Privacy of Health Information

A Report on the 2001 Public Interest Colloquium
Held March 2-3, 2001
Washington, D.C.
Health Lawyers deeply appreciates the following foundations’ support of the 2001 Public Interest Colloquium and Report, _Privacy of Health Information:_
- BlueCross BlueShield of Tennessee Foundation
- California Healthcare Foundation, Oakland, CA
- Human Rights Campaign Foundation
- Mary B. Vanderbeek Foundation
- Tenet Healthcare Foundation

Health Lawyers sincerely thanks the individuals and law firms listed below for their generous donations in support of the 2001 Colloquium, _Privacy of Health Information_, and the Association’s ongoing Public Interest activities.

**Patrons**
- Eli Lilly and Company
- Epstein Becker & Green
- Genentech, Inc.
- Goulston & Storrs
- Healthcare Leadership Council
- Haynes & Boone, LLP
- King & Spalding
- Reed Smith, LLP

**Benefactors**
- American Hospital Association
- Baker Donelson Bearman & Caldwell
- Baker & Hostetler, LLP
- Timothy P. Blanchard, Esq.
- Calfee Halter & Griswold, LLP
- Coppersmith Gordon Schermer
- Owens & Nelson, PLC
- First Chesapeake Group, Inc.
- Gardner Carton & Douglas
- Douglas A. Hastings, Esq.
- Husch & Eppenberger, LLC
- Mark A. Kadzielski, Esq.
- Thomas C. Shields, Esq.
- Jennifer A. Still, Esq.
- T.J. Sullivan, Esq.
- Sanford A. Teplitzky, Esq.
- Harvey M. Tettlebaum, Esq.
- Tufts Health Plan

**Contributors**
- Michael F. Anthony, Esq.
- Elisabeth Belmont, Esq.
- Katherine Benesch, Esq.
- Almeta E. Cooper, Esq.
Privacy of Health Information

# Table of Contents

Contributors ....................................................... Inside Front and Back Covers  
Preface: In the Public Interest ........................................ iv  
Acknowledgments ..................................................... vi  
Colloquium Participants ........................................... vii  
Colloquium Topic Selection Criteria and Colloquium Objectives ........ viii  
Core Questions ....................................................... ix  

**Colloquium Report**  
Executive Summary .................................................. 2  
Welcome and Introductions ......................................... 8  
Core Question One: What Are the History, Politics, and Public Policy Goals of Laws to Protect the Privacy of Health Information? .... 10  
    Timeline: Major Federal Privacy Laws, Regulations, and Other Developments ........................................ 16  
Core Question Two: What Are the Legal Issues in the Current Debate on Privacy of Health Information? ................................. 20  
Core Question Three: What Are the Economic Issues in the Current Debate on Privacy of Health Information? ................................. 36  
Core Question Four: What Are the Areas of Consensus and Points of Tension in the Debate on Privacy of Health Information? ...... 40  
Appendix A: Breakout Sessions Consider Health System Changes, Cyber Issues, and Balancing Protections with Legitimate Use .................. 46  
Appendix B: Highlights of the Final HIPAA Privacy Regulations ........ 50  
Appendix C: What Is Health Information? ............................ 55  
Appendix D: State Healthcare Privacy Laws .......................... 59  
About the American Health Lawyers Association ....................... 61  
American Health Lawyers Association  
Leadership and Staff .................................................. 62
Preface: In the Public Interest

“...and to serve as a public resource on selected healthcare legal issues.” — From the mission statement of the American Health Lawyers Association

This report summarizes the American Health Lawyers Association’s 2001 Public Interest Colloquium, *Privacy of Health Information*. The Colloquium was held March 2-3, 2001, in Washington, DC.

As chair of our Association’s 2000-2001 Public Interest Committee, I am pleased to present this Colloquium Report to health policymakers, the healthcare industry, the media, our members, and the public as Health Lawyers’ nonpartisan contribution to the debate on this important policy issue.

Privacy of individually identifiable health information has emerged as one of today’s most highly charged public policy issues. Adding great complexity to the debate is the development of new information technologies, and the rapid adoption of those technologies by many sectors of the economy, including healthcare. Computers, the Internet, and other information technologies are transforming the methods by which personal healthcare information is acquired, used, disclosed, and stored. The maintenance and exchange of personal healthcare information is now an integral component in the organization, delivery, and financing of modern healthcare services.

The controversy over privacy of health information arises from two conflicting public “goods”: (1) Protection of individually identifiable medical data, and (2) The legitimate use of such data by caregivers, payors, researchers, and others.

On the one hand, individuals rightfully expect an assurance of confidentiality so they will feel free to give their physicians detailed information about their health conditions and behavior—information that is needed for effective diagnosis and treatment. Unauthorized use and disclosure of confidential medical information can subject individuals to embarrassment, social stigma, and discrimination.

On the other hand, healthcare providers, public and private payors, and suppliers and vendors of healthcare ancillary and support services rely on the provision of such information in order to administer healthcare benefits, accurately and promptly process claims for payment, determine benefit eligibility and risk adjustment mechanisms, detect and prevent fraud and abuse, and review the appropriateness, efficiency, and quality of care received by beneficiaries.

What is the appropriate balance of privacy protection and legitimate use? That question lies at the center of the current debate. Finding that “balance” was also the goal of much of the discussion at the 2001 Colloquium.

Conducted every two years, Health Lawyers’ Colloquiums provide a forum for an in-depth, nonpartisan examination of a complex health policy issue that has a clear legal nexus. The meetings feature discussion by a roundtable of experts who represent major interests that are involved with the Colloquium’s topic. The 24-member panel for the 2001 Colloquium included health policy analysts, government officials, health consumer representatives, data/technology experts, and healthcare industry representatives.

To ensure a free exchange of ideas on health policy topics that often provoke intense partisan debate, Colloquiums are conducted without an audience. This report preserves confidentiality of the views expressed in the meeting by not attributing comments to specific participants.

The Colloquium discussion was facilitated by members of Health Lawyers’ Public Interest Committee and other volunteer leaders. Over the course of one-and-one-half days, the Colloquium panel examined and discussed privacy of health information in the context of four core legal questions:

1. What are the history, politics, and public policy goals of laws and regulations governing the privacy of health information?
2. What are the legal issues in the debate on health information privacy, including: application, jurisdiction, use and disclosure, individual rights, a framework for a legal response, and regulatory compliance and enforcement?
3. What are the economic issues in the debate on privacy of health information?

4. What are the areas of consensus and points of tension in the current debate?

The panel explored the core questions in general discussions and in three breakout sessions that examined privacy protection in an evolving healthcare system, privacy protection in the Digital Age, and balancing protection with legitimate uses of health information.

In December 2000, the Department of Health and Human Services (HHS) published final privacy regulations, as required by the Health Insurance Portability and Accountability Act of 1996 (HIPPA). Those regulations, and the proposed regulations that preceded them, provoked intense debate in the health policy community. At the time of the Colloquium, a host of health-related organizations were preparing comments on the final HIPAA regulations, and Washington was abuzz with speculation on whether HHS would, in fact, allow the rules to become effective. Health Lawyers’ 2001 Colloquium focused on the broad policy considerations relating to privacy of health information. Issues arising from the HIPAA regulations were discussed throughout the Colloquium, but panelists graciously complied with Health Lawyers’ request that the Colloquium not become a debate on the HIPAA rules. Broad topics such as protections for genetic information were addressed, as were fundamental questions such as individual and organizational rights and responsibilities with respect to the use and disclosure of health information. State laws and regulations governing sensitive health information were also discussed.

This report summarizes the Colloquium discussion, including points of consensus and points of tension that emerged from the panel’s deliberations. The report also contains four sidebar articles, written by staff of Deloitte & Touche, LLP, that provide helpful information on the history of health information privacy laws and regulations, highlights of the final HIPAA privacy regulations, state privacy laws, and the meaning and uses of “health information” in today’s complex healthcare system.

We believe readers will gain an appreciation of the complex issues involved in the debate on privacy of health information. We are pleased to present this report on the 2001 Public Interest Colloquium as Health Lawyers’ nonpartisan contribution to the debate on privacy of health information.

Almeta E Cooper, Esq.
2000-2001 Chair
Public Interest Committee
Acknowledgments

This report on the 2001 Colloquium, Privacy of Health Information, reflects the commitment, hard work, and support of a number of dedicated individuals.

First, Health Lawyers is deeply grateful to the many contributors—foundations, individuals, law firms, healthcare organizations, and businesses—whose generous donations helped make possible the Colloquium and this report. Their names are listed on the inside front and back covers of the report.

Second, Health Lawyers sincerely thanks the members of the Colloquium panel. Their willingness to take the time from their schedules to participate in a one-and-one-half-day meeting (including part of a weekend) is deeply appreciated. Their knowledge, energy, and spirit of cooperation produced the thorough, nonpartisan discussion of health information privacy that is summarized in this report.

Appreciation also goes to Health Lawyers’ Board of Directors and, in particular, the members of the 2000-2001 Public Interest Committee. Without their commitment, dedication, and months of planning, the Colloquium would not have occurred. Special thanks go to the following committee members and volunteer leaders who acted as facilitators at the Colloquium: Almeta E. Cooper (chair), Elisabeth Belmont, Alan S. Goldberg, Douglas A. Hastings, Thomas Wm. Mayo, Beth J. Schermer, Nancy J. Severson, and Jennifer A. Stiller. These members and committee member Adele A. Waller also provided valuable assistance through their technical review of the draft report.

Health Lawyers also sincerely thanks Deloitte & Touche LLP for its technical assistance on topics covered in sidebar articles in the report. Health Lawyers gratefully acknowledges the work of the firm’s senior manager, Lisa L. Dahm, who wrote the following articles: “Timeline: Major Federal Privacy Laws, Regulations, and Other Developments,” “Highlights of the Final HIPAA Privacy Regulations,” “What Is Health Information?” and “State Healthcare Privacy Laws.” The sidebar articles provide general information only and should not be relied on for legal or other professional advice or services. The sidebar articles are not a substitute for such professional advice or services, and Deloitte & Touche LLP shall have no liability to any person or entity who relies on such articles.

Finally, Health Lawyers acknowledges and thanks our association staff, whose interdepartmental teamwork was essential to the success of the Colloquium and the publication of this report. Special thanks go to Peter M. Leibold, Executive Vice President/CEO and Joseph A. Kuchler, Director of Public Interest, for his work as project director of the Colloquium and writer/editor of this report. Health Lawyers also sincerely appreciates the support provided by Mary Boutsikaris, Art Director/Graphic Designer; Rita Brinley, executive assistant; and Dionne Harris, temporary project assistant.
Colloquium Participants

Panelists

Elisabeth Belmont, Esq.
Corporate Counsel
MaineHealth
Portland, ME

Paula Bruening
Staff Counsel
The Center for Democracy
and Technology
Washington, DC

Bette-Jane Crigger, Ph.D.
Editor, IRB
The Hastings Center
Garrison, NY

Donna Z. Eden, Esq.
Senior Attorney
Office of the General Counsel
Health Care Financing Administration
Baltimore, MD

J. Michael Fitzmaurice, Ph.D., FACMI
Senior Science Advisor for Information Technology
Immediate Office of the Director
Agency for Healthcare Research and Quality
Rockville, MD

Robert Gellman
Privacy and Information Policy Consultant
Washington, DC

Alan S. Goldberg
Goulston & Storrs PC
Boston, MA

Jennifer Goldberg Low
Associate General Counsel
Express Scripts, Inc.
Maryland Heights, MO

Mary R. Grealy
President
Healthcare Leadership Council
Washington, DC

Melinda Hatton
Vice President and Chief Healthcare Counsel
American Hospital Association
Washington, DC

Mark Hayes
Health Policy Director
Committee on Health, Education, Labor & Pensions
Washington, DC

Joseph Holahan
Director and Counsel for Policy Development
Health Insurance Association of America
Washington, DC

Joanne L. Hustead
Senior Counsel
Health Privacy Project
Institute for Health Care Research and Policy
Georgetown University
Washington, DC

David Korn, MD
Senior Vice President for Bioethics and Health Services Research
Association of American Medical Colleges
Washington, DC

Christopher Labonte
Senior Policy Advocate
The Human Rights Campaign
Washington, DC

Keith Malone
Chief Privacy Executive
McKesson HBOC, Inc.
San Francisco, CA

Craig A. Nulan
HIPAA/Security Practice Director
Cerner Corporation
Kansas City, MO

Lee Peeler
Associate Director
Division of Advertising Practices
Federal Trade Commission
Washington, DC

Anne Phelps (unable to attend)
Special Assistant to the President for Health Policy
The White House
Washington, DC

Marjorie E. Powell
Assistant General Counsel
Pharmaceutical Research and Manufacturers of America (PhRMA)
Washington, DC

Ross Rubin, Esq.
Vice President of Legal Affairs
American Medical Association
Chicago, IL

Louis J. Saccoccio
General Counsel
American Association of Health Plans
Washington, DC

Professor LaTanya Sweeney
Carnegie Mellon University
Heinz School of Public Policy and Management
Pittsburgh, PA

Bernice R. Welles, MD
Senior Director
Genentech, Inc.
South San Francisco, CA

Joy Johnson Wilson
Senior Committee Director, Health
National Conference of State Legislatures
Washington, DC

Steven Wojcik (unable to attend)
Director of Public Policy
Washington Business Group on Health
Washington, DC

2000-2001 President, Health Lawyers Board of Directors

Beth J. Schermer, Esq.
Coppersmith, Gordon, Schermer, Owens & Nelson PLC
Phoenix, AZ

2000-2001 President-elect, Health Lawyers Board of Directors

Douglas A. Hastings, Esq.
Epstein Becker & Green
Washington, DC

2000-2001 Public Interest Committee

Almeta E. Cooper, Esq., Chair
Ohio State Medical Association
Hilliard, OH

Daniel B. Higgins, Esq.
Paul, Hasting, Janofsky & Walker
San Francisco, CA

Thomas Wm. Mayo, Esq.
Haynes and Boone, LLP
Southern Methodist University School of Law
Dallas, TX

Nancy J. Severson, Esq.
Denver, CO

Jennifer A. Stiller, Esq.
Haverford, PA

T. J. Sullivan, Esq.
Gardner Carton & Douglas
Washington, DC

Adele A. Waller, Esq.
Bell Boyd & Lloyd
Chicago, IL

Glenn A. Reed, Esq., Ex Officio
King & Spalding
Atlanta, GA

Staff

Peter M. Leibold
Executive Vice President/CEO
American Health Lawyers Association
Washington, DC

Joseph A. Kuchler
Director of Public Interest
American Health Lawyers Association
Washington, DC

Rita Brinley
Executive Assistant
American Health Lawyers Association
Washington, DC
Colloquium Criteria and Objectives

Colloquium Topic Selection Criteria

The topic selected for a Health Lawyers’ Colloquium must be one that:
- Is in the public interest or has a charitable component;
- Has a clear legal nexus;
- Is timely;
- Draws diverse constituency participation; and
- Is practical.

Colloquium Objectives

1. To provide a neutral forum that provides a frank exchange of views and analyses among various constituency groups with differing, and sometimes adverse, points of view. To explore the basis for these differences and identify ways and means of accommodating the differences in the course of pursuing their respective missions to serve the public interest.

2. To crystallize the intersection of policy, business, and regulatory issues in an effort to have a constructive impact on the substantive debate over these issues.

3. To create opportunities for representatives of different groups to identify shared goals and interests and to develop potential collaborative working relationships.

4. To publish a report based on the findings of the Colloquium. To disseminate the report to Health Lawyers members, participating constituency groups, policy and law makers, academicians, and others in order to educate key players in the debate and those who are charged with advising clients on these matters.

5. To provide an environment throughout the Colloquium that allows for the free exchange of views and articulation of tensions while preserving confidentiality and appropriate anonymity for Colloquium participants in the written report.
Core Questions

1. What Are the History, Politics, and Public Policy Goals of Laws to Protect the Privacy of Health Information?

- To what extent should individuals have an expectation of privacy in their personal health information?
- What laws, regulations, and judicial opinions are already in place or under consideration at the federal, state, and local levels to protect the privacy of health information?
- What are the public interest goals of laws to protect the privacy of health information?
- What “competing values” do these laws and proposed laws strive to balance?
- How effective are current laws in protecting privacy of health information?

2. What Are the Legal Issues in the Current Debate on Privacy of Health Information?

a. Applicability Issues

- What types of health information should be protected? Should there be more stringent rules for certain types of health information such as genetic information, HIV test results and AIDS records, mental health and developmental disability records, alcohol and drug abuse diagnosis and treatment records, and sexually transmitted disease records?
- For which types of health information should there be less stringent rules?
- Should individually identifiable health information from persons detained in the justice system be subject to different rules?
- Should law enforcement officials have access to protected health information without requiring a judicial order, grand jury subpoena, or administrative request?
- Which levels of government officials should have access? Which individual officials?
- What types of healthcare entities (e.g., institutions, medical personnel, employers, individuals) should be subject to federal medical privacy laws? Should certain entities be exempt?
- How should privacy protections apply to “business associates” and other secondary users of individually identifiable health information?
- How can privacy interests be reconciled with laws and regulations relating to research projects and protection of human subjects? When do clinical research and healthcare operations overlap?

b. Jurisdictional Issues

- Should federal law preempt all state medical privacy laws or should it serve as a “floor,” letting stand state laws that offer broader protections?
- Is there potential for overlap with existing federal rules or programs (for example, ERISA, Federal Privacy Act, Federal Alcohol and Drug Abuse laws and regulations, Department of Defense, VA and Federal Employees Health Benefits programs, E-Signature directive, Gramm-Leach-Bliley Act, European Union directives)?
- What role should courts have in enforcing privacy laws?

c. Use and Disclosure Issues

- How do individuals’ expectations differ with respect to the “use” versus “disclosure” of individually identifiable health information? What is the difference between use and disclosure?
- What is an individual’s health information “identity” in an era of computer-based communications and advances in biotechnology?
- Does an individual’s identity include cultural or ethnic information? When and how should that information be protected?
- When is health information no longer individually identifiable?
- What use or disclosure activities are appropriate for “de-identified” health information?
- Should protection of de-identified information be of unlimited duration? What protections can be provided to prevent future “re-identification” of health information?
Core Questions

When is use or disclosure of health information without specific individual authorization appropriate? With specific authorization?

Should use or disclosure of covered information be subject to a “minimum necessary” standard? How should that standard be defined?

d. Individual Rights Issues

What rights and liabilities should individuals have regarding the handling of their protected health information?

What protections should minors or incapacitated individuals have regarding the handling of their protected health information?

Should any class of covered entities be exempt from these individual rights-related requirements?

How long should individuals have access to their information?

Should records of disclosure be maintained?

Under what circumstances should individuals be denied access to inspect, copy, or amend part or all of their own information?

What are appropriate costs and processes for photocopying, printing, or electronically transmitting health information?

Should individuals have the right to preclude access by certain individuals or entities?

How should issues of “succession” be addressed (that is, information transferred to new owners of an organization following a merger or bankruptcy)?

Should federal law establish a private right of action for individuals to sue physicians, hospitals, health plans, or other entities that make unauthorized disclosures of confidential health information?

e. Framework for Legal Response to Privacy Issues

What legal approach or combination of approaches should be used to address privacy concerns?

Can a mixed government-industry approach, such as a limited antitrust exemption to allow uniform standards to be developed, be of assistance?

f. Regulatory Compliance and Enforcement Issues

If a regulatory approach is used —

What methods should government use to ensure compliance and encourage covered entities to develop a “culture of compliance”?

