

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



BEYOND THE
HIPAA PRIVACY RULE

Enhancing Privacy, Improving Health Through Research



INSTITUTE OF MEDICINE

Committee Charge

- To investigate the effects of the HIPAA Privacy Rule on health research:
 - Examining a range of research types (e.g. clinical trials, epidemiology, data repositories, public health research...)
 - Includes research sponsored by government, academia, and for-profit organizations
 - Looking at interpretation of the regulation vs. requirements of the regulation
- To seek ways to balance patient privacy against researchers' need for identifiable health information

Types of Recommendations Considered

- Changes in interpretation of the regulation through the release of new guidance documents
- Changes to the Privacy Rule regulation
- Changes to HIPAA (the Act)
- Beyond HIPAA (new legislation, HHS initiatives not specified by HIPAA, or voluntary activities by holders of health data)

Surveys of the Research Community

- **Survey of US Epidemiologists (IOM Commissioned)**
PI: Roberta Ness, MD, MPH, University of Pittsburgh
JAMA, November 14, 2007—Vol 298, No. 18
- **Surveys of the HMO Research Network (IOM Commissioned)**
Surveys of Researchers and IRB Administrators
PIs: Ed Wagner, MD, MPH and Sarah Greene, MPH
Group Health Center for Health Studies
- **Survey of AcademyHealth Members**
David Helms, PhD, AcademyHealth
- **Survey of AHA/ACC Members**
- **Qualitative Evidence Gathering Projects**
ASCO Structured Interviews and AAHC Focus Groups

Summary of Researchers' Concerns

The Privacy Rule, as interpreted by covered entities, has:

- Increased the cost and time of research projects
- Complicated recruitment and increased selection bias
- Confused participants regarding their rights and protections
- Led researchers to abandon important studies
- Created barriers to the use of patient specimens
- Failed to create an effective way to conduct studies with de-identified data

Harris Survey: Public Attitudes Towards Health Research And Privacy

- IOM commissioned survey
- Web-based survey conducted Sept 11 - 18, 2007
- 2,392 respondents
- Included closed and open-ended questions

Summary of Harris Survey

- 70% of respondents trust health researchers to protect privacy
- 8% of respondents had declined to allow information for research
 - 30% of refusers concerned about privacy
- Attitudes towards notice and consent
 - 28% of respondents grant researchers access to their PHI without giving specific consent for each research project
 - 38% of respondents wanted to be to consent to each research study
 - 13% of respondents did not want researchers to contact them or use their PHI in research under any circumstances
 - 20% of respondents were unsure

Committee's Conclusions

- 1) Privacy protections and health research both benefit individuals and society as a whole, so we should strive to support both to the extent possible.

Committee's Conclusions

2) The HIPAA Privacy Rule does not protect privacy as well as it should.

and

3) As currently implemented, the HIPAA Privacy Rule impedes important health research.

Privacy Rule falls short

- Overstates the ability of informed consent to protect privacy
- Fails to protect privacy through security, transparency, and accountability
- Imposes burdensome procedures that offer little privacy protection

Privacy Rule falls short

- Inconsistent application, depending on holder of data, source of data
- Discrepancies with other regulations
 - May offer less protection than Common Rule
- Impedes research that is exclusively information-based

Privacy Rule falls short

- Inconsistent interpretation and implementation by covered entities
- Creates new challenges for multi-institutional research

Committee's Overarching Goals

- 1) Improve the privacy and data security of health information.
- 2) Improve the effectiveness of health research.
- 3) Improve the application of privacy protections for health research.

Recommendations

- The Committee's first and foremost recommendation is that **HHS should develop a new framework for protecting privacy in health research**
- Alternatively, HHS should revise the Privacy Rule and associated guidance
- The Committee also recommends changes, independent of the Privacy Rule, that are necessary for either policy option

New Framework

- **Congress should authorize a new approach to ensuring privacy that would apply uniformly to all health research.**
- **The new approach would enhance privacy protections through improved security, transparency and accountability.**
- **HHS should exempt health research from the HIPAA Privacy Rule.**

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.**
- **Goal-oriented, rather than prescriptive, regulations.**
- **Distinguish interventional research and research that is exclusively information based.**
- **Certify institutions that have policies and practices to protect data privacy and security.**
- **Facilitate greater use of deidentified data in health research, and include legal sanctions for unauthorized reidentification.**

The new approach should do all of the following:

- **Require ethical oversight of research using personally identifiable health information without informed consent.**

Oversight should consider:

- **Measures to protect the confidentiality of the data;**
 - **Potential harms from disclosure; and**
 - **Potential public benefits of the research.**
- **Require strong data security safeguards.**
 - **Include federal oversight and enforcement to ensure regulatory compliance.**

Alternative Policy Option

Revise the HIPAA Privacy Rule and associated guidance.

