interpretation of the HIPAA Privacy Rule with the Common Rule on several points, simplify or clarify the relevant processes in research, and develop new tools for data aggregation.

First, the committee recommends that HHS develop guidance which clearly states that individuals can authorize use of PHI stored in databases

or associated with biospecimen banks for specified future research under the HIPAA Privacy Rule with IRB oversight, as is allowed under the Common Rule. Future uses should be described in sufficient detail to allow individuals to give informed consent, and researchers should be required to have IRBs determine that the new research is not incompatible with the initial consent. Second, the committee recommends that HHS develop clear guidance for use of a single form that permits individuals to authorize use and disclosure of health information in a clinical trial and to authorize the storage of their biospecimens collected in conjunction with the clinical trial. This will simplify the authorization process for interrelated research activities by integrating all relevant information into one simple document.

Third, the committee recommends that HHS clarify the circumstances under which DNA samples or sequences are considered PHI. Genetic information does not itself identify an individual in the absence of other identifying information, however, in some circumstances, a person's genetic code could be construed as a unique identifier in that it could be used to match a sequence in another biospecimen bank or databank that does include identifiers. The committee advocates a focus on strong security measures and the adoption of strict prohibitions and legal sanctions against the unauthorized reidentification of individuals from DNA by anyone.

Fourth, HHS should develop a mechanism for linking data from multiple sources so that more useful datasets can be made available for research in a manner that protects privacy, confidentiality, and security. One way this could be accomplished, for example, might be through data warehouses that are certified for the purpose of linking data from different sources. The organizations responsible for such linking would be required to use strong security measures and would maintain the details about how the linkage was done, should another research team need to recreate the linked dataset.

Recommendation II.C. The committee recommends that HHS revise provisions of the HIPAA Privacy Rule that currently hinder research but do not provide substantive privacy protections. First, HHS should reform the requirements for the accounting of disclosures (AOD) of PHI made for research and public health purposes. Until technology advances make automatic AOD tracking feasible, affordable, and widely available, the HIPAA Privacy Rule should permit covered entities to inform patients in advance that PHI might be used for health research with IRB/Privacy Board oversight or for public health purposes. As an alternative to AOD, to ensure transparency, institutions should maintain a list, accessible to the public, of all studies approved by an IRB/Privacy Board.

In addition, HHS should simplify the criteria that IRBs and Privacy Boards use in determining whether to waive the requirement that

researchers obtain authorization from each patient whose PHI will be used in a research study. If HHS decides to retain the current waiver criteria, HHS should provide clear and reasonable definitions to the vague terms used in the waiver criteria (i.e., what constitutes “minimal risk” to the privacy of individuals and what constitutes “impracticable”), as well as providing specific case examples. This would be especially helpful for multi-institutional studies, which fall under the jurisdiction of multiple IRBs or Privacy Boards.

RECOMMENDATION III. IMPLEMENT CHANGES NECESSARY FOR BOTH POLICY OPTIONS ABOVE (RECOMMENDATIONS I AND II)

The committee’s last set of recommendations do not directly relate to the HIPAA Privacy Rule, but should be adopted in order to achieve the committee’s overarching goals under both policy options described above (the new framework or revisions to the HIPAA Privacy Rule and associated guidance).

Recommendation III.A. The committee recommends that all health research institutions improve the security of personally identifiable health information. For example, institutions could: appoint a security officer responsible for assessing data protection needs and implementing solutions and staff training; make greater use of encryption and other techniques for data security; include data security experts on IRBs; implement a breach notification requirement, so that patients may take steps to protect their identity in the event of a breach; and implement layers of security protection to eliminate single points of vulnerability to security breaches. In addition, the federal government should support (1) the development and use of genuine privacy-enhancing techniques that minimize or eliminate the collection of personally identifiable data, and (2) standardized self-evaluations and security audits and certification programs to help institutions achieve the goal of safeguarding the security of personal health data.

Recommendation III.B. The committee also recommends that HHS—or, as necessary, Congress—provide reasonable protection against civil suits brought pursuant to state or federal laws for members of IRBs and Privacy Boards for decisions made within the scope of their responsibilities under the HIPAA Privacy Rule and the Common Rule. The limitation on liability should not include protection for willful and wanton misconduct in reviewing the research, but should instead be reserved for good-faith decisions, backed by minutes or other evidence. Effective oversight of health research depends on the recruitment of qualified and knowledgeable volunteers to serve on IRBs and Privacy Boards. But the increasing workload and complexity of IRB and Privacy Board service have made it difficult to recruit

and retain knowledgeable IRB members and to ensure time for the ethical reflection necessary to make appropriate decisions about human research projects. Moreover, because of the growth over the past decade of lawsuits naming individual IRB members as defendants, fear of penalties and civil suits can be a significant deterrent in recruiting qualified volunteers to serve on IRBs and Privacy Boards.