What steps can government take to ensure coordination among agencies in implementing laws and directives governing privacy?

What assistance should government offer to assist with compliance?

What types of sanctions or liabilities are appropriate for non-compliance?

Are additional penalties appropriate for intentional non-compliance?

What limits should be placed on government’s use of any personal health information that it obtains through compliance and enforcement activities?

What Are the Economic Issues in the Current Debate on Privacy of Health Information?

What types of costs and operational changes for all parties are involved with the implementation of federal medical privacy protections?

How should those costs be funded?

Which types of entities would bear the greatest economic burden? Are there ways to achieve parity in cost allocation?

What are the minimum security standards necessary to achieve privacy of individually identifiable health information, recognizing that different types of data (paper vs. electronic records) require different administrative and technological safeguards to ensure privacy? How should techniques to achieve privacy and security be developed in a manner to ensure scalability for the various covered entities?

What Are the Areas of Consensus and Points of Tension in the Debate on Privacy of Health Information?

On which issues is there clear consensus?

What are the areas of near-agreement?

On what issues does strong disagreement remain?
Privacy of Health Information
Executive Summary

This report summarizes the American Health Lawyers’ Association’s sixth Public Interest Colloquium, *Privacy of Health Information*. Held March 2-3, 2001, in Washington, DC, the Colloquium was a nonpartisan, in-depth panel discussion of the public interest aspects of laws, regulations, and policy considerations in the debate on privacy of health information. Over the course of one-and-one-half days, a 24-member panel composed of health policy analysts, government officials, consumer representatives, data/technology experts, and healthcare industry representatives explored four core legal questions:

1. What are the history, politics, and public policy goals of laws and regulations governing the privacy of health information?

2. What are the legal issues in the debate on health information privacy, including: application, jurisdiction, use and disclosure, individual rights, a framework for a legal response, and regulatory compliance and enforcement?

3. What are the economic issues in the debate on privacy of health information?

4. What are the areas of consensus and points of tension in the current debate?

The Colloquium panel’s discussion was wide-ranging. This summary presents highlights of each session and does not attempt to encapsulate the full discussion of each core question. Readers are encouraged to turn to the report for a full understanding of the 2001 Colloquium topic, *Privacy of Health Information*.

**Welcome and Identification of Goals**

The Colloquium was facilitated by members of Health Lawyers’ Public Interest Committee and other volunteer leaders. After welcoming the participants and outlining ground rules for the discussion, Health Lawyers’ chief moderator asked the panelists to identify a priority or goal that they particularly hoped the Colloquium would address. Goals identified included:

- Identifying the appropriate balance between privacy protection and legitimate use of health information;
- Gaining perspective on how health privacy fits into the debate on privacy in society at large, particularly as set against the reality of the Internet, sophisticated marketing techniques, and technological advances that threaten privacy every day;
- Ensuring access to data for medical research;
- Clarifying administrative issues and appropriate federal and state roles in protecting health information;
- Ensuring access to needed information for groups that might be subject to discrimination; and
- Discussion of health information privacy in the context of the Internet and e-commerce.

During the course of the Colloquium, several topics emerged as major themes that underlie the debate on privacy of health information. These include:

- The need for “transparency” in interactions between the health industry and consumers with respect to health information;
- The need for public education on beneficial uses of health information and the rights and responsibilities of the healthcare industry and consumers with respect to the use of health information;
- The need for the healthcare industry to develop a pervasive “culture of privacy” that includes both the use of security technology and the implementation of management processes and procedures to guard against breaches of privacy;
- Recognition that perfect privacy protection is a laudable but elusive goal. Protection of health information can be greatly improved, but “leaks” that re-identify individuals inevitably will occur, perhaps from human error, perhaps through inferences that sophisticated analysts draw from demographic data or other sources.

**Core Question One:**

**What Are the History, Politics, and Public Policy Goals of Laws to Protect the Privacy of Health Information?**

A second Health Lawyers moderator began the discussion of Core Question One with an overview of milestones in the evolution of laws to protect the privacy of health information. The overview was designed to complement background materials that participants received before the Colloquium and to provide a common basis for the panel’s discussions.
**Fundamental Expectations Regarding Health Information Privacy**

The panel engaged in a lengthy discussion of a basic policy question: To what extent should individuals have an expectation of privacy in their personal health information? Highlights of the discussion included:

- Expectations of privacy must include the recognition of certain underlying responsibilities. For example, individuals need to recognize their responsibility as members of society to allow de-identified data to be used for medical research or for the compilation of health statistics.

- Groups that are subject to discrimination are cautious about having their information released to users who, they believe, may use the information against them;

- Individuals generally are willing to share their health information for medical research or other legitimate uses, but they view personal consent as a prerequisite for such use. Generally, the public would like to be better informed on the ways in which their personal health information may be used;

- The phenomenal growth of the Internet and other developments in information technology have radically altered what individuals can realistically expect with respect to privacy of their personal information, including health information.

- Some segments of society, for example, prisoners and military personnel, enjoy few protections with respect to their health information. Technological advances, combined with a growing recognition of the commercial value of health information, may result in an erosion of personal autonomy in other segments of society.

**Public Interest Goals of Privacy Laws and Regulations**

The discussion of expectations of privacy segued into a new topic, the public interest goals of privacy laws and regulations. Much of the discussion centered on the need to balance privacy protection with uses that benefit society at large. Highlights included:

- For many individuals, the principal public interest goal likely would be protection against discriminatory use of their information by employers, insurers, or others.

- The public has high expectations of the healthcare system, but a “disconnect” occurs because most consumers do not understand how their information will be used to benefit society. They may not realize the role health information plays in medical research, quality assurance, and quality improvement. Ensuring public health and safety—for example, tracking whether birth defects are the result of environmental pollution—is another worthwhile use of health information;

- Most public interest goals can be achieved with de-identified data, that is, data from which obvious identifiers such as name and Social Security number have been removed. Total anonymity is a myth, however. It is sometimes possible to infer an individual’s identity from databases of public health information. One panelist reported that a recent analysis found that 87 percent of the United States population can be uniquely identified from publicly available databases by using just three pieces of information: date of birth, gender, and zip code.

**How Effective Are Current Privacy Laws?**

The panel concluded its discussion of Core Question One with a brief examination of the effectiveness of current privacy laws. Points raised during the discussion included:

- Some voices in the debate believe existing privacy laws do not provide sufficiently specific guidance on appropriate and inappropriate uses of health information. Others favor a less prescriptive approach and call for general guidelines centered on rights and responsibilities in the use of health information.

- Effectiveness involves two questions. First, how “good” are current laws? State privacy laws frequently are not comprehensive. They may apply to physicians, for example, but not to hospitals. Also, many privacy laws have not been updated to reflect changes in the healthcare system or advances in information technology. Second, are current privacy laws being complied with?
The Colloquium panel next discussed a variety of legal issues in the current debate, including application (covered information and covered entities), jurisdiction, use and disclosure, individual rights, and a framework for a legal response. The discussion revolved around three broad questions: (1) What types of health information are entitled to protection, and should some types receive heightened or reduced protection? (2) Which entities or individuals should be required to comply with privacy requirements? (3) What are appropriate and inappropriate uses of health information?

Applicability—Covered Information

The panel agreed that all health information is “sensitive” and should be protected by privacy laws. Attempts to differentiate among various diseases and conditions would end in frustration, the group concluded. Psychiatric notes warrant special protection, however.

The group held a lengthy discussion of genetic information and other data that might be used in a discriminatory fashion. Panelists disagreed on whether discrimination is appropriately addressed through privacy laws or through existing anti-discrimination statutes. Everyone agreed with one panelist that “as long as the conversation stays at 40,000 feet, it’s easy to agree on what should be protected.” For discrimination and other individual issues, however, “it’s the details.” The panel concluded that generally all information should be afforded protection because, in genetics, for example, new uses and linkages are continually being discovered. As one panelist expressed it, “The better approach long term for our society is to adequately protect all the information because we can’t tell today what’s going to be linked to something tomorrow.”

Applicability—Covered Entities

The panel’s discussion focused on the question, “Are there entities that should be excluded from coverage of a broad privacy rule, or that should be specifically included?” The final HIPAA privacy rules take a segmented approach, applying the federal standards to a variety of “covered entities.” Panelists differed in their views on the merits of this approach. Several argued that privacy standards should apply across the board, with an emphasis on the uses of information rather than the types of entities involved. Others defended the focus on entities, suggesting, as one panelist put it, “There are a variety of different users. You can’t apply the same standards to everybody.”

Jurisdiction

The panel focused next on federal preemption of state privacy laws, which one participant termed “a curiously emotional issue.” No consensus was reached, but the dialogue captured important issues in the debate. Points raised during the discussion included:

- Healthcare systems often transcend state borders. Patients may be employed and have healthcare coverage in one state, receive care in another jurisdiction, and have a prescription filled back in the first state. The need to comply with various states’ privacy requirements imposes a significant administrative burden, healthcare groups argued. Electronic health information now crisscrosses the country, adding a further layer of potential confusion.
- State governments acted to fill a vacuum on health information privacy. States do not categorically oppose preemption, a panelist said, but they are concerned that patients not lose state-level protections that are not included in the federal standards.
- Patient advocates believe state laws that are more stringent than the HIPAA privacy standards should be allowed to provide that extra level of protection. Moreover, establishment of the HIPAA privacy standards likely will lead to more uniformity among states, thus reducing the potential administrative burden on healthcare organizations.
- Unfortunately, preemption frequently is discussed as an either/or issue. The reality is that there are certain areas—encryption standards are one example—where national standards should prevail. On the other hand, states should be able to set their own requirements on certain matters that do not have national implications. Examples might include copying costs for patients’ access to their records or access to information by state officials for law enforcement purposes.
- The last comment prompted an exploration of potential areas of common ground. One panelist said calls for a list of national policy imperatives or for “carve outs” of areas where states could enact more stringent protections are “two sides of the same coin—are there areas for states and areas for federal protection?” The panelist suggested several activities where
consensus on federal preeminence appeared likely. “We could probably have uniformity in areas of research, both records-based and controlled trials. The area of public health is probably another area where we could achieve uniformity. Identifying the dead, again, [may be] an area for uniformity.”

**Use and Disclosure**

The panel briefly explored differences between “use” and “disclosure” and concluded that, while technical distinctions can be drawn, privacy regulations should not attempt to differentiate between the two terms. For individuals, a practical distinction may be the difference between the medical uses they believe will be made of their information versus how data actually may be disclosed to non-healthcare entities such as banks or their employers.

The panel focused extensively on issues relating to identification and de-identification, and how that affects the use and disclosure of protected individual health information. The final HIPAA privacy rules specify which personal identifiers should be excluded by covered entities. In terms of preserving anonymity, the HIPAA approach does not address de-identification “in a constructive way,” one panelist asserted, because it still may be possible to identify individuals through analysis of seemingly unrelated items such as age, gender, and zip code. Other panelists noted that most medical researchers are not interested in finding out an individual’s identity. Eliminating obvious personal identifiers such as names and Social Security numbers is sufficient for most research purposes, one panelist asserted. Researchers need “linkages” among the data so they can identify common medical traits or trends, but, on the whole, de-identification processes should be kept simple.

Panelists agreed that many healthcare organizations lack sophistication on data de-identification. New approaches under development by government agencies will help, however. One technique would establish a database of identifiable information against which researchers could run their analyses. Another approach would use “dummy data sets.” “You can still have the research. You can have as many different runs against the data as you wish without indentifiability,” a panelist explained. Another approach would be to clear requests for data through a “learned body,” similar to an institutional review board, that would screen data for potential identifiers and establish rules of use.

**Individual Rights**

This discussion addressed individuals’ responsibilities, as well as their rights, with respect to use of their personal health information. Highlights include:

- **What happens in other countries?** In Europe, for example, questions of individual rights do not arise in the same fashion as in the United States. A clear delineation of those rights, coupled with the presence of universal health insurance, creates a culture in which individuals share their health information as participants in a national health system. The panel recognized that the U.S. healthcare system and economy are radically different and that comparisons with other nations are not valid.

- **Participants generally agreed that individuals should have the right to amend their individual health record.** Such changes should provide clarification or additional information, however. They must not alter the original record. Changes also should be limited to current health information.

- **Individuals have certain responsibilities with respect to control of their health information.** They have a responsibility to become informed about what uses may be made of their information, and they have to consider the potential adverse consequences to their own health or the good of society if they arbitrarily deny access to their data.

**Framework for a Legal Response**

Discussion in this segment focused on the question of a “private right of action,” that is, whether individuals should be allowed to file lawsuits for alleged violations of privacy standards governing use of their health information. Major points in the discussion included:

- **Individuals are being asked to take more responsibility for their health information and how it is used.** Consumer advocates believe the public needs a private right of action at the federal level as protection against misuses of their information.

- **One health industry panelist suggested that the prospect of vigorous enforcement by government agencies, combined with recognition of the sanctions included in HIPAA and other laws, will provide sufficient protection from unwarranted breaches of privacy.** The government’s aggressive enforcement of fraud and abuse laws has made healthcare organizations—responsible providers as well as “bad actors”—acutely aware of the consequences of being found out of compliance with federal requirements.
Ambiguity is the major concern of healthcare organizations. The trade-off for the industry’s acceptance of a private right of action, another panelist suggested, might be “clarity in what a law or regulation seems to be saying is inappropriate [behavior].”

Core Question Three: What Are the Economic Issues in the Current Debate on Privacy of Health Information?

The panel’s discussion on Core Question Three focused on two issues: (1) minimum security standards needed to achieve privacy of health information; and (2) implementation costs.

Minimum Security Standards

Highlights of this discussion included:

- Compliance with the HIPAA privacy standards would require implementation of three technical security mechanisms—authentication, access control and authorization, and auditability, the panelist said. These mechanisms verify the identity of users, allow access only to authorized users and at the level authorized for a given user, and record and examine system use to identify possible violations. Credible systems are very expensive, however, and likely beyond the budgets of most healthcare organizations, the panelist said. Not even Fortune 50 companies have a “gold standard” of compliance, another panelist observed. The real issue is not sophisticated security systems, but the human factor. Most security breaches are created by people who have authorized access. To achieve acceptable security, the goal has to be balancing technical capabilities with training and processes that will make healthcare personnel aware of the need to protect privacy.

- Another panelist agreed that technology is not the major concern. Auditing systems can track every computer keystroke. The human factor actually causes most breaches of privacy. Healthcare workers may go to lunch and leave their computers running with a password prominently displayed on a sticky note affixed to their monitor, the panelist noted.

- Another panelist said academic medical centers represent a particularly difficult problem with respect to the use of “minimum necessary” information because their dual purpose—treatment and research—conflicts with privacy goals. Medical students are a major source of privacy breaches, one panelist suggested, because, in the interest of knowledge and patient care, they are inclined to share information widely. Other panelists disagreed with this assertion.

Implementation Costs

Major points in the panel’s discussion included:

- For physicians, implementation costs are an important consideration. Compliance with the privacy regulations will be very costly for a segment of the economy that already is highly regulated. Moreover, one panelist said, physicians worry that over time, the task of complying with federal privacy regulations—or OSHA requirements or healthcare fraud and abuse guidelines—“is converting a physician who is trained in clinical management and treatment of patients into a manager of process.”

- One panelist criticized the healthcare industry for not moving quickly to implement security technologies. A health industry panelist countered that, for organizations that are highly regulated and generate small operating margins, it would have been “a bad business decision” to purchase and install expensive security systems before knowing what final federal privacy standards would look like.

- Researchers worry that compliance costs, particularly compliance with a variety of state privacy standards, could impede new breakthroughs. Research organizations incur major costs in conducting prospective, randomized, controlled clinical trials, one panelist said. “Ultimately what you may find is, you wish you had a therapy that could have benefited 50 percent of patients with breast cancer, and you’re stuck with a therapy that maybe only benefits 25 percent.”

- Although hospitals and other institutional providers are at the center of the privacy debate, several panelists agreed that the worst examples of privacy breaches occur outside the clinical setting.
Core Question 4:

What Are the Areas of Consensus and Points of Tension in the Debate on Privacy of Health Information?

After one-and-one-half days of intensive discussion, the expert panel was pleased to discover that, despite the mix of views that were expressed over the course of the Colloquium, there was, in fact, strong consensus on several points, and near consensus in other areas. Not surprising in view of the controversial Colloquium topic, the panel also identified points of tensions, including areas of clear disagreement and issues or concerns on which no resolution was reached. The Colloquium’s points of consensus, points of near consensus, and points of tension are presented in the adjacent box.

The moderator adjourned the 2001 Colloquium, Privacy of Health Information, stating that, as has been the practice with other public interest reports published by Health Lawyers, the report on this Colloquium would be distributed widely to the health policy community, including members of Congress, federal agencies, professional healthcare associations and consumer organizations, the news media, and Health Lawyers’ members.

Points of Consensus, Near-Consensus, and Tension

Points of Consensus
1. There is a need for transparency, notice, consent, and public education.
2. Privacy is an important aspect of the healthcare system.
3. There is a need for trust and a recognition of legitimate uses of health information.
4. Individually identifiable health information should be protected.

Points of Near Consensus
1. At present, market forces are not sufficient to provide an adequate level of privacy in the traditional healthcare market.
2. There can be legitimate uses of patient information to improve quality, to improve efficiency, and to reduce disparities in healthcare.

Points of Tension—Areas of Disagreement
1. Federal privacy standards should preempt state privacy laws.
2. Individuals should enjoy a private right of action for privacy violations.
3. Some participants in the debate are trying to legislate other agendas under the guise of privacy.

Points of Tension—Unresolved Issues or Concerns
1. There is a lack of coherence between federal and state legislative and regulatory approaches to privacy.
2. The discussion did not adequately address privacy of healthcare information that is used for commercial purposes, particularly the rights of individuals with respect to information used for e-commerce.
3. Why is privacy important to people?
4. Is privacy a right or commodity? Who owns the rights to the commodity? What is ethical behavior in this context?
Welcome and Introductions

Health Lawyers’ Public Interest Committee Chair and principal moderator welcomed participants to the 2001 Colloquium, provided background information on the Association, and outlined ground rules for the discussion. The moderator noted that the Colloquium was taking place at a time when the health policy community’s attention was focused on recent final privacy regulations issued under “HIPAA,” the Health Insurance Portability and Accountability Act. She stressed, however, that the Colloquium’s focus was the broad policy considerations relating to privacy of health information. “This isn’t a debate on HIPAA,” she cautioned.

The moderator then asked the panelists to introduce themselves and make a brief statement about their organizations. She offered each panelist the opportunity to identify one priority or goal for the discussion that he or she particularly wished to see the Colloquium address. Goals identified by the panelists included:

Balancing Protection and Legitimate Use

One-third of the participants used the words “balance” or “common ground” in describing their goal for the Colloquium and the privacy debate in general. Representative comments included:

- My biggest concern is how we balance the desire to guarantee privacy of people’s health information with the need to ensure that, as we provide that guarantee, we don’t inconvenience patients unnecessarily and also disrupt the healthcare system —A Government Panelist

- I’m hoping that today and tomorrow will give me a sense of whether it’s possible for the various stakeholders to have a balanced discussion and come up with some common ground on how we can make sure that our common interests really are met. And that is to promote privacy, but to do so in a way that is sensible and workable, and that actually improves access to quality care and to research —A Consumer Representative

- I hope we can find common ground between [on the one hand] appropriate uses of this information for innovations, for advances in healthcare, for improving quality for consumers and [on the other hand] meeting the need of consumers to feel confident that their information is used appropriately and is protected —A Health Industry Panelist

- My biggest concern has been that in the five years I’ve been fighting this battle, I haven’t yet seen an approach that properly balances the public goods that derive from the use of medical information with a genuine respect for the privacy of individuals whose information is being used —A Health Industry Panelist

- I’m hoping that today and tomorrow will give me a sense of whether it’s possible for the various stakeholders to have a balanced discussion and come up with some common ground on how we can make sure that our common interests really are met. And that is to promote privacy, but to do so in a way that is sensible and workable, and that actually improves access to quality care and to research —A Consumer Representative

Perspective

One government panelist sought a sense of perspective from the Colloquium: “I need a better understanding of how health privacy fits within society’s attempt to grapple with privacy issues in this time of expanded Internet access, expanded marketing abilities, and some of the technological advances that make what appear to be invasions happen on an everyday basis. I’d like to get a better sense of where the health industry fits in that overall picture.”