HHS should:

- Reduce interpretive variability through revised and expanded guidance and harmonization
- Develop guidance materials to facilitate more effective use of existing data and materials for research
- Revise some provisions of the HIPAA Privacy Rule that currently hinder research but that do not provide meaningful privacy protections

Reduce Variability in Interpretation of the Privacy Rule

HHS should:

1. Promote “best practices” for privacy protection in responsible research
2. Expand use and usability of data with direct identifiers removed to enhancing privacy in research
3. Clarify the distinctions between “research” and “practice” to ensure appropriate IRB and Privacy Board oversight
4. Facilitate appropriate oversight of identification and recruitment of potential research subjects

Facilitate Effective use of Existing Data and Materials

HHS should:

1. Facilitate use of repositories for responsible health research
2. Simplify authorization for interrelated research activities
3. Clarify the circumstances under which DNA samples or sequences are considered protected health information
4. Facilitate linking of health data from multiple sources for research

Revise Provisions of the Privacy Rule

HHS should:

1. Reform the requirements for the accounting of disclosures of protected health information for research
2. Simplify the criteria for waiver of patient authorization for the use of protected health information in research

Changes Necessary for Both Policy Options:

1. Safeguard personal health information
2. Protect members of Institutional Review Boards and Privacy Boards who serve in good faith
3. Disseminate research results to study participants and the public
4. Educate the public about how research is done and what value it provides

Potential Security Measures

- Appointing a security officer
- Increasing use of encryption and other techniques for data security
- Including a data security expert on IRBs
- Implementing a breach notification requirement, so that patients may take steps to protect their identity in the event of a breach
- Implementing layers of security protection, and eliminate single points of vulnerability to security breaches
- Supporting the development and use of genuine privacy-enhancing techniques that minimize or eliminate the collection of personally identifiable data
- Creating standardized self-evaluations and security audits, and certification programs to help institutions achieve the goal of safeguarding the security of personal health data.

Acknowledgments

Committee Members:

Lawrence O. Gostin, JD (Chair)
Georgetown University Law Center

Paul S. Appelbaum, MD
Columbia University Medical Center

Elizabeth Beattie, Ph.D.
The Queensland University of Technology

Marc Boutin, JD
National Health Council

Thomas W. Croghan, MD
Mathematica Policy Research, Inc.

Stanley W. Crosley, Esq.
Eli Lilly and Company

Sandra Horning, MD
Stanford University School of Medicine

James S. Jackson, Ph.D.
University of Michigan

Mary Beth Joubanc, JD
Arizona Government Technology Agency

Bernard Lo, MD
University of California, San Francisco

Andrew F. Nelson, MPH
HealthPartners Research Foundation

Marc Rotenberg, JD
Electronic Privacy Information Center

Wendy Visscher, Ph.D.
Research Triangle Institute

Fred Wright, MD
VA Connecticut Healthcare System

Clyde W. Yancy, MD
Baylor University Medical Center

IOM Staff:

Sharyl Nass, PhD Study Director

Laura Levit, JD Associate Program Officer

Roger Herdman, MD Director, Board on Health Care Services

Andrew Pope, PhD Director, Board on Health Sciences Policy

Study Funders

National Institutes of Health
American Cancer Society
Burroughs Wellcome Fund

National Cancer Institute
American Heart Assn.
C-Change

Robert Wood Johnson Foundation
American Society for Clinical Oncology

For more information....



**BEYOND THE
HIPAA PRIVACY RULE**

Enhancing Privacy, Improving Health Through Research



www.iom.edu/hipaa

Or

www.nap.edu