Recommendation III.C. Finally, the committee recommends that HHS and researchers take steps to provide the public with more information about health research. Surveys indicate that the vast majority of Americans believe health research is important, and they are interested in the findings of research studies. Yet patients often lack information about how health research is conducted and are rarely informed about research results that may have a direct impact on their health. The committee recommends that researchers inform interested research participants (who granted authorization for a particular study) with a simplified summary of the results at the conclusion of a research study. HHS should also encourage researchers to register their trials and other studies in public databases, particularly when the research is being conducted under a waiver of authorization. In addition, HHS and the health research community should work to educate the public about how research is done, and what value it provides. These recommendations could be accomplished without any changes to HIPAA or the Privacy Rule by making them a condition of funding for research grants from HHS and other research sponsors, and by providing additional funds to cover the cost.

BEYOND THE HIPAA PRIVACY RULE

Enhancing Privacy, Improving Health Through Research

Sharyl J. Nass, Laura A. Levit, and Lawrence O. Gostin, *Editors*

Committee on Health Research and the Privacy of Health Information:
The HIPAA Privacy Rule

Board on Health Sciences Policy

Board on Health Care Services

INSTITUTE OF MEDICINE

OF THE NATIONAL ACADEMIES

CONFIDENTIAL!

EMBARGOED UNTIL

WEDNESDAY, FEBRUARY 4, 2009,

AT 11:00 a.m. (EST)

THE NATIONAL ACADEMIES PRESS

Washington, D.C.

www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

The project is sponsored by the National Institutes of Health and the National Cancer Institute, the Robert Wood Johnson Foundation, American Cancer Society, American Heart Association/American Stroke Association, American Society for Clinical Oncology, Burroughs Wellcome Fund, and C-Change. 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 the project.

Library of Congress Cataloging-in-Publication Data

[to come]

Additional copies of this report 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, <http://www.nap.edu>.

For more information about the Institute of Medicine, visit the IOM home page at: www.iom.edu.

Copyright 2009 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

Suggested citation: IOM (Institute of Medicine). 2009. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Washington, DC: The National Academies Press.

*“Knowing is not enough; we must apply.
Willing is not enough; we must do.”*
—Goethe



INSTITUTE OF MEDICINE
OF THE NATIONAL ACADEMIES

Advising the Nation. Improving Health.

PREPUBLICATION COPY — Uncorrected Proofs.
Copyright © National Academy of Sciences. All rights reserved.

This executive summary plus thousands more available at <http://www.nap.edu>

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

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

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

Consultants

- SARAH M. GREENE, M.P.H.**, Group Health Center for Health Studies, Seattle, WA
- DAVID HELMS, Ph.D.**, President and CEO, AcademyHealth, Washington, DC

ROBERTA NESS, M.D., University of Pittsburgh, Pittsburgh, PA
JOY PRITTS, J.D., Health Policy Institute, Georgetown University,
Washington, DC
ED WAGNER, M.D., M.P.H., Director of the W.A. MacColl Institute
for Healthcare Innovation, Center for Health Studies, Group Health
Cooperative of Puget Sound, Seattle, WA
ALAN WESTIN, Ph.D., Privacy Consulting Group, Teaneck, NJ

Study Staff

SHARYL NASS, Ph.D., Study Director and Senior Program Officer
LAURA LEVIT, J.D., Associate Program Officer (Christine Mirzayan
Science and Technology Policy Graduate Fellow, December 2006 to
March 2007)
CATHERINE REYES, Ph.D., 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)
ROGER HERDMAN, M.D., Director, Board on Health Care Services
ANDREW POPE, Ph.D., Director, Board on Health Sciences Policy
JULIE WILTSHIRE, Financial Associate (until July 2007)
PATRICK BURKE, Financial Associate (from July 2007)

Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

CLARA D. BLOOMFIELD, M.D., Distinguished University Professor,
The Ohio State University Comprehensive Cancer Center and James
Cancer Hospital and Solove Research Institute, Columbus
ALEXANDER M. CAPRON, LL.B., Professor of Law and Medicine,
Gould School of Law, University of Southern California, Los Angeles
ANN CAVOUKIAN, Ph.D., Information and Privacy Commissioner of
Ontario, Office of the Information and Privacy Commissioner, Canada
DEBORAH COLLYAR, President, PAIR: Patient Advocates in Research,
Danville, CA
EDWARD GOLDMAN, LL.B., Associate Vice President and Deputy
General Counsel, University of Michigan Health System, Ann Arbor
EMMETT B. KEELER, Ph.D., Senior Mathematician, Pardee RAND
Graduate School, UCLA School of Public Health, Los Angeles, CA