Research Needs

A number of panelists identified access to data for medical research as their top priority. Comments included:

- My priority is ensuring that academic medical centers have access to patient information for research purposes —A Health Industry Panelist

- I’m concerned with the balance between protecting patients’ privacy and our sector’s ability to run multi-centered clinical trials across the United States. We are concerned that some of these regulatory policies may inhibit the ability to continue generating hypotheses that will complement our research —A Health Industry Panelist

- The issue I want to raise and sponsor is how to ensure that researchers get access to personal health information and treat it responsibly, how do we improve ethical behavior in our country, and, in general, how do we balance the public good that can come from such access against the potential for private harm. Where do we strike the balance —A Government Panelist

Administrative Issues and Federal-State Roles

Several panelists identified administrative burden as their top issue. Some panelists particularly stressed the need for federal preemption of state privacy laws and the potential
administrative burden of complying with a variety of state requirements. Comments included:

- I’d like to see discussion of how physicians and other healthcare providers are going to respond to the administrative requirements that arise from federal regulations. A related goal is discussion of what will happen to the medical record, especially physicians’ clinical impressions, in light of pending disclosure requirements—A Health Industry Panelist

- My concern is, as we develop a body of law and regulations in the area of health privacy, how do we coordinate and rationalize the various state and federal standards that are now growing like weeds—A Health Industry Panelist

- A very serious concern is, how do we rationalize the various regulations across 51-plus potential entities in a way that effectively delivers healthcare—A Data/Technology Representative

- My primary concern is the lack of federal preemption and the harm that could ensue with 51 jurisdictions trying to legislate—A Health Industry Panelist

**Discrimination**

A consumer representative stressed that an important outcome of the debate is both privacy protection and access to needed information for groups that might be subject to discrimination: “We’re most concerned about ensuring that the right to privacy is secure and that gay and lesbian families are well protected within [HIPAA] and other federal regulations to ensure that they have the information needed to provide care and treatment to their loved ones, and [to] make sure that ‘family’ is defined broadly enough to include them.”

**Cyber Issues**

Several panelists identified the Internet and e-commerce as priorities for discussion. Comments included:

- I’d like to learn the panel’s consensus on informatics suppliers’ obligation to provide security mechanisms to enforce privacy requirements—A Data/Technology Expert

- I’m particularly interested in the intersection of concerns about provider confidentiality with e-commerce—A Government Panelist

- I’m very interested in the use of healthcare information in the online world, particularly as it’s collected through Internet websites, how that information is best protected, and what the privacy concerns are specific to that kind of information collection—A Consumer Representative
Overview

A second Health Lawyers moderator led the discussion of Core Question One: the history, politics, and public policy goals of laws to protect the privacy of health information. She quickly reviewed milestones in the evolution of the health privacy debate, as noted in background materials that Health Lawyers provided the panelists. The moderator noted that health information privacy dates back to the Hippocratic oath1 and pointed out that privacy has a long history in the United States. Among the milestones the moderator mentioned were:

- In 1977 the U.S. Supreme Court recognized privacy as a fundamental right (Whalen v. Roe 429 U.S.C. 589 (1977)) and distinguished two types of constitutionally protected interests: (1) an individual’s interest in avoiding disclosure of personal matters; and (2) an individual’s interest in being independent in making certain types of personal decisions.
- All 50 states and the District of Columbia now recognize in tort law a common law or a statutory right to privacy. Most states accord sensitive health information—such as mental health and disability records, HIV records, and genetic test results—heightened privacy protection.
- There is no federal statute defining an individual’s specific right to privacy in his or her healthcare information held in private or governmental hands. Several federal laws protect privacy and medical records in certain contexts, however. The moderator noted wryly that although there is no federal statute to protect health information, there is a federal law to protect the disclosure of video rental records.
- Although there is no federal health information privacy law, widespread industry self-regulation has resulted in a collection of ethical guidelines, organizational policy statements, and model policies and procedures. In the international arena, the Council of the European Union has adopted the EU Data Directive requiring all EU countries to enact stringent laws protecting personal data and forbidding the transfer of personal data to nonmember countries whose laws cannot provide adequate protection.
- Finally, the Department of Health and Human Services issued final regulations in late 2000 that provide the first comprehensive federal protection for the privacy of health information.

More detailed information on the history of privacy laws is provided in “Timeline: Major Federal Privacy Laws, Regulations, and Other Developments” on page 16. For a brief summary of the final HIPAA privacy rules, see Appendix B, “Highlights of the Final HIPAA Privacy Regulations,” on page 50.

Fundamental Expectations Regarding Health Information Privacy

Following her brief overview of the history of privacy laws, the moderator engaged the panel in discussion of a key subquestion: To what extent should individuals have an expectation of privacy in their personal health information?

A health policy analyst led off with the observation that, in the legislative arena, privacy often is discussed in terms of individual rights.
“We don’t speak much in terms of the responsibilities that underlie those rights,” she said. “What too often gets left out of consideration is not simply the public benefit that may come from research, innovation, all of that, but also a sense of our responsibility to one another as members of the community to enable that to go forward.”

A consumer representative focused on the amount of information that is shared. “Most people have a mindset that goes back to the 1950s, when they had a personal relationship with one healthcare provider, usually a doctor, and their records stayed in that office. Most people would be blown away if they knew the extent to which their information is actually used and shared today,” this panelist said. The HIPAA privacy rules, the panelist said, “put into federal regulation a lot of what is already happening.”

A government panelist, however, asserted that patients are taking a more active role in their own interactions with providers and are demanding more information about their physician’s experience with a given procedure, potential side effects, complications, and so forth. “They’re wanting information from their physician that only a review of other people’s records and aggregation of that information can give,” the panelist said. With respect to consent forms, “patients’ expectations about having [outcomes] information is going to be tempered against their unwillingness to share their own information.”

A consumer representative said segments that are subject to discrimination may be willing to share information with some recipients, but not with others. “People should expect very stringent privacy laws, but it’s a question of to whom your information is being given. If it’s given to other healthcare providers, I think people would probably say that’s okay. Is it given to insurance companies? Well, maybe that’s okay. But if it’s shared with their employer, people might not think that’s such a great idea.” For gays or patients with mental illness, “there’s discrimination that still exists out there,” the speaker concluded.

“A consumer representative

Most people have a mindset that goes back to the 1950s, when they had a personal relationship with one healthcare provider, usually a doctor, and their records stayed in that office. Most people would be blown away if they knew the extent to which their information is actually used and shared today.”

— A consumer representative

A panelist with expertise in medical research picked up on the first speaker’s comment that privacy protection includes both rights and responsibilities: “One of the very troubling aspects of this whole debate has been the failure to understand the public goods that are at stake in this issue as opposed to the focus on individual privacy protection. The pendulum has been way, way too far over on the privacy side for some aspects of the use of medical information. And I’m not making a sweeping generalization there because I certainly do understand concerns about inappropriate access, employers getting information they shouldn’t have, and so forth.”

The panelist stressed the importance of individual medical data: “The plain fact is that everything we know about disease and its response to treatment comes from historical studies of experience. There is no theory in medicine yet, even with genomes and all; it’s all empirical. For centuries, what we know has been accreted by systematic studies of . . . large groups of patients, segregated by some kind of disease presentation, or illness, or whatever. Like it or not, that’s how the knowledge base has developed. And the key is to get to the point where that knowledge base is not being confounded by statistical aberrations due to selection biases.”

This panelist added that over the last 40 years, “the vast majority of definitive studies—diet, the effect of oatmeal on cholesterol, the effect of contraceptives on breast cancer, or air pollutants and water pollutants, food stuffs, drug toxicities, whatever—have come out of Scandinavia. Why? Because Scandinavia has a comprehensive birth-to-death record system of every single individual in every one of those countries, so that when investigators need to look at the issue on a large population scale, this is the least biased, the least distorted database in the world.”

If some population segments don’t want their medical information used to aid medical research, the speaker continued, “it builds biases and distortions into the database from which conclusions will then be made years or decades later that can have enormous public policy implications.” For example, if patients with mental disorders don’t want their records used, the speaker said, then “a study of women with breast cancer would say that there is absolutely no worry about depression in women with breast cancer. Why? Because people with depression said, ‘No, I don’t want my records used for research,’ and people without depression more likely said, ‘Yes, it’s okay to use them.’ That’s the kind of distortion that can
come out when any specific kind of symptom, or diagnosis, or whatever drives a predisposition towards saying ‘No.’”

In a later reference to the Scandinavian model of data collection, a policy analyst agreed on the value of research and supported access to medical records by researchers without consent. However, he said, “The Scandinavian countries have some of the strongest data protection laws in the world. That may be one reason why some of this activity is tolerated.” In the United States, this panelist said, polls indicate that the public wants a consent requirement for use of personal medical information. He suggested that the medical community needed to educate the public about how their health information can assist medical research.

Another speaker, representing the health industry, said, “Overall, there is this expectation of privacy. But, remember, in this country we also have a high expectation for good healthcare. So, while there is this expectation of privacy, there are some cases where that expectation is overcome by public health goals, or by the need for research. Then the issue is, how is health information used and how is it protected?”

A government panelist endorsed the “potential for public good in the appropriate use of health data” but raised a caution about “having that same information shared on and on and on” by other users. The speaker continued, “Research for medical purposes doesn’t take much stretching of my brain at all. But research for marketing color choices among packaging inserts, for example, or research on better mechanisms for communication—well, you could argue that communicating with patients is very important, but you could also argue that basically you’re doing advertising research that can then be used to market everything else under the sun.”

A technology expert discussed public expectations in the context of the explosion of information that now is collected on people in all areas of their lives. The proliferation of data, combined with the spread of computers and increases in computer power, makes it “extremely difficult to draw a boundary and look at the past as a way of proceeding to the future. Today and the future just don’t look at all [like the past]—the natural boundaries that existed before are just simply not there,” the panelist said.

As a guide to individual expectations, the panelist pointed to a Harris-Equifax poll that “says for the most part, with respect to the secondary use of data, the public doesn’t mind if their data is used for research purposes, provided that they can’t be identified.” But, the way our society is organized, the panelist noted, “it’s the individual who bears the risk.” Current laws don’t protect individuals against problems with creditworthiness, discrimination by employers, and so forth. The problem will only get worse in coming years, the panelist predicted.

The solution, according to this panelist, is to ensure that research is committed to using data that is minimally invasive to privacy. At the same time we have to understand biases in data or conclusions that might result from laws and policies that are put in place and ensure that the data remains practically useful. “I would like to see that be the [focus] of conversation, not do you get the data or not. I don’t think that that’s a useful construct,” the panelist concluded.

A health industry panelist observed that in the discussion of societal and individual expectations, it is important to remember that “the patient has power themselves. The patient can already self-redact their own information. Now, they may do that in a way that is not beneficial to themselves. They may withhold information from their doctor. They may ask the doctor not to put it in the medical record.” Many physicians no longer enter their subjective impressions into a patient’s record even though traditionally that was important in developing long-term treatment plans. Patients may even opt out of the healthcare system rather than reveal information that might have adverse consequences. “Psychiatric patients are avoiding health insurance coverage for the very reasons that they have no reasonable expectation that that information will be safe and protected,” the panelist said.

Two other panelists, a health industry representative and a government official, pointed out that, in addition to public health or public safety needs that may limit a person’s expectation of privacy, technology is an impediment to privacy protection. “Previously,” the government official

“Overall, there is this expectation of privacy. But, remember, in this country we also have a high expectation for good healthcare. So, while there is this expectation of privacy, there are some cases where that expectation is overcome by public health goals, or by the need for research. Then the issue is, how is health information used and how is it protected?”

— A health industry panelist
noted, “the issue was the expense of building the data, of collecting data and having it made available to the people who needed to use it. Think of all the resources needed to go through paper records, and to pull that data out and collect it. Technology has flipped things around so that now the cost is not in collecting the data; the cost is in individually protecting the data or accommodating the fact that that I want my data protected one way and [John Doe] wants his data protected another way. We have totally changed the economic nature of the data handling.”

A health industry panelist suggested a “bright line” standard on the use of data in research: “I don’t believe research data should ever be accessed for anything other than an improved research protocol—by anybody.” The panelist said that his organization has urged that a statute known as the Certificate of Confidentiality be expanded to “include the information that we’re concerned about [in the privacy debate] as extremely sensitive and protect it.”

A data and technology expert noted that prisoners and military personnel already have no practical control over their health data and suggested that commercial considerations would lead to erosion of autonomy for other segments of society. “There are certain inevitabilities about the compromise of privacy and confidentiality” and “realistically, there’s probably little or no economic means to safeguard privacy,” the panelist said.

**Public Interest Goals of Privacy Laws and Regulations**

The moderator pointed out that the discussion overlapped with another subquestion, the public interest goals of privacy laws, and steered the discussion in that direction. Much of the discussion revolved around the need to balance privacy protection with societal benefits such as medical advances and improved health and safety for society at large.

A health industry panelist suggested that individuals’ top priority is protection against discriminatory use of their information by employers, insurers, or others. “It isn’t so much that your information is being shared, but is it being used in a way that discriminates against you?” The panelist noted, “There are a lot of uses, new uses, for this information that will improve healthcare for the patient. So all of those things need to be balanced.”

Re technology as an impediment to privacy protection: “Previously, the issue was the expense of building the data, of collecting data and having it made available to the people who needed to use it. Think of all the resources needed to go through paper records, and to pull that data out and collect it. Technology has flipped things around so that now the cost is not in collecting the data; the cost is in individually protecting the data or accommodating the fact that that I want my data protected one way and [John Doe] wants his data protected another way. We have totally changed the economic nature of the data handling.”

— A government panelist

A panelist from the provider community picked up on the last point to suggest other public purposes beyond research, including quality assurance, quality improvement, and patient safety. “Those are enormous and important public interest goals that have to be met . . . and they’re goals that patients expect the system to meet,” the speaker said. This panelist went on to stress that patients have greatly expanded their expectations of the healthcare system. “They expect information about quality. They expect report cards on health plans, on hospitals, how one hospital compares to another, how one health plan compares to another.”

The “disconnect” on privacy, the speaker continued, occurs because consumers generally don’t understand how their information will be used. And HIPAA requires that providers tell individuals what their information will be used for. “For 90 percent of the information that we’re talking about, when individuals understand why it’s being collected and what it’s being used for, most people would agree that that’s a good public interest, and it should be used for that purpose. The problem is they just don’t know that, and someone needs to tell them that,” the panelist concluded.

A policy analyst agreed with the earlier speaker’s point about discrimination, but added, “At the same time, we’re in a context where in very many cases an awful lot of people want precisely the same information about the guy next door that they don’t want to give out. What’s his HIV status? Does he have a mental health diagnosis?” We all have contradictory attitudes about privacy, and “I think that kind of psychological dynamic has to be part of the mix,” the panelist concluded.
A government panelist suggested management of birth defects as a laudable public interest goal and noted that some states are implementing “public health surveillance systems” as an alert to health problems that may be caused by an environmental problem that needs to be addressed. “But if you don’t have a large group of data, you’re never going to see the patterns,” this panelist said. The government panelist pointed out that some public interest needs don’t necessarily require identifiable data. “We don’t necessarily need to know who this data belongs to, and we can find out some of the surveillance things that we may want to know. We can do research. We can do a lot of things without having personally identifiable health information.”

The panelist noted, however, that circumstances might arise when it would be desirable to reconnect identities to the information “in order to contact some people with potentially life-saving information.” He then asked, “Can we trust a public agency to hold the key to that anonymized data so that if a public interest is served by contacting the individuals who are the subjects of that data, the data can be put back together so we can get in touch with them?”

The government speaker’s comments about “public health surveillance systems” sparked a lively discussion of trends in information security and myths and realities of “de-identified” health information.

One technology expert connected the discussion to national concerns about bioterrorism, explaining, “The economics of bioterroristic asymmetrical warfare are so compelling that the likelihood of that is deemed extremely high. It just doesn’t cost much to manufacture a couple of hundred kilos of Anthrax, and then deploy it. And basically all the technology you need for a weapon of mass destruction like that is what you have in a brewery.” For policymakers in the defense area, the panelist continued, “[that risk] overrides a lot of these individual privacy interests.” And the expectation is that this is not going to be de-identified information that’s used; they’re going to want very specific information. Because in order to intercede in the event of an attack, you’re going to need to know specifically who is exhibiting signs of Anthrax or 1918 influenza or whatever.” Those considerations, the panelist said, may mean that “a lot of this individual privacy discussion is almost moot.”

A second data/technology-oriented panelist has been working with the Department of Defense on bioterrorism surveillance. “I find it interesting that the kind of data that the work in bioterrorism primarily uses really is not medical information in the first round. . . . Because of the widespread use of data, the Department of Defense has been adamant about using sufficiently anonymous data. And so [the first question] is how you guarantee that the data really are anonymous.”

Interestingly, the panelist noted, “People have no idea what is identifiable data. Last summer, we surveyed the entire United States population and found that 87 percent of the population is uniquely identified by their date of birth, gender, and the five-digit zip code in which they live. I don’t need your Social Security number; I don’t need your name. I don’t need your ethnicity or your race. All I need is your date of birth, gender, and zip code, and I can find out all kinds of information about you—certainly if you’ve been in the hospital—using only publicly available information.”

A policy analyst challenged an earlier speaker’s assertion about the many potential benefits of sharing health information. “The American business community tries to turn the issue into a question of ‘What’s the harm?’ and ‘We can do anything we want with data until patients or people are bleeding in the street.’ That’s not the point. The point is whether people have a right to privacy and some interest in how their records are used, and it doesn’t matter whether there is some identifiable harm or not.”

The speaker also took issue with a widely publicized 1999 quote from Sun Microsystems CEO Scott McNealy that Americans “already have zero privacy. Get over it.” McNealy seemed to be “talking about privacy as if it is a unitary concept and a single thing,” the speaker said. “That’s a very big mistake and a very big barrier to any kind of reasonable analysis. Privacy is composed of a variety of elements. You can have medical records, any records, that are used for a wide variety of purposes, and you may not be doing a very good job as a result for good or bad reasons with respect to how you protect those records against secondary and tertiary uses and disclosures. So
it’s not something that is a simple concept, that we either have privacy or we don’t. You really have to break it down into its elements.”

How Effective Are Current Privacy Laws?

The moderator moved to bring the discussion on the history and goals of privacy laws to a conclusion, posing a final question, “How effective are current laws in protecting privacy of health information?”

A government panelist led off, asserting, “A lot of current laws are deficient in that they don’t go far enough in trying to define what is appropriate and what is inappropriate” use of health information.” The panelist continued, “We need more laws that [follow] public opinion and say, ‘I don’t think people ought to be able to discriminate on insurance, for example—you can’t discriminate for Medicare or you can’t have enrollment parties on the third floor where people would have to walk up—so you’d get the healthier people.”

The panelist concluded, “We need to define what is fair use and fair disclosure and what is not fair use and fair disclosure. Perhaps we should leave enough room for individuals to argue in a court about the fairness, the potential benefits, the potential harm—and who should have the right to use the data to get that efficiency. I think [privacy] can be looked at as a market transaction, and laws could facilitate this market transaction by giving the individuals some additional rights.”

A technology representative suggested that rather than try to define privacy in more detail, “Could we say property as opposed to privacy? Let’s address this as if your data is your property and set up a category of controls or restrictions, consensus, all the rest, around that property and enforce it accordingly.”

A health industry panelist spoke against that suggestion. “I would argue against calling the medical information property. Who owns the data is really not the question anymore. It’s, how is the data used, and how is the data maintained. To try and figure out who owns it—well, I think it’s a waste of time and a waste of resources, and would bring us down a road where many more arguments would occur.” A far better approach is to “look at use and responsibilities for maintaining it in a certain way.” The moderator asked if the speaker were “moving away from the ownership model of patient information, which existed statutorily in some states, towards the rights and responsibilities model?” The speaker’s response: “Absolutely.”

A policy analyst suggested looking at the effectiveness of current laws as a two-part question: The first: How good are the laws to begin with; do they really address privacy? There are dozens of state laws that affect health privacy in some way. Many of them, however, aren’t comprehensive. They may address physicians but not hospitals. Or, the speaker added, “They are highly old-fashioned,” meaning that the laws haven’t been updated to reflect advances in technology or changes in the healthcare system. “They simply don’t reflect the modern reality of the world,” the speaker said.

A second question: Are the laws being complied with? “That’s a much harder question to answer,” the speaker asserted, but the fact that many people in healthcare aren’t aware of the laws’ existence probably means they aren’t being complied with. “When you stand up and present the basics of health confidentiality law to any healthcare audience, no matter who they are, it’s a revelation. They didn’t know there were any laws. . . . They just do whatever everybody else in their organization does. If there’s anything good that will come out of the HIPAA process, it will be to force people to pay attention, for the first time ever, to the fact that there are rules about confidentiality, and that people have to do something about it.”

The moderator announced that time had run out and thanked the panelists for their stimulating discussion on the public’s expectations regarding privacy, the public interest goals of privacy laws, and the competing values that lie at the heart of the health information privacy debate. The moderator then turned the program over to another Health Lawyers facilitator for discussion of the next core question.

1 “What I may see or hear in the course of treatment or even outside of the treatment in regard to the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret.”

Timeline: Major Federal Privacy Laws, Regulations, and Other Developments

1890—
**Harvard Law Review Article**—Definition of “Privacy”—In a law review article, Louis D. Brandeis and Samuel D. Warren defined an individual’s right to privacy as the “right to be let alone.” Justice Brandeis used this same definition in his opinion in the precedent case, **U.S. v. Olmstead** in 1928. 277 U.S. 438 (1928).

1914—
**Federal Trade Commission Act (FTC Act)**—The first major consumer protection law. Enacted to police unfair methods of competition, the FTC Act expanded over time to cover a variety of business practices. The law was amended in 1938 to protect consumers against fraudulent and deceptive trade practices, establishing the FTC as one of the principal “guardians” of individual privacy. Sept. 26, 1914, ch. 311, 38 Stat. 717.

1928—
**U.S. v. Olmstead**—In a Supreme Court ruling, Justice Louis Brandeis defined an individual’s right to privacy as the “right to be let alone.” 277 U.S. 438 (1928).

1944—
**Public Health Service Act**—Under this statute, entities engaged in clinical research may request a “Certificate of Confidentiality” from the Department of Health and Human Services that provides special privacy and confidentiality protections from subpoenas, court orders, and other compelled disclosures involving research. July 1, 1944, ch. 373, 58 Stat. 682.

1965—
**The U.S. House of Representatives creates a special Subcommittee on Invasion of Privacy**

**Griswold v. Connecticut**—The U.S. Supreme Court held that an individual’s right to privacy, founded in the concept of personal liberty expressed in the Fourteenth Amendment, protects the right of a husband and wife to use contraceptives in their own home. 381 U.S. 479 (1965).

**Medicare/Medicaid Conditions of Participation**—Requires all Medicare- and Medicaid-participating healthcare providers to protect the privacy and confidentiality of patient records and to ensure that unauthorized individuals do not access or alter the records. Pub. L. 89-97; 42 C.F.R. 401 (Administrative Requirements including official records confidentiality and disclosure); 42 C.F.R 482 (conditions of participation for hospitals).

1966—
**Freedom of Information Act**—Expressly prohibits the disclosure of medical and/or personal files by governmental or regulatory entities for the purpose of commercial use. Pub. L. 89-487.

1970—
**Fair Credit Reporting Act**—Protects an individual’s credit records and provides the individual with specific rights related to his/her credit records, including the right to amend or correct them in case of errors. Pub. L. 90-321.

**Confidentiality of Records Provisions**—Affords special protection to substance abuse and treatment records. These records may not be disclosed without the subject individual’s written authorization unless so ordered by a court following a special, “show cause” hearing. 42 U.S.C. §290dd-3; 42 C.F.R. Part 2.

1973—
**Department of Health, Education and Welfare— Code of Fair Information Practice Principles**—These principles formed the basis for the 1974 federal Privacy Act.

**Roe v. Wade**—The U.S. Supreme Court first recognized the individual’s right to interact privately with his/her physician. 410 U.S. 113 (1973).

1974—
**Privacy Act**—Regulates the government’s use of personal information of individuals. Specifically prohibits disclosures of records or personal information contained in records that are maintained by a federal agency or its contractors unless the agency or contractor has first obtained a written request or consent from the individual who is the subject of the records or information. The Privacy Act also allows individuals to access their own records or personal information, requires federal agencies to specify the purposes for which they collect personal information, and establishes civil and criminal penalties for the misuse of personal information. Pub. L. 93-579.
Family Education Rights and Privacy Act—Provides specific privacy protections to student records that are maintained by federally-funded educational agencies and institutions. Special protections are given to records of parents and to the records of students who are eighteen years of age or older. Pub. L. 93-380.

Whalen v. Roe—The U.S. Supreme Court held that the fact that information is stored electronically does not necessarily mean such information would be disclosed in violation of an individual's right of privacy. However, the Court held that the keeper of the electronically stored information must have in place adequate protections against improper disclosure of that information. 426 U.S. 589. (1977)

Right to Financial Privacy Act—A predecessor to the Gramm-Leach-Bliley Act (see below), this law covers only financial institutions as they are traditionally defined (that is, banks, credit unions, etc.). Prohibits government authorities from accessing or obtaining copies of or information stored in an individual's financial record unless the individual has authorized the disclosure or unless the request is in the form of a subpoena, search warrant, judicial subpoena, or is some other formal written request. Pub. L. 95-630.

Protection of Human Subjects Regulations—The Food and Drug Administration (FDA) issued regulations that protect human subjects who participate in clinical trials. The regulations require the Primary Investigator who is responsible for conducting a clinical trial to obtain an individual's prior written consent to (1) participate in the trial and (2) allow the investigator to share the individual's health information (medical record) with the sponsoring entity(ies). 21 C.F.R. Parts 50, 56 (FDA issued); 45 C.F.R. Part 46 (HHS issued).

Privacy Protection Act—Makes it unlawful for a government officer or employee, in connection with an investigation or a prosecution, to search for or seize any work product or materials in the possession of someone who would be disclosing them to the public in some form of public communication such as a book, a newspaper, or a broadcast. In addition, requires that the public communication be made in the context of, or affect, interstate or foreign commerce. However, the law does not protect the work product or materials from search or seizure unless there is probable cause that the person holding them is involved in the criminal offense or their disclosure is necessary to prevent death or serious bodily injury to any person. Pub. L. 96-440.

Electronic Communications Privacy Act—Prohibits the intentional interception of or access to stored e-mail messages. The law does not, however, protect the content of such e-mail messages once a prohibited interception has occurred, unless the communication is subject to a recognized privilege of confidentiality such as the physician-patient privilege. Pub. L. 99-508.

Video Privacy Protection Act—Prohibits video rental stores from disclosing personal information about their customers, including the individuals’ names or addresses. Pub. L. 100-618.

Employee Polygraph Protection Act—Under this law, employers that are engaged in commerce or produce goods for commerce cannot directly or indirectly require, request, suggest, or cause their employees to take or submit to any lie detector test. Employers and prospective employers are also prohibited from using, accepting, referring to, or inquiring about the results of such a test taken by any of their employees or applicants. Finally, employers are prohibited from threatening to or discharging, disciplining, discriminating against, or denying employment or promotion to an employee for refusing to take a lie detector test. Pub. L. 100-347.

Telephone Consumer Protection Act—Specifically protects an individual’s right to privacy from unrestricted telemarketing. Congress found such communications an “intrusive invasion of [the individual’s] privacy” as well as a risk to public safety (in cases where such telemarketing would interfere with the individual calling for help in an emergency or prevent someone from being able to contact the individual in an emergency. Pub. L. 100-243.
**1994—**

**Driver's Privacy Protection Act**—Prohibits employees and contractors of Departments of Motor Vehicles from disclosing personal information about any individual that has been obtained by the Department in connection with the individual's motor vehicle record. In addition, the Department is not allowed to sell mailing lists of drivers without first providing the individual the right to prohibit such action. Pub. L. 103-322.

**1996—**

**Telecommunications Act**—Requires every telecommunications carrier to protect the confidentiality of the proprietary network information of, or relating to, its customers. “Proprietary network information” includes the quantity, configuration, type, destination, and amount of use of the particular telecommunications service that the customer subscribes to that is made available to the carrier by virtue of the customer-carrier relationship. It does not include information contained in the customers’ bills or subscriber list information such as that found in a telephone directory. Pub. L. 104-104.

**Health Insurance Portability and Accountability Act of 1996 (HIPAA)**—Under Subtitle F, Title II of HIPAA, Congress specifically recognized the absence of and need for comprehensive federal privacy legislation to protect the privacy of individually identifiable health information transmitted in connection with a HIPAA-mandated electronic transaction. Congress stipulated that if it failed to enact privacy legislation within 36 months of HIPAA’s enactment, the Secretary of HHS should proceed within the following six months to issue final regulations containing health information privacy standards. Pub. L. 104-191.

**1997—**


**Institute of Medicine**—Published “For the Record: Protecting Electronic Health Information,” a study that examined and reported on the existence of and need for electronic medical records in the United States.

**Fairfax Hospital v. Curtis**—The Supreme Court of Virginia upheld a $100,000 judgment against Fairfax Hospital for disclosing Mrs. Curtis’ medical records without her written authorization. 492 S.E.2d 642 (Va. 1997).

**1998—**

**Children's Online Privacy Protection Act (COPPA)**—Requires on-line service providers or entities that operate Web sites for the purpose of collecting personal information from children under the age of thirteen to provide notice on the Web site that personal information is being collected, how that information is expected to be used, and to describe the routine disclosures of that information. COPPA also requires the entity collecting the information to first obtain verifiable parental consent to such collection, use, and disclosure. Pub. L. 105-277.

**Identity Theft and Assumption Deterrence Act**—Makes it a felony to produce, transfer, or possess with the intent to use or unlawfully transfer a false identification or means of identification. Under the Act, it is prohibited to use one or more of the following elements by themselves, or in combination with any other information, to identify a specific individual: name; Social Security Number; date of birth; driver's license number; alien registration number; government passport number; employer or taxpayer number; unique biometric data such as a fingerprint, voice print, retina or iris image, or other unique physical representation; unique electronic identifier, address, or routing code; telecommunications identifying information or access device. Pub. L. 105-318.

**Proposed HIPAA Security Standards**—As required by HIPAA, the Department of Health and Human Services (HHS) published proposed Security Standards. The proposed Standards require that individuals or entities that collect, maintain, or transmit health information electronically protect the confidentiality of that information and ensure its availability and integrity. 63 Fed. Reg. 43263 (Aug. 12, 1998). To be codified at 45 C.F.R. Part 142.
Proposed Transactions and Code Sets Standards—Under HIPAA, Congress identified nine specific administrative transactions that healthcare organizations use to conduct business. These proposed standards established the format for seven of the nine and the more than 40 code sets that define the data elements that are or may be contained in such transactions. May 1998. To be codified at 45 C.F.R. Parts 160 and 162.

Health Care Financing Administration (HCFA) Internet Security Policy—Establishes a minimum set of security mechanisms, including encryption, that must be implemented by any entity that transmits Medicare beneficiary information over the Internet.

Gramm-Leach-Bliley Act (also known as the Financial Modernization Act of 1999)—Requires that health insurers provide notice to their customers before they share the individuals’ non-public, personal information with unaffiliated entities. Insurers also must give their customers an opportunity to opt-out of such disclosures. Pub. L. 106-102.


Cossette v. Minnesota Power & Light—The Eighth Circuit Court held that an employee may file suit against her employer under the Americans With Disabilities Act (ADA) for an unauthorized disclosure of her medical records even if the employee is not disabled. No. 98-3042 1999 WL 6190 942 (8th Cir. Aug. 17, 1999).

Biddle v. Warren General Hospital—The Ohio Supreme Court ruled that Warren General Hospital breached its patients’ confidentiality when it released patients’ records to a law firm to assist with collection efforts. 86 Ohio St. 3d 395 (Ohio Sept. 1999).

Executive Order 13145—President Clinton’s order bans the use of an individual’s genetic information in federal hiring and promotion decisions.

FTC v. Toysmart.com, LLC—The FTC Settlement with Toysmart.com required the on-line retailer to immediately delete or destroy all of the information it had collected in violation of COPAA, and prohibited Toysmart.com from offering to disclose and subsequently sell its customers’ personal information to a successor in violation of its online Privacy Policy. In re Toysmart.com, L.L.C., ___ B.R. ___ (Bnkr. Mass. E. Div 2000).


Final HIPAA Transactions and Code Sets Standards—Issued on August 17, 2000, these standards, which included certain changes to the 1999 proposed regulations, require all covered entities to be in compliance with them by October 16, 2002 except for small health plans, which have until October 16, 2003. 65 Fed. Reg. 50312 (Aug. 17, 2000). Codified at 45 C.F.R. Parts 160 and 162.

Final HIPAA Privacy Regulations—After receiving over 52,000 comments on its proposed Privacy Regulations, HHS published final Privacy Regulations on December 28, 2000. The final regulations prohibit disclosing an individual’s protected health information without first obtaining the individual’s written consent or authorization unless such disclosure is allowed by the regulations or as otherwise required by law. (See “Highlights of the Final HIPAA Privacy Regulations,” page 50, for a summary of the final HIPAA regulations.) 65 Fed. Reg. 82462 (Dec. 28, 2000). Codified at 45 C.F.R. Parts 160 and 164.

Privacy Regulations Become Effective—The final privacy regulations became effective on April 14, 2001. All organizations that are subject to the regulations must be in compliance no later than April 14, 2003. Small health plans have an additional twelve months to achieve compliance.
What Are the Legal Issues in the Current Debate on Privacy of Health Information?

a. Applicability Issues

1. What types of health information should be protected? Should there be more stringent rules for certain types of health information such as genetic information, HIV test results and AIDS records, mental health and developmental disability records, alcohol and drug abuse diagnosis and treatment records, and sexually transmitted disease records?

2. For which types of health information should there be less stringent rules?

3. Should individually identifiable health information from persons detained in the justice system be subject to different rules?

4. Should law enforcement officials have access to protected health information without requiring a judicial order, grand jury subpoena, or administrative request?

5. Which levels of government officials should have access? Which individual officials?

6. What types of healthcare entities (e.g., institutions, medical personnel, employers, individuals) should be subject to federal medical privacy laws? Should certain entities be exempt?

7. How should privacy protections apply to “business associates” and other secondary users of individually identifiable health information?

8. How can privacy interests be reconciled with laws and regulations relating to research projects and protection of human subjects? When do clinical research and healthcare operations overlap?

b. Jurisdictional Issues

1. Should federal law preempt all state medical privacy laws, or should it serve as a “floor,” letting stand state laws that offer broader protections?

2. Is there potential for overlap with existing federal rules or programs (for example, ERISA, Federal Privacy Act, Federal Alcohol and Drug Abuse laws and regulations, Department of Defense, VA and Federal Employees Health Benefits Programs, E-Signature directive, Gramm-Leach-Bliley law, European Union directives)?

3. What role should courts have in enforcing privacy laws?

c. Use and Disclosure Issues

1. How do individuals’ expectations differ with respect to the “use” versus “disclosure” of individually identifiable health information? What is the difference between use and disclosure?

2. What is an individual’s health information “identity” in an era of computer-based communications and advances in biotechnology?

3. Does an individual’s identity include cultural or ethnic information? When and how should that information be protected?

4. When is health information no longer individually identifiable?

5. What use or disclosure activities are appropriate for “de-identified” health information?
Should protection of de-identified information be of unlimited duration? What protections can be provided to prevent future “re-identification” of health information?

When is use or disclosure of health information without specific individual authorization appropriate? With specific authorization?

Should use or disclosure of covered information be subject to a “minimum necessary” standard? How should that standard be defined?

d. Individual Rights Issues

What rights and liabilities should individuals have regarding the handling of their protected health information?

What protections should minors or incapacitated individuals have regarding the handling of their protected health information?

Should any class of covered entities be exempt from these individual rights-related requirements?

How long should individuals have access to their information?

Should records of disclosure be maintained?

Under what circumstances should individuals be denied access to inspect, copy, or amend part or all of their own information?

What are appropriate costs and processes for photocopying, printing, or electronically transmitting health information?

Should individuals have the right to preclude access by certain individuals or entities?

How should issues of “succession” be addressed (that is, information transferred to new owners of an organization following a merger or bankruptcy)?

Should federal law establish a private right of action for individuals to sue physicians, hospitals, health plans, or other entities that make unauthorized disclosure of confidential health information?

e. Framework for Legal Response to Privacy Issues

What legal approach or combination of approaches should be used to address privacy concerns?

Can a mixed government-industry approach, such as a limited antitrust exemption to allow uniform standards to be developed, be of assistance?

f. Regulatory Compliance and Enforcement Issues

If a regulatory approach is used —

What methods should government use to ensure compliance and encourage covered entities to develop a “culture of compliance”?

What steps can government take to ensure coordination among agencies in implementing laws and directives governing privacy?

What assistance should government offer to assist with compliance?

What types of sanctions or liabilities are appropriate for non-compliance?

Are additional penalties appropriate for intentional non-compliance?

What limits should be placed on government’s use of any personal health information that it obtains through compliance and enforcement activities?
Core Question Two

Echoing an earlier comment by one of the panelists, the moderator for Core Question Two emphasized that “privacy isn’t just one thing—we need to understand it as a multifaceted set of issues.” Accordingly, there would be some repetition of certain ideas and themes as the Colloquium addressed the remaining core questions. However, the moderator explained, “It’s desirable to have that element of repetition in our discussion.” Core Question 2, the moderator suggested, revolves around three sets of issues or themes: (1) What types of health information are entitled to protection, and should some types receive heightened or reduced protection? (2) Which entities or individuals should be required to comply with privacy requirements? (3) What are appropriate and inappropriate uses of health information? Explaining the last point, the moderator said, “Are there uses of particular concern or uses that should be broadly or specifically exempted because of a particular public good that is achieved by that particular use?” (For additional information on the meaning and uses of health information, see Appendix C, “What Is Health Information?, on page 55.)