BETSY KOHLER, M.P.H., C.T.R., Executive Director, North American Association of Central Cancer Registries (NAACCR), Springfield, IL
MELISSA L. MARKEY, Esq., Associate, Hall, Render, Killian, Heath & Lyman, P.L.L.C., Troy, MI
DEVON MCGRAW, J.D., Director, Health Privacy Project, Center for Democracy & Technology, Washington, DC
LYNNE WARNER STEVENSON, M.D., Director, Cardiomyopathy and Heart Failure Program, Brigham and Women's Hospital, Cardiovascular Division, Boston, MA
MARCY WILDER, Esq., Partner, Hogan & Hartson, L.L.P, Washington, DC

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations nor did they see the final draft of the report before its release. The review of this report was overseen by **Neal A. Vanselow, M.D.**, Chancellor Emeritus and Professor Emeritus of Medicine at Tulane University Medical Center, and **Bradford H. Gray, Ph.D.**, Editor, *The Milbank Quarterly*, and Principle Research Associate, The Urban Institute. Appointed by the National Research Council and the Institute of Medicine, they were responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Acknowledgments

The Committee is grateful to many individuals who provided valuable input and information for the study, either through formal presentations or through informal communications with study staff and Committee members. Contributors to the study include: Joan E. Bailey-Wilson (National Institutes of Health), Marianna Bledsoe (National Institutes of Health, Office of Science Policy), Stefan Brands (Credentica), Suanna Bruinooge (American Society of Clinical Oncology), Robert Califf (Duke Translational Medicine Institute), Fred H. Cate (Indiana University School of Law), Janlori Goldman (Columbia University, Mailman School of Public Health), Elizabeth Goss (American Society of Clinical Oncology), Sarah Greene (HMO Research Network), Christina Heide (Department of Health and Human Services, Office for Civil Rights), David Helms (Academy-Health), James Hodge (Johns Hopkins Bloomberg School of Public Health), Judd Hollander (Society for Academic Emergency Medicine), Holly Howe (North American Association of Central Cancer Registries), International Pharmaceutical Privacy Consortium, Katherine Kahn (University of California, Los Angeles), Anthony Knettel (Association of Academic Health Centers), Elizabeth Mayer-Davis (University of South Carolina), Roberta Ness (University of Pittsburgh), Rachel Nosowsky (Miller, Canfield, Paddock and Stone, PLC), Ann O'Mara (National Cancer Institute, Community Clinical Oncology Program), John Pandiani (The Bristol Observatory), Wendy Patterson (National Cancer Institute), Deborah Peel (Patient Privacy Rights), Joy Pritts (Georgetown Health Policy Institute), John Ring (American Heart Association), Kristin Rosati (Coppersmith Gordon Schermer & Brokelman PLC), Mark Rothstein (University of Louisville), Elaine Rubin

(Association of Academic Health Centers), Richard Schilsky (University of Chicago), Frank L. Silver (Registry of the Canadian Stroke Network), Lana Skirboll (National Institutes of Health, Office of Science Policy), Penelope Solis (American Heart Association), Ed Wagner (HMO Research Network), Alan Westin (Privacy Consulting Group), Marcy Wilder (Hogan and Hartson, L.L.P.), and Marsha Young (Booz Allen Hamilton).

Contents

Summary	1
Overview of Conclusions and Recommendations	15
Definitions, 16	
Definition of Privacy and Why Privacy Is Important, 16	
Definition of Health Research and Why Health Research Is Important, 19	
The HIPAA Privacy Rule, 21	
The Committee’s Charge and the Overarching Goals of the Recommendations, 22	
Improve the Privacy and Data Security of Health Information, 24	
Improve the Effectiveness of Health Research, 24	
Improve the Application of Privacy Protections for Health Research, 25	
The Committee’s Recommendations, 26	
I. Develop a New Approach to Protecting Privacy in All Health Research, 27	
II. Revise the Privacy Rule and Associated Guidance, 36	
III. Implement Changes Necessary for Both Policy Options Above, 55	
1 Introduction	63
Brief History of HIPAA and the Privacy Rule, 63	
Privacy and Health Research, 65	
Privacy Concerns, 65	