Applicability—Covered Information

The moderator started the discussion of applicability by posing the following question: “Is it possible to identify in some meaningful way the types of information that we’re most concerned with or the types of information that we’re least concerned with, in terms of fashioning privacy protections?”

A health industry panelist forthrightly stated his organization’s view. “Just to get the ball in play, our position has been that appropriate privacy protection should be uniformly applicable to all kinds of medical information. The only exception for greater stringency that we can live with, for a variety of reasons, is a carefully delimited definition of psychotherapy notes.” In this respect, the panelist continued, the final HIPAA privacy rules “did a very, very good job. It was thoughtfully done, and we were quite happy with it.”

Aside from psychotherapy notes, the panelist concluded, “we do not like the idea of layered degrees of stringency defined by disease states.”

Another health industry representative agreed and suggested that the key question is how information is used. Certain drugs or medical conditions carry a stigma and discrimination—clearly an inappropriate use—can result if information about those drugs or conditions is released. All health information is sensitive, the panelist asserted. The key issue is “How do you make society accountable for the inappropriate use of the information, or how do you provide the appropriate security for all information, and then define appropriate uses and inappropriate uses?” The moderator summed up this view as “arguing for a blanket protection and more of a focus on use.”

A policy analyst agreed with both speakers, noting that with the broad variety of applicable laws that exist today, “it’s an impossible situation” to try and regulate by disease or condition. “Unfortunately, you have the problem of what I call trophy laws. Somebody says, ‘My information is so important, we need to have our own law on it.’ It’s simply counter-productive and doesn’t get you anywhere.” Genetics-oriented laws are also troublesome, the speaker said. “[Genetics] became the hot issue of the day a couple of years ago, and everybody ran to pass laws. None of the definitions make any sense. You can’t really define genetic information in any specific way.”

A government panelist agreed with the previous speakers but addressed the topic in terms of cost. “All I want to add is, I believe the cost of treating this information differently—of determining that it is different and treating it differently—is much more expensive than the cost of treating all the information in an equally stringent manner.”

A consumer representative expressed support for HIPAA’s treatment of health information, which cordons off psychotherapy notes, but does not otherwise differentiate among types of information. However, the panelist also noted that a refinement included in the HIPAA rules recognizes the need to protect information when particular circumstances arise where a person may “request that certain information not be used in a particular way or disclosed in a particular way.” The panelist also endorsed a HIPAA provision that grants the right to request a confidential communication and cited as an example battered spouses who may not want information they disclose about their domestic situation sent to their house. And so, the panelist said, although there should not be different standards for different types of information, consideration must be given to the impact that certain uses or disclosures might have.

This panelist also commented on the genetics discussion, supporting the suggestion that genetics not be treated differently. The panelist noted that state genetics laws and some federal laws “can, in fact, single out genetic information, not for purposes of privacy, but in order to make sure that genetic information is not used inappropriately to discriminate against people, either in health insurance or employment.” The policy
A different consumer representative agreed with earlier speakers that privacy laws and regulations should not treat various diseases or treatments differently, but emphasized that “there’s discrimination all over the place,” and went on to suggest a need for federal privacy laws and regulations to plug holes in existing anti-discrimination protections. “With only 11 states having anti-discrimination laws in employment based on sexual orientation, there is a clear opening for folks to discriminate if that information does get out,” this speaker said.

A health industry panelist observed, “As long as the conversation stays at 40,000 feet, it’s easy to agree on what should be protected.” For discrimination and other individual issues, however, “it’s the details.” With respect to genetic discrimination, this speaker said, the key issue is to ensure that the protected information cannot be used in a discriminatory way. “Because genetic information is your gender, and the color of your eyes, and the color of your hair, and everything else about you, and it gets absurd unless you’re very, very tailored [in the regulation],” the panelist said.

Another consumer-oriented panelist agreed that anti-discrimination laws should not be viewed as an easy solution to privacy violations. “There are going to be a lot of times when the abuse of a patient’s privacy isn’t going to lead to a result that necessarily rises to the level of a lawsuit. Even if it does rise to the level of a lawsuit, there are going to be people who don’t want to relive whatever trauma they experienced as a result of that privacy violation,” the panelist observed.

A data/technology expert pointed out that “the effectiveness of identifying special kinds of data is extremely limited. For example, anything that we might put forward is not going to be applicable across all communities.” This panelist also weighed in on the discussion of genetics, noting, “What makes [genetic information] very different from what’s available in the hospital is the latent information that it holds. The value of genetic information is a function of time; that is, science knows more and more about what can be revealed in a DNA sequence or other genetic information. So, it is a little different. Not that genetic information should necessarily qualify for either exclusion or inclusion, but it certainly does have a different property.”

Another data/technology panelist said discrimination was an important topic because “somewhere down the line, there’s going to be a breach,” and “ultimately we’re going to be faced with the question of penalties.” The moderator suggested that the panel address this concern during its later discussion of enforcement and regulation.

A policy analyst attempted to pull together panelists’ earlier comments, noting, “Something has come out in several comments is that, even if we have a fairly clear sense at this moment of what information is sensitive, what information ought somehow to be privileged, that is subject to changes we can’t foresee, which, in turn, creates a problem in identifying specific categories or classes of information.” Genetics in one example, the panelist said, but even a routine dental examination someday might yield sensitive information. For example, “If there’s something new that my dentist can say about me, or if there’s some new public health recognition that when this shows up in a dental record, oh-oh, we’ve got a public health problem. That may not be feasible today, but as we learn to exploit data in new ways and think of new questions to ask, that’s going to change.”

A government panelist suggested that the prediction about dental information may already be coming to pass. “Have you been following the research on the interaction between gingivitis and heart disease? There’s now a link between those two. And people who have bad gums really ought to be taking care of their whole body, it appears.”

Picking up on the discussions of research and genetic information, the government panelist said the potential concern reaches across generations. “It’s not just the individual’s
That should be specifically included?" entities that should be excluded from posing the question, “Are there any of applicability to a different topic, a whole host of other diseases, I couldn’t make that decision individually. I’d have to take into account that my children and my siblings would be potentially affected, and possibly negatively affected, if it turned out that I have Huntington’s genes or something else. So even a decision to participate or not participate [in a research study] is already being affected by the perceived lack of protection for this information.” However, the panelist agreed with the general tenor of the discussion that, “The better long-term approach for our society is to adequately protect all the information because we can’t tell today what’s going to be linked to something tomorrow.”

— A government panelist

Re special protections for genetic data: “The better long-term approach for our society is to adequately protect all the information because we can’t tell today what’s going to be linked to something tomorrow.”

— A government panelist

A policy analyst began with a comparison of the European and U.S. approaches to privacy. “The European approach is to have omnibus privacy laws that apply across the board to all kinds of records,” the panelist explained, but emphasized, “I’m not advocating that” because it would not be practical in the United States and “would create a lot of problems.” The U.S. approach is to look at things by sectors, the panelist explained. “Whichever one you do, you have to pay a price. The sectoral approach means you have to define what is and isn’t medical information. We can define it up to a point if it falls reasonably well within the constraints of the statute. But when you call up an airline and order a low-fat meal, is that medical information that has to be treated differently than other information? That’s the kind of question you have to deal with using a sectoral approach.”

A health industry panelist asked the policy analyst for clarification on the European standard, particularly how the European approach to medical records compares to the HIPAA standards. The European privacy regime, the analyst explained, centers on categories of sensitive information such as health data, ethnic origin, sexual orientation, and trade union membership. “The basic policy of the European directive is, that if you want to process sensitive information, you need affirmative consent of some sort.”

Another health policy analyst rejected the notion of regulating privacy by entity. After grappling with the question of who is or is not a covered entity under HIPAA, this speaker said, “I came to the conclusion that we’re going to spend too much time figuring out who it applies to—sort of the forest and the trees problem. I would suggest focusing on the data to properly define what is sensitive information or patient identifiable medical information, and how it is used, how it is disclosed, as opposed to identifying who or who would not be subject to it.” The panelist acknowledged the need for special rules for law enforcement or public health entities, but stressed, “again, it goes to the use and who has responsibility for that particular purpose. . . . The issue of what is the appropriate entity to have the information also, I think, goes to the issue of use of the information.”

Another industry panelist agreed that privacy standards “should apply across the board, regardless of what the entity is. I also agree that use of the information should be the determining factor, not what entity is using them.” The panelist suggested that because the HIPAA rules apply only to certain groups, “the entities to which it does apply are being faced with heightened duties, heightened responsibilities that would not be necessary if we have an across-the-board regulation.”

A government panelist acknowledged that the HIPAA rule’s focus on entities “leads to some very, very odd results. For example, if you have precisely the same information held in two parts of the same entity, subject to different rules. But remember when the legislation was enacted, the determination was made that the restrictions would apply to the parties who handled the information the most,” the official explained.

A policy analyst defended HIPAA’s focus on users. “There are a variety of different users, and you cannot apply the same standards to everybody. You want to have one standard that applies to your doctor, but when the public health agency gets it, or a researcher, they are a different user, they have different uses, and they have to be addressed in some ways on
an individual basis. So whatever you do, you can’t just talk about this as one rule that applies to everybody. You’re going to face these problems however you cut up the pie.”

Because HIPAA applies to a limited number of entities, a health industry panelist suggested, “As the states are looking at comprehensive privacy legislation for themselves, they look at what the federal law covers, and they see these huge gaps, all these other entities that are not regulated. So they’re creating laws that have implications for HIPAA-covered entities as well as other entities, and we’re running into conflicts and problems between the various rules.”

Another policy analyst pointed out that “how laws and regulations apply, to whom they apply, what they do—is a very cumbersome tool for nurturing a culture of respect for privacy. There are cultural messages being sent. Are there some messages that are better sent by other means? Is public education better done in other kinds of ways?”

A data/technology specialist said that attempts have been made to analyze privacy risks by categories of entities that have access to health information. Primary users would include those directly involved in patient care, such as physicians and hospitals, and entities with a specified obvious need, such as insurers. Secondary users would include researchers and others. However, “when you start to try to either find the blanket rule or identify entities in a more defined way beyond that, there are problems with consistency of application because inferences can come from the entities not covered. It’s really a mess having this sector-based privacy in a world where data comes from everywhere,” the panelist said.

A health industry panelist expressed frustration that privacy discussions do not talk about “intent.” “There are problems that are partly defined by the intent of those who are perceived to create a problem, and there are various kinds of solutions to problems that need to be tailored to the intent of the use or misuse of whatever it is we’re trying to protect. Making general statements, or writing general proscriptions, aimed at either the least problematic of those uses or the most problematic absolutely creates chaos. We’ve got to put some kind of intent into the discussions that we have, both to identify what we think are problems and to identify remedies.”

**Jurisdiction**

The moderator moved the discussion on to the subtopic of jurisdiction, suggesting two subquestions: “First, what kind of preemptions should federal regulation produce? Should it establish a floor of protections but make room for state protections that are more protective of information, or should federal regulation be a more complete preemption approach that just knocks out inconsistent state regulation altogether? Second, there’s the complexity problem of 51 or more jurisdictions that are all weighing in, in a cumulative way, just stacking regulation upon regulation, and the kinds of compliance issues and comprehensibility issues that might raise.”

A health industry representative led off the discussion, suggesting that a “common sense approach” would be a uniform set of standards that applied across state borders. However, the political reality is that “it’s almost impossible to get there.” As the debate moves forward, this speaker said, “You’re going to see a clash between this common sense concept of a uniform rule and the political reality of states wanting to protect areas that traditionally have been areas of state concern.”

Another health industry panelist said the lack of federal preemption is “the issue we hear about the most, because of the complexity, but also the cost.” The healthcare system now transcends state borders, the speaker said, citing the Washington, DC, area as just one example of a care setting “where you may receive your treatment in one jurisdiction and have your prescription filled somewhere else. If we’re just looking for how we can make the whole healthcare system more efficient, preemption is really a premier issue that we would all like to see addressed.”

Another health industry panelist endorsed the last two comments, citing that not only care that may be rendered in two different states but information that may flow through computers housed in several states. “Which state’s rules apply,” the panelist asked. “In addition, from a jurisdictional perspective, where would the cause of action be brought?”

A policy analyst came at the issue from several directions, noting that preemption “is a curiously emotional issue.” Patient advocates have strongly held views, in part from a conviction that states should be allowed to enact more stringent protections, and,

---

Too often, “preemption is being discussed at the level of a slogan. It’s either preemptive, or it’s not preemptive. It’s a lot more complicated than that whichever route you take.”

— A policy analyst
in part, from a recognition that preemption “is a great bargaining chip” in the privacy debate. Too often, the analyst suggested, “preemption is being discussed at the level of a slogan. It’s either preemptive, or it’s not preemptive. It’s a lot more complicated than that whichever route you take,” the panelist said. With or without federal preemption, the speaker said, there are complex questions about the status of state laws.

Further, “preemption is not a unitary issue. There are some areas where preemption of state laws makes a lot of sense,” the panelist continued, citing HIPAA transaction standards as an example of where one set of encryption standards should apply. On the other hand, the speaker suggested, “What’s so terrible if the state of Minnesota has a rule that says patients get access to their medical records, and they get one copy for free. If that’s Minnesota’s policy, does that have to be preempted by a federal law?” State agencies also get access to and use health records for a variety of purposes, the speaker continued. “What is so terrible if a state decides to have a higher standard for law enforcement access by state officials? That doesn’t affect the federal scheme,” the speaker said.

A health industry representative supported federal preemption, asserting, “Probably the most salutary thing you can say about a federal privacy law is that it should assure you, whether or not you live in Maine or Minnesota, that there’s a level of protection you get regardless of what state you’re in, and that’s an assured right on the behalf of patients.” Without preemption, the speaker said, “the practical problems with states are legion.” For one thing, state legislators are more influenced by politics. “The way they enforce the law often has less to do with what the law says as opposed to what the political climate is.” Recognizing that neither viewpoint on preemption would prevail, the speaker suggested that federal law establish a baseline for medical privacy but allow states to have an enforcement role. There is precedent for that approach in the FTC’s lemon laws, the speaker suggested.

A government panelist made a similar suggestion. “Is there a functional middle ground? Is there a way to create a federal standard for just about everything but carve out some areas where states have the ability to put more stringent or different rules in place, such as law enforcement, rights of minors, and things like that? Would that be acceptable?” the speaker asked.

A health industry panelist called preemption “an incredibly emotional issue,” and posed two questions: “One, what is the trigger point? Is there a level when the harm of not having preemption reaches a certain point that you have to have preemption? Why is it that we have preemption in the ERISA pension arena and ERISA plans?” A second question: “On the flip side, if the federal government does come in, how do you keep that baseline regulation from getting into such detail that when, for example, Texas decides to create the sensitive and the super sensitive, and redefines who’s covered or not, we as a company, and our clients who have multistate types of operations, find ourselves unable to figure out what the appropriate rules should be.”

A state government panelist acknowledged feeling “lonely, really lonely” in the discussion of preemption but asserted, “States are inconvenient, but we’re not going anywhere.” On a variety of issues, the panelist said, industries say they want one rule, “but we’re not set up that way. And so, you’re not going to get that. . . . So what’s the logical way to make everybody a little more happy than they are currently?” The state panelist pointed out that states have filled a vacuum on health information privacy. “We did find a need, and we filled it, and that’s an important function that states serve, “ the panelist concluded.

“Is there a functional middle ground? Is there a way to create a federal standard for just about everything but carve out some areas where states have the ability to put more stringent or different rules in place, such as law enforcement, rights of minors, and things like that? Would that be acceptable?”

— A government panelist

A consumer advocate returned to the government panelist’s earlier call to seek the “common ground” on preemption. Many states have enacted medical privacy laws, the consumer panelist said, but “very much on a hit-or-miss type of approach” that target specific conditions such as AIDS. The HIPAA preemption standard, she said, by avoiding specific conditions or other areas that states have focused on, “will, in fact, result in a tremendous amount of uniformity across this country.”

The consumer panelist admitted becoming annoyed at industry’s criticism of the HIPAA preemption standard because, “to the extent that entities are subject to state laws, and they are national or multistate corporations, they already have to comply with a lot of different state laws.
HIPAA didn’t create this problem of differing state laws that might apply to a telemedicine transaction, or to somebody who lives in one place but gets healthcare in another and works in yet another area. HIPAA didn’t create that problem, and it actually makes the problem simpler because it will promote uniformity.”

A health industry panelist spoke out against some state privacy laws, asserting, “We have a system in which any component can do anything stupid that it pleases, and there’s not much we can do about it.” The panelist illustrated his point with two state examples. “One of them is the state of Maine, which rescinded its law within days or weeks of enactment because it brought the entire healthcare delivery system in Maine to its knees. The other one is Minnesota, where it is impossible to do public health research, it is impossible to do health services research, and it is impossible to do a phase four post-marketing trial of a drug or device for adverse events.” The real issue with preemption, this panelist said, is this: “Are there policy imperatives that rise to the federal level? If we could identify some of them, and say that those cannot be preempted, then we might have a chance at tailoring a federal policy.”

Another health industry representative stressed the importance of preemption to medical progress. “If we don’t have uniform standards, we will not be able to develop new therapies anymore. We are already caving in under the weight of many regulations that we have to observe when we develop new therapies. If we have to now go to each state every time we have to initiate studies, it will become virtually impossible. Likewise, with regard to safety surveillance, we’re quite apt to miss a very important safety signal if we can get data from some states and not others,” the panelist said.

A consumer panelist focused on federal preemption and online privacy protection. “We’re concerned about privacy, but we’re also concerned about a competing interest—the health of the Internet. We see the value in preemption and its role in solving some of the jurisdictional issues and in providing predictability, not only for business but for consumers, and also preserving the health of the Internet because people going online will understand what they’re getting into, understand what will be happening to their information and what choices they have in it. At the same time, we recognize that states have a very important interest in protecting the privacy of their citizens.” Federal preemption can solve some problems, this panelist concluded, “but we have to be very careful that preemption doesn’t become an excuse for lowering the [privacy] standards overall.”

A government official offered the thought that earlier suggestions for a list of national policy imperatives, or “carve outs,” of areas where states could enact more stringent protections are “two sides of the same coin—are there areas for states and areas for federal protection?” The panelist suggested, “We could probably have uniformity in areas of research, both records-based and controlled trials. The area of public health is probably another area where we could achieve uniformity. Identifying the dead [may be] an area for uniformity.”

A health industry representative linked health privacy to other areas where federal preemption is the rule. “It seems to me that medical privacy laws aren’t any less important than antitrust and telecommunication laws where we’ve made a conscious decision that the federal laws really should preempt the states in most regards. I don’t know why medical privacy should be relegated to a second tier because it’s not a commercial issue. However, I do see a role for the states, and I’d like to see that role [be] enforcing a uniform law.”

—A health industry panelist
issue. However, I do see a role for the states, and I'd like to see that role [be] enforcing a uniform law,” the panelist concluded.

Another industry panelist related the discussion to many panelists’ stated goal of seeking “an appropriate balance.” “I think this is a real balance question,” this panelist said. “Should we be devoting an unbelievable amount of resources towards compliance with this patchwork quilt of regulations and statutes in the various states, or can we strike a better balance between establishing what that standard should be. Maybe [we should] leave certain areas to the states, but simplify it in some way so it’s better for the consumer, better for the patient, as well as better for those that have to comply with the requirements?”

A third health industry representative clarified the Maine experience, describing that state’s original statute as “too restrictive” and “a law of unintended consequences.” The panelist said the original law “prohibited the release of any information without the patient’s consent. Hospitals could not tell family members what was going on with their family other than very general information.” The state learned that “the balancing act is very difficult, and that you have to weigh all interests and draft a law that’s not so restrictive that you end up with consequences you don’t want,” this panelist said.

The moderator gave a state government panelist the opportunity to wrap up the discussion on preemption. The panelist emphasized that states do not necessarily oppose preemption. States are concerned that “federal language could end up pre-empting state laws where there isn’t a federal protection. . . . . We’re concerned about people losing protections that they had at the state level that are not then replaced by a federal protection.” The panelist also expressed concerns about the adequacy of federal enforcement mechanisms. Federal agencies may not have the resources needed to enforce federal privacy regulations, the speaker suggested. “[States] want to make sure that where they’ve put protections in place, that people don’t lose protections, and that whatever is put in place [at the federal level] is enforceable,” the speaker concluded. (For an overview of state developments, see Appendix D, “State Healthcare Privacy Laws,” on pages 59.)

“[States] have not taken the position that there should be no federal preemption. . . . . “[States] want to make sure that where they’ve put protections in place, that people don’t lose protections, and that whatever is put in place [at the federal level] is enforceable.”

— A government panelist

Use and Disclosure

The chief moderator turned the program over to another Health Lawyers facilitator to lead discussion of the next subtopic, use and disclosure of health information. This moderator suggesting examining the following subtopics:

- The distinction between use and disclosure, and how individuals’ expectations differ;
- Exceptions or exclusions from the regulation of use and disclosure;
- The concept of “minimum necessary” information and the standard for use and disclosure;
- Identification and de-identification, and how that affects use and disclosure of protected individual information.

A data/technology specialist said that from a technology standpoint, “use” refers to the person or persons who receive a set of data that a data holder chooses to “disclose” to them. A policy analyst referred to this as a “classic definition,” but said it didn’t work in the real world. “You can take the exact same transfers of data from one person—from one entity to another, from one office to another—and in some cases it’s a use, and in some cases it’s a disclosure because of the reality of the legal relationships between the people. So, in the end it really doesn’t help that much to try and say, ‘Well, this is a use and it has a different kind of rule attached to it; and this is a disclosure, and it has another one.’”

The first speaker clarified that “use is specifically the purpose to which the data is being put,” and “disclosure means the responsibility of the person who holds the data.” The policy analyst agreed but referred to “purpose” as a “weasel word.” “Data isn’t collected for a purpose. It’s collected for a whole passel of purposes, overt and covert,” this speaker said.

The moderator suggested that the two speakers both were focusing on the collector of data, and suggested turning the question around: “What are the individual’s expectations? Do they distinguish between use and disclosure?”

A consumer panelist reiterated a statement made earlier in the Colloquium that distinguished between what individuals think their health information will be used for versus how it is actually disclosed. “I
think people have the expectation that their medical information will be used for medical purposes and not disclosed to other entities such as insurance companies, banks, their pension plan, their employer, etc.

A government panelist stated that the goal of the “minimum necessary” standard was “to restrict gratuitous releases.” The panelist traced regulators’ concern “back to the problems presented in paper records when it takes more effort for a person to sort through to find the particular pieces of information they need from a record, and it’s easier for them just to copy the whole thing and send it on for whatever purpose. They let the second person down the road do the work of extracting the data.”

Computerized records, the speaker noted, make it much more feasible, and actually inexpensive, to select the desired piece of information. The speaker acknowledged that the healthcare system is still very dependent on paper records and “not in a position to take advantage of the economies that are down the road.” The speaker closed by returning to the theme of education raised by various speakers and suggested, “We as a whole need to educate ourselves and the public about the potential benefits and costs and new economic paradigms created by the very, very large computer databases and the flexibility and ‘transmissibility’ of the data.”

The moderator next directed the panelists’ attention to identification and de-identification, and how that affects the use and disclosure of protected individual health information. She posed the question, “How can a person be identified and tied to their health information in today’s Internet environment?”

A data/technology expert said, “It doesn’t take very many pieces of information to uniquely identify you” citing the earlier example that with just three pieces of information—date of birth, gender, and zip code—it is possible to identify 87 percent of the U.S. population. Americans tend to choose homogeneous living arrangements, the panelist said, and “as a result of that, it turns out that it just doesn’t take very much information at all to make you unique.” At the same time, so much information is collected, and shared or otherwise available that one doesn’t need a name, Social Security number, or anything else closely tied to a person in order to re-identify him or her.

Many people, hearing how easy it is to re-identify a person, assume the situation is hopeless. The panelist said, “Actually, for many years there have been disclosure limitation techniques available, and they’ve been used in a variety of communities. We’ve also looked at them in the context of healthcare. But for whatever reason, unlike the national security community, unlike the statistical community and so forth, healthcare has just been incredibly resistant to change the discussion from anything that’s either explicitly identified or de-identified, meaning that the explicit identifiers have been removed. Really, I don’t find that helpful. You really should think in terms of the gray area, of what does it mean to render the data sufficiently anonymous and still have it be practically useful.”

The HIPAA approach, which specifies which identifiers to exclude, does not address de-identification “in a constructive way,” the panelist said. “On the one hand, you really want the data to be practically useful so that [researchers] can get all the information they want. But you also want to destroy inferences to the identity in the least invasive way.” The objective is to “minimally distort the data,” the panelist said, noting that “there are some very simple techniques that can be executed in Microsoft software that can re-identify people but also render the data sufficiently anonymous” for privacy purposes.

A health industry panelist stressed that “a very large amount of what we typically think of as medical and health research information, whether it’s individual or population-based, can be done with information that does not have direct identifiers.” The speaker clarified that he was talking about “direct identifiers” that would tell general users whose record was before them, not information through which a technologically sophisticated user like the previous speaker might be able to re-identify the person. Further, he said,
researchers “do not want to know the identities. They don’t mean anything to us.” Researchers do need “linkages” among data in order to identify commonalities or trends, but the speaker stressed that the whole de-identification process should be kept simple. “Our argument has been keep it very simple and, therefore, easy to do. Allow for linkages, but figure out a way to protect the links so that you can’t just go right ahead and re-identify—but [then] penalize inappropiate efforts to re-identify,” the panelist said.

Another health industry panelist said current wisdom in the online world is that “somebody who has the time, effort, and resources can figure out who you are.” That doesn’t mean no effort should be made to obscure identifiers, “but there has to be some reasonable point at which we acknowledge that somebody with a lot of computer sophistication and a lot of databases can figure out who we are. That’s just the reality of living in the 21st century.” Agreeing with the previous speaker that “we could keep stripping things ad infinitum,” this panelist noted that the final HIPAA regulation enumerates 19 categories of identifiers while the regulations for children’s online privacy contained only four or five identifiers. “Who’s got it right, and why is it so different in the medical arena as opposed to the online privacy arena?” this panelist asked.

A health policy analyst said that over the years he came to “view non-identifiable information as sort of the ‘free lunch’ of privacy.” With what he has learned in recent years about re-identification techniques, he “discovered that the best we could hope for was maybe a ‘free snack.’” This panelist agreed with the first health industry speaker that “there are other ways of trying to control information and still make it useful through laws, through contracts, whatever.” The analyst took the industry to task, however, for lagging behind on privacy. “The healthcare industry—the doctors, the hospitals, the plans, the insurers—have for decades totally ignored privacy, and a lot of the federal agencies as well. One of the reasons we’re in such a mess today is because we have to catch up from ground zero, and it’s a really sophisticated situation. We’ve already foreclosed a lot of options just by the way the industry has developed and the laws have developed or not developed. . . . It requires a cultural shift to go back to the beginning and say, ‘Can you do your business another way, and maybe only get the identifiers at the end when you really need it?’”

A government panelist suggested another avenue for dealing with de-identification/re-identification concerns. “That is to pass it by a learned body—an IRB [institutional review board] or privacy board to say, ‘Yes, you can use identifiable information without the individual’s authorization, but you have to follow the following conditions.’ Then ensure that the conditions are fairly well spelled out.”

Another government official agreed that the healthcare field, both in government and the private sector, lacks technological sophistication on data de-identification. “One of the things I found out when I first got into this area was that the health data community was not aware of the data suppression techniques and some of the statistical techniques that had been developed for economic analysis, for census bureau use, and probably for some others as well.” However, new options are being developed by the Health Care Financing Administration. One would establish a database of identifiable information against which researchers could run their analyses. Another approach would use “dummy data sets.” “You can still have the research. You can have as many different runs against the data as you wish without indentifiability,” the official said.

A second approach under development is similar to the “trusted body” approach suggested by an industry panelist. “There’s another whole group within HCFA that’s working on that service. They would hold sets of data, and then people could send in their data to be linked against it. The researcher would get back the fuller set of data, but it would then be reviewed to ensure that there were no small cell sizes or other uniques held within the data,” the government panelist said.

A health industry panelist noted that states collect a lot of health information and expressed a concern that state governments need to be more careful about their stewardship of health information. The panelist said, “As we know, there’s the famous or infamous case of [states] selling our driver’s license data freely. I think that’s also true with health data. So I don’t know why we’re so worried about individual researchers when the state is collecting it and selling it to the highest bidder, and nobody seems to be suggesting that there need to be strict controls on the states.”

A government panelist acknowledged that state governments had received adverse publicity for their “entrepreneurial escapades” with driver’s license data, and “most states are addressing that.” This panelist picked up on a comment by a technology expert to the effect that genetic studies indicate that a small number of people seem to be “reverters who seem to have a natural immunity to HIV.” The technology specialist had
suggested this as one type of finding that would make it desirable to be able to re-identify people when needed. “I think that increasingly that’s going to be the case with a lot of gene-based therapies. You have to link it back to a person because that person is going to be the source of the material that’s so useful and constructive,” the technology expert had said. The state government panelist suggested that while some efforts to re-identify individuals might stem from altruistic motives, other attempts to identify people with certain genetic markers might arise from less noble motives. “I think that what drives part of this whole [privacy] discussion is the fear that, without your consent, somebody is going to show up with a nugget of information about you, and present you with it, and want to do things with it. . . . It’s the worst-case scenario that drives a lot of the debate,” this panelist said.

The data specialist who earlier discussed various techniques for re-

identifying individuals said there was “a lot of confusion” about linkages. “This notion that you need a trusted party, and that somehow the linkage is on name or Social Security is just wrong,” this panelist said. Social Security numbers and names actually are notoriously bad for linking because of simple clerical errors such as inverted digits or misspellings. Items such as gender, birth date, or zip code, which the panelist termed “quasi-identifiers,” “turn out to be the key to doing real linkage.”

A health industry panelist stressed that researchers need to be able identify the population of a medical study. However, “you do not need names, addresses, phone numbers, photographs, and Social Security numbers. You need something that will allow you to follow the course of the illness in each of those people over time, and so you need linkage. That linkage can be a hospital accession number, it can be a random number that’s unique to that individual with 7,000 digits in it, or whatever you want.”

A government official said the last speaker’s assertion was not accurate for all situations. “Sometimes the very information that will identify the individual is also needed for research.” In these instances, the best way to protect an individual’s privacy might be “a legal document that confers the ability to use the data but also restricts the information and shows what’s going to be done at the end of the research project with the data.”

The moderator noted that consensus on identification/de-identification had not emerged from the discussion, although many interesting and important points were raised. She then directed the panel’s attention to a new topic: individual rights.

Individual Rights

The moderator explained that this segment would not deal with individuals’ expectations, but rather with individuals’ rights and responsibilities. Subtopics, the moderator said, could include:

- What are individuals’ rights and responsibilities regarding the handling of data in the event that individuals put conditions on use of their information?
- Are there any classes of covered entities or users that should be excepted or exempted from individual rights-related requirements?
- What access should individuals have to their records; should they be able to amend those records; should records of disclosures be maintained?
- What legal recourse should individuals have in the event their rights are jeopardized or abused; should they have the right to sue?

A legal expert began with a focus on the rights of a less visible sector of society—prisoners—noting that this group had been passed over in the proposed HIPAA regulations. This was rectified in the final rules, but the speaker said he “remains concerned that there’s not enough focus being given at the national and local levels to the fact that prisoners don’t have a lot of rights and remedies when it comes to their personal privacy.” A technology expert noted that military personnel are another group that is relatively unprotected.

A consumer panelist mentioned another important group—minors. The HIPAA rule, this speaker said, has “a very balanced approach to the rights of minors,” recognizing that as a general rule, parents exercise rights on behalf of their children. However, there are some instances where minors should be able to exercise those rights themselves.

The moderator asked how the Scandinavian countries, referred to earlier, and other nations are able both to allow broad access to information but also to provide protections so that
individuals are willing to have their data used. A government official related a story of raising this issue during a talk and having a French woman reply, “You know, there is no need for this in our country because (a) we have rights, and (b) we have universal health insurance.” That is also the case in Scandinavia, the panelist said, but said that the U.S. and European healthcare systems are fundamentally different. “Availability of the Scandinavian data would be very tempting and we would love to have that, but that’s not the economic system under which our people have to operate [in the United States],” the panelist said.

A data/technology expert noted that privacy risks do vary in other nations because “as soon as you have a country that has a different healthcare system, the risks change.” However, a key difference from the U.S. situation is that citizens in other nations do not have to “show harm” as we do in this country. In the United States, “when an individual is harmed, and they go into court, they have to actually show that they’ve been hurt.” In most other nations, the panelist said, “all that I would have to show is that it was possible or that the [violation of privacy] could exist, and that alone would be sufficient to take [legal] action.”

The moderator observed that the flip side of individual rights is individual responsibilities. “What are the responsibilities that an individual will have to the extent they want to limit their consent, access their records, make modifications, etc.? Are there liabilities that individuals should face in the event that they exercise their rights?”

A consumer representative returned to the ongoing theme of public education, suggesting, “The public really has a responsibility to go out there and know what can be done with their information, and whether or not they have informed consent, whether they should consent, or whether or not they can opt out of giving individual information.”

> “The public really has a responsibility to go out there and know what can be done with their information, and whether or not they have informed consent, whether they should consent, or whether or not they can opt out of giving individual information.”
> — A consumer representative

A health industry panelist addressed individual responsibility with respect to a patient’s right to amend his or her medical record. “Our concern is that you should [be able to] modify it if you’re going to make it more accurate,” this panelist said. However, patients need to recognize that they could put themselves at risk if they delete information they don’t want others to know that may be needed by health professionals to provide appropriate healthcare. With the growing reliance on electronic records, there are also practical concerns about the allowable length of patients’ amendments.

Another industry panelist said his understanding of existing laws and regulations was “that you never change a record.” Providers may be required to accept a correction or amendment to a record, but that is not regarded as a problem. This panelist also reported that in states where patients had a right to amend their medical records, “it’s used very, very infrequently and has not been a burden” to the industry.

A government official explained that “the right of amendment has existed under the federal Privacy Act for 26-plus years.” The industry panelist is correct that it’s seldom used. “People have really exercised this right very judiciously. They’ve saved it for really egregious cases.” The panelist said the HIPAA provision also provides for an addendum or amendment. The original entry is not changed, and the amendment must be signed and dated. “So it’s not a case of going in and rewriting someone’s medical history,” the official explained.

A health industry panelist raised one caution, that the right to inspect and amend a record should be limited to information that is currently being used. Some insurance companies have records that are more than one hundred years old. They need to be assured “that they’re not expected to go back and search all of those records and find information that might identify an individual,” the panelist said.

The moderator said she sensed consensus that, with some cautions, individuals should have the right to append amendments to records of their health information.

The moderator announced that one individual rights issue—a private right of action—would be considered under Core Question Two’s last subtopic, the framework for a legal response to privacy issues.

**Framework for a Legal Response**

A different Health Lawyers moderator facilitated this discussion and explained that, because of time constraints, the framework for a legal response to privacy issues would be combined with the discussion of regulatory and enforcement issues. In fact, panelists filled the time available with discussion of one major, controversial
issue—a private right of action for privacy violations.

A consumer representative began by asserting that for consumer advocates, “there is unanimity in the belief that there should be at the federal level a private right of action for individuals for misuse of their healthcare information.” This is particularly important in view of increased use of computers, whether for medical records or as repositories of other identifiable sensitive information. “We’re asking individuals to take more responsibility for knowing what’s being collected and maintained about them, and then to act accordingly to protect themselves. To ask consumers to do that and not provide a private right of action is counterintuitive,” this panelist said.

A government official discussed implementation of the Children’s Online Privacy Protection Act (COPPA), a simpler statute than HIPAA that applies to a smaller range of activities. Based on experience thus far, the official said, “If there were a private right of action associated with technical violations of that statute, there would be a lot of Web sites out of business very quickly.” Clearly defining what conduct is prohibited or allowed is essential, and affected parties need some time to come into compliance. Relying on federal and state enforcement, the panelist said, “provides a way for implementing the statute in the best way.” One approach worth considering, this speaker said, is the model provided by the Fair Credit Reporting Act, which provides a graduated approach to liability based on the degree of harmful conduct and creditors’ experience with the requirements.

A policy analyst countered that COPPA, in fact, provides a “great example” of the need for a private right of action. This panelist said, “There are Web sites all over the place that would have been sued, and might have been closed down, or might have changed their act if private lawyers could sue them. Instead, we have nothing. Enforcement by the FTC is nothing. The FTC has brought a handful of privacy cases. . . . Unless you have some kind of private right of action, you’re not going to get any kind of significant compliance because nobody’s afraid of the FTC, and nobody’s afraid of HHS.”

A health industry panelist strongly disagreed with the last speaker. “With the private right of action, the first thing I thought of was, ‘Oh, so is that in addition to the jail time that I will have to serve and the $250,000 penalty? What was it—ten years in jail? So now I’ve got a private right of action on top of this.’” For corporations, this panelist suggested, the FTC does wield a lot of influence, particularly with respect to privacy and e-commerce. Corporations carefully watch for inconsistencies between their practices and their state privacy policies, recognizing that government is watching. “So I think the model that the FTC represents has actually been quite effective,” the panelist concluded.

A data/technology expert suggested whether a private right of action is needed in view of other courses of action open to consumers or agencies. HHS’ Office of Civil Rights, for example, will be vigorously enforcing the HIPAA regulations, which include both fines and criminal penalties for violations. “And criminal penalties, at least in the hospital community where, in order to support e-commerce, corporations had to come up with [processes] that would protect privacy so that people would feel comfortable enough to use their credit cards.”

Re using economic incentives rather than lawsuits: “When the money is behind privacy protection, you come up with incredibly cheap solutions that are quite effective. One of the best examples has been in the Internet community where, in order to support e-commerce, corporations had to come up with [processes] that would protect privacy so that people would feel comfortable enough to use their credit cards.”

Another industry panelist asked whether a private right of action is needed in view of other courses of action open to consumers or agencies. HHS’ Office of Civil Rights, for example, will be vigorously enforcing the HIPAA regulations, which include both fines and criminal penalties for violations. “And criminal penalties, at least in the hospital community where, in order to support e-commerce, corporations had to come up with [processes] that would protect privacy so that people would feel comfortable enough to use their credit cards.”

A data/technology expert suggested whether a private right of action is needed in view of other courses of action open to consumers or agencies. HHS’ Office of Civil Rights, for example, will be vigorously enforcing the HIPAA regulations, which include both fines and criminal penalties for violations. “And criminal penalties, at least in the hospital community where, in order to support e-commerce, corporations had to come up with [processes] that would protect privacy so that people would feel comfortable enough to use their credit cards.”