	The Concerns of Health Researchers, 66	
	Origins of the Study, 67	
	Committee Appointment and Charge, 68	
	Methods, 68	
	The Committee's Conclusions and Recommendations, 70	
	Framework of the Report, 72	
	References, 72	
2	The Value and Importance of Health Information Privacy	75
	Concepts and Value of Privacy, 75	
	Definitions, 75	
	The Importance of Privacy, 77	
	Public Views of Health Information Privacy, 78	
	Historical Development of Legal Protections of Health Information Privacy, 86	
	Principles of Fair Information Practice, 91	
	Security of Health Data, 93	
	The HIPAA Security Rule and Its Limitations, 94	
	Potential Technical Approaches to Health Data Privacy and Security, 100	
	Summary and Conclusions, 104	
	References, 105	
3	The Value, Importance, and Oversight of Health Research	111
	Concepts and Value of Health Research, 111	
	Definitions, 111	
	The Importance of Health Research, 112	
	Public Perceptions of Health Research, 119	
	Oversight of Health Research, 122	
	Historical Development of Federal Protections of Health Information in Research, 122	
	Overview of the Common Rule, 123	
	FDA Protection of Human Research Subjects, 131	
	Distinguishing Health Research from Practice, 131	
	Public Health Practice Versus Public Health Research, 133	
	Quality Improvement Versus Health Research, 136	
	The Importance of Effective Communication with the Public, 139	
	Disseminating Health Research Results, 139	
	Research Registries, 141	
	Informing the Public About the Methods and Value of Research, 142	
	Conclusions and Recommendations, 145	
	References, 148	

- 4 HIPAA, the Privacy Rule, and Its Application to Health Research 153
 - Overview of HIPAA, 153
 - Portability and Tax Provisions, 153
 - Administrative Simplification Provisions, 154
 - Development of the Privacy Rule Regulations, 155
 - Overview of the HIPAA Privacy Rule, 157
 - Entities Subject to the Privacy Rule, 157
 - Type of Information Protected, 158
 - Restrictions on Use and Disclosure, 159
 - Individual Rights, 160
 - HIPAA and Research, 162
 - Research Uses and Disclosures with Individual Authorization, 163
 - Research Uses and Disclosures Without Authorization, 167
 - Linking Data from Multiple Sources, 177
 - Genetic Information and the Privacy Rule, 180
 - Accounting for Research Disclosures, 181
 - Enforcement of the Privacy Rule, 184
 - Relationship Between HIPAA and Other Laws, 186
 - Federal Research Statutes, 186
 - General Federal Laws, 186
 - State Laws, 187
 - Conclusions and Recommendations, 188
 - References, 193

- 5 Effect of the HIPAA Privacy Rule on Health Research 199
 - Overview of Survey Results, 199
 - Association of American Medical Colleges Survey, 200
 - National Cancer Advisory Board Survey, 203
 - AHRQ Survey, 203
 - National Survey of Epidemiologists, 204
 - HMO Research Network Survey, 204
 - AcademyHealth Survey, 206
 - American Heart Association/American College of Cardiology Survey, 206
 - North American Association of Central Cancer Registries, 207
 - American Society of Clinical Oncology Interviews, 208
 - Association of Academic Health Centers Focus Groups, 208
 - Selection Bias, 209
 - General Studies of Consent and Selection Bias, 210
 - HIPAA Authorization and Selection Bias, 212
 - Efficiency of Research, 214
 - Cost and Time, 214
 - Recruitment, 218

IRB and Privacy Board Oversight, 220	
Business Associate Agreements, 227	
International Collaboration, 228	
Abandoned Studies, 228	
Deidentified Information, 230	
Access to Deidentified Data, 230	
Quality of Deidentified Data, 232	
Authorization Process, 233	
Concerns About Potential Legal Consequences, 234	
Potential Ways to Reduce Interpretive and Variability Among IRBs, Privacy Boards, and Covered Entities, 235	
Conclusions and Recommendations, 239	
References, 240	
6 A New Framework for Protecting Privacy in Health Research	245
Review of the Limitations of the Privacy Rule, 247	
Improve the Privacy and Data Security of Health Information, 247	
Improve the Effectiveness of Health Research, 253	
Improve the Application of Privacy Protections for Health Research, 255	
The New Framework, 257	
Examples of Informative Models, 258	
The Committee's Recommendation, 264	
The Role of Informed Consent in the New Framework, 266	
The New Framework Addresses the Overarching Goals, 269	
Improving the Privacy and Data Security of Health Information, 269	
Improving the Effectiveness of Health Research, 271	
Improving the Application of Privacy Protections for Health Research, 272	
Relevance of the Recommendation to Other Federal Actions, 272	
Conclusions and Recommendations, 279	
References, 281	
Appendixes	
A Previous Recommendations to the Department of Health and Human Services	285
B Commissioned Survey Methodology	293
C Committee Member and Staff Biographies	301
Glossary	311