A policy analyst countered that COPPA, in fact, provides a “great example” of the need for a private right of action. This panelist said, “There are Web sites all over the place that would have been sued, and might have been closed down, or might have changed their act if private lawyers could sue them. Instead, we have nothing. Enforcement by the FTC is nothing. The FTC has brought a handful of privacy cases. . . . Unless you have some kind of private right of action, you’re not going to get any kind of significant compliance because nobody’s afraid of the FTC, and nobody’s afraid of HHS.”

A health industry panelist strongly disagreed with the last speaker. “With the private right of action, the first thing I thought of was, ‘Oh, so is that in addition to the jail time that I will have to serve and the $250,000 penalty? What was it—ten years in jail? So now I’ve got a private right of action on top of this.’” For corporations, this panelist suggested, the FTC does wield a lot of influence, particularly with respect to privacy and e-commerce. Corporations carefully watch for inconsistencies between their practices and their state privacy policies, recognizing that government is watching. “So I think the model that the FTC represents has actually been quite effective,” the panelist concluded.
solutions that are quite effective. One of the best examples has been in the Internet community where, in order to support e-commerce, corporations had to come up with [processes] that would protect privacy so that people would feel comfortable enough to use their credit cards.” Developments by online companies that deal with health information are “very exciting,” this speaker said. They have recognized that solving privacy problems is necessary to their business goals, “and they’ve come up with some really interesting, different techniques, [including] data linkages where all the data all the way through the channel is totally anonymous but out the other end comes the linked result.”

A policy analyst found it hard to accept “at face value” the industry panelists’ assertions that a private right of action would be ineffective. Available sanctions will, in fact, do little. “The criminal penalties, if they’re used at all in the next 15 years, will be against some incredibly awful player and not any legitimate business, any legitimate hospital. The good players have nothing to fear by criminal penalties or by private rights of action,” this panelist asserted.

A different health industry panelist cautioned that the physician community generally supports the HIPAA privacy rules. However, physicians already are burdened with compliance requirements for antifraud and abuse laws, English proficiency compliance, and so forth. Allowing a private right of action, this panelist said, would “create a firestorm in the medical community” that could result in total opposition to the entire regulatory effort on privacy.

A state government panelist suggested that in view of the value of health information to some corporate users, “it would be cost-effective to pay the fines that are in many of the statutes. . . . The fine would be a cost of doing business, and well worth it.” Allowing a private right of action would raise the ante, this panelist said, suggesting this as one reason why many organizations support giving individuals the right to sue for privacy abuses. Lesser sanctions, such as allowing suits only for intentional violations or imposing additional penalties for intentional violations, likely would win support, this panelist said, particularly if they addressed major areas of concern such as discrimination in employment or eligibility for insurance.

“Most of the things that happen to consumers happen invisibly,” a government official observed, suggesting that “the only thing that’s really going to work for detection is letting consumers somehow have access to enough information to determine whether the violations have occurred.”

A health industry panelist suggested that the analyst was “underestimating the power of the federal government and the regulatory penalties” that are available. In areas such as compliance with antifraud and abuse regulations, this panelist said, “it isn’t just a few bad actors that get caught up in this enforcement mechanism. It’s been thousands of hospitals that felt that if there were billing errors that were characterized as fraud and abuse, they would be prosecuted thoroughly and would pay huge fines—both through the efforts of the Department of Justice, as well as the OIG.” The panelist endorsed the comments of an earlier industry representative that allowing a private right of action would “tip the balance toward total opposition to privacy regulations.

A consumer representative said it was “crazy” to believe the HHS Office of Civil Rights will have the resources that it needs to enforce HIPAA. Although a private right of action appears politically unfeasible, this speaker said, “it is in the best interest of consumers to have that as an option and to give the industry a greater [incentive] to do the right thing.”

A different policy analyst reminded the panelists that, in the broadest sense, the regulatory approaches that are chosen make a statement about society’s values. “[Should we have] a punitive focus on individual bad actors or a positive reinforcement of the values we think are at stake?”
Either course carries a message, this speaker said. “It’s not just about what regulations you come up with, but what kinds of messages you [send] the world,” the panelist said.

A health industry panelist said the major issue for the healthcare field “is ambiguity—and nobody wants to be sued for ambiguity. . . . At a minimum, the trade-off for a private right of action is clarity in what a law or regulation seems to be saying is inappropriate [behavior].”

With the allotted time nearly expired, another industry panelist closed the discussion by reiterating the variety of remedies that are available that, unlike a private right of action, “don’t require showing harm.” These include enforcement by HHS and the FTC, consumer protection laws, and a variety of state laws. “The healthcare community wants to be in favor of robust privacy protections,” the speaker said, but in the face of often-ambiguous privacy standards and the variety of other penalties that might be imposed, “facing a private right of action could really tip the balance” against HIPAA and other initiatives.
The moderator suggested beginning the discussion with the last subquestion, which deals with the minimum security standards needed to achieve privacy of individual health information. The panel then would address the other subquestions together, since all related to implementation costs. For that discussion, the moderator said, it would be appropriate for panelists to reference costs or operational changes that might be required by the HIPAA regulation or other initiatives.

### Minimum Security Standards

A data/technology specialist led off by briefing the participants on the overall economics of implementing privacy security mechanisms for electronic records. Meeting the HIPAA privacy standards would require implementation of three technical security mechanisms—authentication, access control and authorization, and auditability, the panelist said. These mechanisms verify the identity of users, allow access only to authorized users and at the level authorized for a given user, and record and examine system use to identify possible violations. Credible systems are “extraordinarily expensive” to implement, and “the likelihood of healthcare organizations actually being able to technically implement these safeguards is minimal,” the panelist said.

Another technology expert agreed that the systems described by the previous speaker are costly but, “in fact, very few of the Fortune 50 companies probably have that sort of gold standard.” This panelist was struck by the fact that “there’s a lot of security issues—non-electronic—that we have do deal with” and added, “A lot of the [security] breaches, whether intentional or unintentional, will be done by people who have authorized access.” It’s very difficult, this speaker suggested, to “have a [security] system approach, no matter what the cost, to really address those issues.” Given the human factor, this speaker said, it is important to “balance the technical capabilities and needs but also to understand the people, and initiate the training, the education, and the processes that you need to have in place to make people aware.”

“...will be done by people who have authorized access.”
—A data/technology expert

Another data/technology panelist took a similar tack, stressing that “security is not privacy.” Security refers to issues like access control. “Does the person have the right password, do they have access, are they authorized to use the data, who’s viewed the data, that kind of thing...” But 90 percent of what we’ve talked about today absolutely doesn’t have anything to do with security. It has to do with the way the healthcare system is decentralized, and how many different people hold the information,” the speaker said.

This panelist also pointed out that for small healthcare practitioners, help is at hand from a variety of e-health companies. These firms offer to maintain records and implement needed security measures. “They’re basically using e-commerce technology, which not only satisfies the security standards but does so pretty cheaply because it doesn’t really cost the individual practitioner very much to participate,” the panelist said.
A health industry panelist addressed security from the perspective of academic medical centers, noting that a handful of the larger systems that are recognized leaders in medical informatics believe they can achieve reasonable compliance within the required timeframe. However, the speaker continued, “Many teaching hospital executives, including large urban hospitals, say they can’t. And I haven’t met anybody who believes the HHS cost estimates—talk about fuzzy arithmetic.” The panelist went on to suggest that “a useful outcome of this whole debate would be a big federal, private, state initiative—sort of Hill-Burton, Jr., perhaps—that instead of bricks and mortar, would go toward bringing electronic information capability to the entire U.S. healthcare delivery system.”

A government panelist said this last suggestion was “a good idea,” but added, “of course, there is no money to implement HIPAA even within the federal government, much less to help the rest of the world implement it.” This panelist then turned to the issue of implementing security standards, noting that anecdotal evidence indicates that small healthcare practitioners seem to be addressing security concerns by retaining information in-house. Health insurance plans, on the other hand, seem to already have in place mechanisms for authentication, access, and so forth, perhaps, as one security analyst suggested to the panelist, “because they perceive the data as being economically valuable.”

The “nightmare situation” for security, the government speaker said, is the academic medical center, where “they have a dual purpose—treatment and research—and students everywhere.” In the interest of research and patient care, many students “think they are entitled to see everything” and to share their data freely with other students, sometimes across the Internet with students at other medical centers. Relating this to an issue raised earlier, the panelist suggested that where there is an economic incentive to guard data, security is maintained. Where other interests are paramount—patient care, research—the data flows freely without controls.

A health industry representative took issue with the government panelist’s comments about medical students. “I would argue that a medical student should have access to everything that the resident has access to and everything that the attending physician has access to. In fact, the [HIPAA] rule leaves that up in the ether of ambiguity, and it’s a big concern as to the impact of the rule on medical students’ and other health professionals’ education,” this panelist said.

A health law expert sought to lend perspective to the discussion. “First, technology is neither the solution nor the problem; it’s just an interesting by-player in the whole endeavor,” the speaker said. “Let’s recognize that there are technological solutions already that will create a reasonable degree of expectation that security can be maintained. I didn’t say perfect security. I didn’t say absolute security. I didn’t say total security.” In the final analysis, the speaker suggested “all that will be required under HIPAA, all that will be required in most instances under laws generally, is a reasonable set, a reasonable group of measures that provide security.”

Technology is not the issue, the panelist continued. Tracking systems can monitor and retain every computer keystroke. Computers can be locked with hardware or software. “That’s not the problem. The problem is, someone goes to lunch and leaves the computer on, and their password is written on a yellow sticky, and it says ‘password.’” Also, electronic data may be secured, but paper copies—computer printouts and faxes—are not. “The fax room to me is the big area of concern,” the panelist said. Given these realities, “We have to get off this notion of absolute security, absolute protection, absolute privacy, absolute anything. . . . We have to think of privacy and security and technology and in-paper and in-voice as a continuum. Some of us have a little bit more, some of us have a little bit less. If we can frame the debate that way, we’ll have some reasonable solutions,” the panelist said.

“We have to get off this notion of absolute security, absolute protection, absolute privacy, absolute anything. . . . We have to think of privacy and security and technology and in-paper and in-voice as a continuum. Some of us have a little bit more, some of us have a little bit less. If we can frame the debate that way, we’ll have some reasonable solutions.”

— A health law expert
Core Question Three

Implementation Costs and Operational Changes

The moderator directed the panel to a different subtopic, the various costs and operational changes required to comply with federal health privacy protections.

This aspect of the HIPAA regulations “makes physicians the most nervous,” a health industry panelist said. Compliance will be very costly, and in the current environment of government payment cuts and hard bargaining private payors, many physicians will find it difficult to foot the bill for compliance. Beyond the issue of meeting the privacy requirements, this speaker said, physicians are concerned that over time, the task of complying with these regulations—or OSHA requirements or healthcare fraud and abuse guidelines—“is converting a physician who is trained in clinical management and treatment of patients into a manager of process.”

Although they may hire a compliance officer, “ultimately a physician who operates a practice is responsible for everything that goes on.”

A policy analyst reminded the panel that ultimately compliance depends on having a “robust culture of a respect for privacy.” Without that, “none of the technical solutions in the world are going to make a difference.”

The panelist continued, “Given the self-contradictions in our culture [with respect to privacy], it’s very difficult for any of the technical solutions—either the punitive ones or the positive incentives—to inculcate the ethos of ‘respect’ that we want.”

Acknowledging it might sound “wildly naive,” the speaker suggested that part of the answer is “to enable people to do the right thing because it is the right thing.”

Another policy analyst again criticized the industry for not embracing available technology. “Vendors of computer systems for the medical care industry have said for years, ‘We have security solutions; nobody will buy them. Hospitals, whoever, don’t care.’ Maybe they’ll care now,” the panelist said. The same speaker then acknowledged compliance problems and said it would be well if the technical security requirements could be phased in over a longer period. “It’s just unreasonable; it can’t be done,” the panelist said. Audit trails, another highly touted security measure, are also problematic, according to this panelist. “I love audit trails, but I don’t see them as practical.” The reason: such tracking systems create massive amounts of data, and the question is, “What are we going to do with it? No one’s going to look at it,” the speaker said.

Picking up on earlier comments about privacy abuses in the healthcare sector, a health industry panelist said, “Let’s not confuse allegations with actual facts.” Further, even though breaches of privacy have occurred in the healthcare system, “I think what’s remarkable about these examples is that when you consider this industry, and the number of records, and the number of actors, that there isn’t more of this as opposed to being startled that there’s actually some of it.”

“Suppose you’re a hospital that’s working on a small margin anyway. And you go out and you invest a lot of money in security systems and procedures, and then the regulations come out and say, ‘Oh, you’ve got that wrong; you have to go back and retrofit.’ What a terrible business decision. I wouldn’t want to be the CIO in that situation.”

— A health industry panelist

This panelist also challenged allegations that hospitals should have moved more quickly to invest in privacy protection technologies.

“HIPAA’s been looming for a long time, since at least 1996, and before that, the industry was well aware that privacy bills were out there,” the panelist said. “But it would have been a bad business decision, knowing that these laws and regulations were looming out there, to invest an inordinate amount of money in security procedures not knowing what you were going to have to do. Suppose you’re a hospital that’s working on a small margin anyway. And you go out and you invest a lot of money in security systems and procedures, and then the regulations come out and say, ‘Oh, you’ve got that wrong; you have to go back and retrofit.’ What a terrible business decision. I wouldn’t want to be the CIO in that situation.”

Another health industry representative responded to a government panelist’s statement that many health plans have already adopted security technologies because they perceive that health information has value. “The economic value of the information to [insurers] is not that they’re interested in selling it or using it for...
marketing purposes. It’s the fact that if they allow breaches of confidentiality, they’re not aware of any employer that’s going to want to do business with them. It’s the economic value of the good will that’s really most important to them.

A data/technology expert also addressed the “notion of abuse” of privacy in the healthcare industry. The abuses “certainly seem to get far more shocking as you move away from the clinical setting,” the panelist said. “So it’s kind of a funny thing that when we talk about abuses, we always want to run to the Holy Grail of the hospital system, when, in fact, the worst examples are as you start to move outside of the clinical setting.”

The same panelist expressed regret that all too often, “privacy is a pacifier. It’s an add-on after the economic decisions of the various parties have been made.” It’s only because of the Internet and the HIPAA debate, the panelist said, that “privacy has moved into the economic mainstream” because of concerns about the “survivability of the [healthcare] business.”

For the various segments of the healthcare industry, the economic incentives for embracing privacy differ, this panelist suggested. Individual practitioners see privacy as “their individual word of respect to the patient . . . . For the most part, members of various medical [disciplines] who work on an individual level with patients make us all proud of their view of privacy.” For hospitals, “the economic incentive is rooted in costs versus privacy.” Basically, “it’s an add-on,” the panelist said. For research facilities, privacy comes down to “research money versus privacy.” Accordingly, “It’s not surprising that students are freely given the data because the money is behind the research. And if privacy constraints aren’t there, that just translates into research dollars.”

The panelist closed by stressing the need for health data that is “sufficiently anonymized.” “That doesn’t mean it’s useless. It has to fit the [user’s] purpose, but I don’t have to give you more than you need.” It is particularly important that “public-use” data be made sufficiently anonymous, the panelist said. “It’s not acceptable that hospital discharge data from the states, from NCQA, through the CDC, through HCFA, is not sufficiently anonymous. That’s not even a security issue; that’s a privacy issue,” the panelist concluded.

A government panelist mentioned again the need for an underlying culture of privacy. The panelist related how, at a recent conference on privacy, one registrant at his luncheon table, with very little prompting, related “four or five stories of inappropriate disclosures that had happened in her hospital” that were uncovered by the auditing system the hospital had implemented. The panelist observed, “I just wonder if some of these privacy disclosures—if it’s sort of like cockroaches. For every one you see, there are twenty you don’t see.”

The same panelist suggested that as the nation’s widely dispersed healthcare information infrastructure “becomes more and more sophisticated, more and more robust, security issues are going to become more important.” All will be for naught, however, if an underlying culture of privacy is missing.

A health industry panelist addressed a concern of researchers. There are operational costs associated with prospective, randomized, controlled clinical trials. “Imagine if one is trying to get a 100-site study up and running in multiple states, and you’ve got IRBs to attend to, and privacy boards as well, and if you have to alter contracts, alter informed consent, etc., etc.—you can really slow, if not halt, the pace of this kind of research,” the panelist cautioned. “And ultimately what you may find is, you wish you had a therapy that could have benefited 50 percent of patients with breast cancer, and you’re stuck with a therapy that maybe only benefits 25 percent. So please recognize that down the road, there will be other costs society will have to bear.”

With the allotted time for Core Question Three at an end, a data/technology expert closed the discussion by reiterating an earlier point about the shortcomings of hospitals’ information security systems. In terms of “porousness,” or computer systems’ vulnerability to security breaches, “healthcare organizations have some of the worst systems and networks in the world.” The panelist added, however, “Frankly, I don’t think that healthcare organizations are the primary bad actors. I don’t think that providers are. I think that it’s corollary businesses that profit from data warehousing and datamining and who are establishing huge interests in that space that will ultimately reap the biggest economic benefit. I don’t think that real enforcement capability exists to deter or prevent those people from abusing the data that they have access to.”
**Core Question Four**

What Are the Areas of Consensus and Points of Tension in the Debate on Privacy of Health Information?

- On which issues is there clear consensus?
- What are the areas of near-agreement?
- On what issues does strong disagreement remain?

Following reports from the breakout groups (see Appendix A, page 46, “Breakout Sessions Consider Health System Changes, Cyber Issues, and Balancing Protections With Legitimate Use”), the moderators moved the panel through the Colloquium’s final task, identifying points of clear consensus, and “points of tension.” The latter are issues on which there was near-consensus, clear disagreement, or no resolution achieved during the Colloquium.

The discussion began with an assignment in which each panelist wrote down what he or she believed to be the single clearest point of consensus and the main point of tension to emerge during the Colloquium. A moderator called on each panelist in turn and used the resulting suggestions as the basis for the Colloquium’s closing discussion. The following points of consensus and points of tension emerged.

### Points of Consensus

1. **There is a need for transparency, notice, consent, and education.**

   The panelists overwhelmingly agreed that “transparency” in interactions between the healthcare system and consumers with respect to healthcare information is essential to achieving an appropriate balance between protection of health information and the beneficial uses of such information for medical research, payment of medical claims, and so forth. The panel concluded that transparency is closely linked to public education efforts and to the health system’s development of patient consent forms and notices on privacy protection policies and the uses that may be made of patients’ health information.

   Comments that clarified the panel’s thinking on transparency included:

   - The education and awareness we all need (patients, providers, policymakers) is a clearer understanding of how information drives healthcare, plus awareness of the implications when we forego privacy—A Policy Analyst
   - There needs to be education and awareness of rights and responsibilities on the part of providers, patients, and payors about how information drives healthcare and how use of your information can fit within the common good—A Consumer Representative

   - A fair amount of healthcare information should be shared, and this fact should be communicated to the public. There needs to be education on how the healthcare system works—A Government Panelist

   - The importance of transparency is not just for consumer empowerment; it’s also a big driver of institutional change. By having to provide notices, to provide the transparency, institutions need to both understand and be comfortable with their privacy practices—A Healthcare Provider Representative

   - [Transparency] is also educating the policymakers, providers, and the media. With respect to providers, it’s educating them about their responsibility to assure the public about the benefits of using information and that providers are acting responsibly in using the information. With respect to the media, there’s a lot of work for healthcare system to make the case for using information—A Health Industry Representative

   “There needs to be education and awareness of rights and responsibilities on the part of providers, patients, and payors about how information drives healthcare and how use of your information can fit within the common good”
   — A consumer representative
2. Privacy is an important aspect of the healthcare system.

The panel endorsed the basic principle that privacy protection is an essential component of the nation’s evolving healthcare system. The trend toward digital medical records, and the transmission of those records by electronic means, has heightened the importance of privacy protection in the eyes of consumers, policymakers, and the health industry. “Technology is increasingly important to the healthcare system, and therefore privacy is,” a government panelist noted. Another government panelist, however, suggested that despite the attention given to privacy, “there are insufficient market forces in traditional healthcare to provide privacy through competition in the marketplace.” A third panelist expressed her broad view as, “When I go up to about 50,000 feet, I guess what I see is that patient privacy should be provided, and a recognition that there are costs and benefits associated.”

“Technology is increasingly important to the healthcare system, and therefore privacy is.”
— A government panelist

3. There is a need for trust and a recognition of legitimate uses of health information.

The panel agreed that, as one provider panelist expressed it, “There’s a strong value to patient autonomy. When that autonomy needs to be breached, patients need to view the system with trust and legitimacy.”

4. Individually identifiable health information should be protected.

The panel agreed that “individually identifiable health information should be protected,” but only after discussing and rejecting several suggestions to clarify the word “protected.”

As originally offered, the point of consensus stated that “individually identifiable health information should be uniformly protected.” [Emphasis added.] The proposal’s sponsor explained that he intended “uniformly” to mean that all health information should be treated as equally sensitive; there should not be different standards of protection established for information based on its sensitivity. He noted, for example, that even in the sensitive area of psychiatric care, it is not always clear when something is mental health information. Accordingly, policymakers should not create variable standards based on the type of information.

A vigorous discussion followed, and after several panelists raised concerns about other ways in which “uniformly” might be interpreted, this descriptor was deleted. Concerns raised during the discussion included:

I  “Uniformly” could imply identical standards at all levels of government, raising the federal preemption issue on which there clearly was no consensus.

I  The United States already has varying standards in place. Public health data, for example, is exempt from the final HIPAA regulations.

Points of Near Consensus

1. At present, market forces are not sufficient to provide an adequate level of privacy in the traditional healthcare market.

The panel touched on this issue a number of times over the course of the Colloquium, including during the breakout session on the changing healthcare system (see page 46). Among the points raised:

I  Real security and privacy protection is difficult to implement, is costly, but ultimately is beneficial to patients. A government panelist originally offered this as a proposed point of consensus. Several panelists disagreed, asserting that many security systems are readily available and relatively inexpensive.

I  Although hospitals and other providers have adopted computerized systems in many administrative areas, healthcare generally lags behind other industries in management’s use of information technology as a tool for short- or long-term decision-making. Certain factors unique to healthcare contribute to this situation:

I  Cost consciousness in this highly regulated industry makes it difficult to install and update state-of-the-art information technology.

I  Healthcare systems generally have less internal uniformity or integrated management than other industries. There are many key players and a lot of autonomy in individual departments.

I  The sensitive nature of medical information makes healthcare administrators cautious about using patients’
health information as a management tool. However, several panelists noted that healthcare providers have missed opportunities to inform consumers of beneficial uses of health information for cost reduction and improvements in quality of care.

Although hospitals and physicians previously have lacked economic incentives to fully embrace information technologies or to explain to patients the uses of health information, this is changing. The advent of assertive, computer-savvy patients and providers’ recognition of the cost-saving and quality improvement uses of health information will lead to adoption of more sophisticated technologies, and toward the goal of greater transparency in the uses of health information endorsed by the Colloquium panel as its first point of consensus.

Non-institutional areas of the health industry have moved more quickly to adopt the latest technologies and to use them as management tools. However, these strategies have led to criticism about invasions of privacy and the use of personal health information for commercial purposes.

2. There can be legitimate uses of patient information to improve quality, to improve efficiency, and to reduce disparities in healthcare.

A moderator presented this point from an earlier discussion as, “It is appropriate to use information for quality, to improve efficiency, and reduce costs.” Panelists raised concerns about whether there are “uses” or “demands” for health information for quality, efficiency, and cost reduction, and whether such uses should be described as “legitimate.” The panel reformulated the statement as “There can be legitimate uses of patient information to improve quality, to improve efficiency, and to reduce disparities in healthcare,” and adopted it as a point of near consensus.

Points of Tension—Areas of Disagreement

1. Federal Preemption of State Privacy Laws

The panel thoroughly discussed the arguments for and against federal preemption of state privacy laws, but recognized this as a clear area of disagreement.

2. Private Right of Action

Panelists “agreed to disagree” on the question of whether individuals should be allowed to file lawsuits for alleged violations of privacy standards governing their health information.

3. Some participants in the debate are trying to legislate other agendas under the guise of privacy.

The panelist who offered this point stated that there are legislative and regulatory issues that don’t really have anything to do with privacy. She cited the example of HIPAA’s marketing provision, which, she said, allows use of information for marketing unless a third party pays for it. This simple phrase brings into action the 1998 FDA draft guidance on the issue of pharmacy benefits managers being used by manufacturers for certain purposes. The panelist asserted that the fact that there is a money flow involving a third party has nothing to do with privacy. Several other panelists strongly disagreed.

Points of Tension—Unresolved Issues or Concerns

1. There is a lack of coherence between federal and state legislative and regulatory approaches to privacy.

The panelist who offered this point suggested that while data collection by hospitals, pharmacies, and so forth is the focus of the HIPAA debate, public health data such as states’ hospital discharge data, and data collected by HCFA and AHRQ, which is exempt from the federal rules, poses a far greater risk of breaches of privacy.

2. The discussion has not addressed privacy of healthcare information that is used for commercial purposes, particularly the rights of individuals with respect to information used for e-commerce.

The panelist who offered this point noted that a great deal of personal health information is being collected in e-commerce transactions on the Internet, and none of this is covered by the final HIPAA rules. How is the nation going to deal with the rights of individuals with respect to e-commerce? she asked. The panelist concluded, “There are places where healthcare information is being collected . . . and it’s not getting any level of protection, other than the level of protection we’re giving to information we give to L.L. Bean about what color sweater we’d like to buy.” The moderator noted that this panelist’s point was similar to an earlier statement by a government panelist that “this debate is not taking place just within the healthcare community—this is a debate about the
use of personal information throughout our entire society.” The panel did not formally resolve this issue, but noted its importance and the link between concerns about e-commerce and the need for “transparency” in all areas where health information is collected.

3. Why is privacy important to people?

A policy analyst noted, “I’m not sure that we’ve really come to grips with the fundamental value of privacy in this context, of why privacy is a value of importance to people.” Another policy analyst rephrased the issue as, “We didn’t ask what privacy is, as an intrinsic or an instrumental value, and what is we’re talking about protecting.” A government panelist related the issue to consumer choice, asserting that the panel had not talked about the basic choice consumers are going to make—whether to enter the health system, and whether to give full information. Those choices, he noted, are directly dependent on the question of basic values raised by the first panelist.

Although this topic arose several times during the Colloquium, it remained unresolved. Defining the “fundamental value of privacy” hinges on determining the appropriate balance of privacy protection versus legitimate use—a hoped-for outcome identified by a number of panelists at the start of the Colloquium. The panelist who, near the end of the Colloquium, raised the concern about the “fundamental value of privacy” provided a signal that this question would not be easily settled. In explaining his concern, he said, “I don’t mean to suggest that there is one reason [or definition] that we should all agree upon, because I’m sure we would not agree on what that reason is.”

4. Is privacy a right or commodity? Who owns the rights to the commodity? What is ethical behavior in this context?

The government panelist who raised this issue suggested that in the United States “we tend to think of privacy as a commodity that people have rights to, and buy and sell it accordingly. So the questions are, who has the commodity right, that is, the ability to license others to use the personal health information, how should these rights and uses be protected, and what is ethical behavior when using this data?” Another panelist strongly objected to the concept of “commodification of privacy,” asserting, “No, we don’t commodify rights that we have. That’s the wrong way to look at this issue.”

5. Other Unresolved Issues

Over the one-and-one-half days of the Colloquium, panelists raised a number of other issues or offered observations that were not separately considered or resolved. These included:

- I see a lack of accountability. I don’t mean that in the sense of a private right of action; I mean a lack of responsibility, on the part of people in the healthcare system, to accept the burden of trying to do something about privacy
  — A Policy Analyst
- Who decides the rules of use?
  — A Health Industry Representative
- There is no single decider. We’ve had proposals that the individual decide, that the providers decide, that the Secretary decides, that the community decides. I would like to suggest that because there are multiple uses, and multiple inappropriate harms that can come from the uses of the data, that we have an entire array of deciders.
  — A Government Panelist
- There are costs and benefits but who’s going to bear the cost? Who’s going to give up the money and the power?
  — A Technology Expert
- One point of tension is the link between money as profits to a secondary user, and responsibilities to tie use of information back to the healthcare system.
  — A Policy Analyst
- A major point of tension is—who decides how much privacy protection is enough?
  — A Health Industry Panelist
- A point of tension is the level of value attached to different end users, what the needs and values are that are high enough to overcome patient autonomy.
  — A Health Industry Panelist
- There’s disagreement about the degree to which the community should dictate decisions for healthcare institutions and others about how to operationalize a set of privacy principles, and whether

“A major point of tension is—who decides how much privacy protection is enough?”

— A health industry panelist
there’s a role for market forces in assuring an acceptable degree of privacy.—A Health Industry Representative

- There is tension about what constitutes de-identified information, and when in the continuum you use any type or piece of information.—A Health Industry Panelist

- There is tension about the intersection between privacy and discrimination—whether or not privacy rules can be used to protect people from discrimination.—A Consumer Representative

- We agreed that people should be educated, but there’s no real consensus on how much the patient really needs to know.—A Government Representative

- There’s tension in the extent to which we will let transparency and notice take the place of all the other fair information practices.—A Government Panelist

- There’s a tension between the commercial use of data and the possibility that some commercial use could improve healthcare.—A Data/Technology Expert

Suggestions for Policymakers

Noting the presence of several government representatives on the panel, a moderator suggested using the Colloquium’s closing minutes as an opportunity for the government panelists to seek input on policy issues they would be wrestling with in refining the HIPAA privacy rules or addressing other privacy initiatives. Highlights of that discussion included:

- “There’s tension on ‘everything else.’ Once you get below 40,000 feet, the details become very complicated.”—A consumer representative

- One government representative said that, on the whole, “I’m amazed that I haven’t seen an awful lot that I would change in the privacy rule.” Pointing to the lack of consensus on many issues, this panelist said, “You know, you change it one way, you’re not going to make any more people happy than if you change it the other way.”—A Health Industry Panelist

- Another government representative welcomed the opportunity the Colloquium provided to discuss privacy with all the major constituencies. His major question was, “Do we have to start over? Is it so bad? I’ve heard some say that.”—A Government Panelist

“Everyone agrees we should have notice, but how much choice should an individual consumer have?—A Government Panelist

- There is tension on the question of who chooses and how much choice, but also on how you implement that system.—A Government Panelist

- “We can’t let the perfect be the enemy of the good. So, what do we move forward with?”—A government panelist

Or, on the other extreme, don’t change anything, go forward with it as is. But are the issues that have been raised fixable in the regulatory process? And if they’re not, then what other options would people see are viable in our current environment?” He acknowledged that government would never issue a perfect rule on privacy, but concluded, “We can’t let the perfect be the enemy of the good. So, what do we move forward with?”

Input from health industry representatives and other panelists included:

- Because HIPAA does not provide for federal preemption, regulators need to recognize that states will be enacting privacy laws. Rather than micromanage with a lot of definitions designed to address the myriad situations that can occur, federal regulators should consider crafting a rule that allows states to innovate while still meeting a minimum federal protection standard.—A Health Industry Panelist

- A federal rule is needed, but deficiencies in the statutory authorization have led to the problems many people see with the HIPAA rule. So federal officials should “write a proper law.”—A Health Industry Panelist

- A policy analyst disagreed with the suggestion for broad statutory guidance. “If you write something that’s more general, every lawyer in every healthcare company then comes in and says, ‘What about this circumstance?’”

The major
problem is that “there is no consensus about what to do, below the level of ‘privacy is important.’ After that every detail is fought over.”

- A health industry panelist sought clarification on how the government would oversee organizations’ postings of their privacy policies on the Internet. A government official explained that enforcement of HIPAA-related matters on the Internet would be coordinated between the relevant agencies. He noted that a lot of privacy policies on the Internet today “aren’t very good.” They promise to protect users’ information in the first paragraph but then claim the right to use the information in the last paragraph. Implementation of the HIPAA rule the official said, “will make a real contribution to trying to work out, ‘What’s a good privacy policy.’”

- Replying to a government official’s question about how to fix the HIPAA rule, a consumer representative noted that issues that are outside HHS’ jurisdiction would have to be handled by Congress. With respect to the rule itself, this panelist characterized some of the health industry’s criticisms as “hysterical in tone and not really based on a reasoned reading of the actual regulation.” To the extent serious problems exist, they can be addressed through HIPAA, which gives the Secretary authority to make modifications needed to achieve compliance. A health industry panelist took exception to this panelist’s use of “hysterical” and suggested the underlying tone of privacy advocates’ concern was “paranoia.”

- A government representative said a “weak link” in HIPAA is that the rule allows to stand only state laws that are more stringent than federal standards. It will require many states to revise their laws to ensure that they are “more stringent,” not just “equal to or as protective” as the federal standards. The current rule also raises enforcement concerns because enforcement falls to the federal government when states’ laws are preempted, and “we don’t believe there are enough federal enforcers to do that job,” the panelist concluded.

- A technology expert asserted that while the debate has focused on “abuse” of privacy, the real issue is “risk.” A lot of emphasis is placed on protecting information in hospitals, but the risk actually increases the farther one moves from the hospital setting. The greatest risk for breaches of privacy comes with public use data—state discharge data collections and other data collected by public agencies—which is exempt from HIPAA.

- A health industry panelist suggested that a major improvement to the rule would be the establishment of a general rule with detailed safe harbors that meet the standard.

- Another health industry representative endorsed the suggestion for safe harbors and suggested that, for this subject, HHS’ approach on HIPAA “. . . wasn’t the best model of rulemaking.” The panelist suggested that HHS look at innovative approaches used by other agencies, citing the Federal Trade Commission’s development of rules to implement the Children’s Online Privacy Protection Act. With that rule, the panelist said, “when [the FTC] encountered a very thorny, unexpected issue, they had a day-long workshop.”

A government official had the final word. This panelist thanked the other participants for their input and stressed that rulemaking is an iterative process. States that have implemented privacy rules, the official noted, learned that “there were a number of unintended consequences that were not seen until the rule actually hit the ground.” Federal regulators expected to have a similar experience. The key need is for “consensus standards.” Development of such standards is in a “toddler stage,” the official said, but, with all the affected groups continuing to participate in the debate, consensus standards for privacy of health information will become a reality.

**Adjournment**

Health Lawyers’ principal moderator sincerely thanked the expert panel for their participation in the Colloquium and assured them that their discussions would provide the basis for a Colloquium Report that would be a valuable asset for policymakers and others as the debate on privacy of health information evolves. The moderator formally adjourned the 2001 Public Interest Colloquium, *Privacy of Health Information.*
Appendix A

Breakout Sessions Consider Health System Changes, Cyber Issues, and Balancing Protections with Legitimate Use

Towards the end of the first day, the chief moderator divided the panel into three broadly representative groups for two-hour, focused discussions of the following topics:

- Privacy protection in an evolving healthcare system
- Cyberworld: privacy protection in the digital age
- Balancing protection with legitimate uses of health information

When the Colloquium reconvened the following morning, a representative from each breakout group reported back to the full panel.

Privacy Protection in an Evolving Healthcare System

The spokesperson for this breakout session said his group focused on technology as the force that will drive health system changes and the industry’s response to the call for improved privacy protection. The group recognized that technological innovations are inevitable and often beneficial. At the same time, the advent of increasingly sophisticated technology, and its use throughout society, may be making privacy illusory. In terms of health information, a key question is, “Can we disclose data for appropriate uses today, such as for public health [goals], and still protect privacy?”

The healthcare system is in a “catch-up” position with respect to both technology and public education, the group concluded.

Healthcare has been slow to adopt the latest information technologies, in part because “economic incentives have not existed,” the spokesperson reported. At the same time, the industry has “not done a very good job of informing patients about how their data is being used.” There is a growing awareness that “we have a complex and constantly evolving health care system, and so as a result, our privacy safeguards have to match that complexity.” The long-term effect of complex technology on some parts of the healthcare system as a whole is unknown, however. “Will small providers be able to keep up with our evolving healthcare system—including all the privacy rules—and still survive?” the spokesperson asked.

The group concluded its session by trying to identify trends or forces that are shaping healthcare privacy and technology, the spokesperson said. These trends include:

The Economy: A potential economic downturn and ongoing concerns over rising healthcare costs are important factors, but their impact is unclear. Will concerns over costs lead to an investment in technology as a way to boost productivity? Or will a slower economy make it harder to spend the money for new technology?

Federal Reserve Board chair Alan Greenspan has credited much of the economic boom of the 1990s to increased productivity brought about by technological innovations. Healthcare did not share in this trend, but some observers believe this industry will be the next economic sector where technology will drive gains in productivity. However, the industry’s long-standing resistance to change may have a dampening effect, the spokesperson noted.

Growing Interest in Privacy Protection: Largely because of the Internet, breaches of privacy, including breaches in the confidentiality of health information, are a matter of growing concern to many Americans. The public expects the healthcare industry to adopt technology systems and initiate management controls to protect the privacy of patients’ medical information. Many uses of information are appropriate and beneficial, however, and the healthcare industry needs to do a better job of public education on what uses may be made of a
person's medical information. A major challenge (and opportunity) for the healthcare industry, the spokesperson said, is to develop privacy "notices" that inform patients in an open and straightforward manner about the ways in which their medical information may be used.

**Cyberworld: Privacy Protection in the Digital Age**

This breakout session focused on the intersection of healthcare and health information with the Internet. The spokesperson said the group began by "looking at what's available on the Internet today, from a health information or health services point of view." Then, the group's task would be to consider "what's needed to protect health information on the Internet."

In terms of "what's available," the group identified:

- Health information sites;
- Health advice sites;
- Internet extensions of physician group practices or hospital systems (which allow patients to communicate with their provider by e-mail);
- Online patient databases;
- Prescription drug-related sites; and
- Telemedicine, which allows a physician, either directly or via consultation with a distant physician, to provide services to or consultative advice for the benefit of a patient located at some distance from the physician.

The group touched briefly on two developments that have raised privacy concerns in some quarters, the spokesperson said. Telemonitoring of patients in their homes raises "Big Brother" concerns that a broad range of individual behavior, largely unconnected with a patient's medical condition, might be gathered for later use.

The Outcome and Assessment Information Set (OASIS), a standardized form that HHS requires home health agencies to use to measure quality and patient satisfaction, has generated concerns for two reasons. The form gathers information on topics, such as living arrangements, that are not directly related to patient care. Security and de-identification are also concerns since home agencies transmit the OASIS form electronically to the Health Care Financing Administration (HCFA) and to state Medicaid agencies.

Government officials have assured Congress that HCFA has implemented procedures to de-identify OASIS data and to ensure security through encryption and by requiring authorized users to enter passwords at several checkpoints.

Concluding that the Internet does, indeed, contain a broad range of health information and services, the group sought to relate this phenomenon to the privacy debate, the spokesperson said. A threshold concern, which may relate more to quality than privacy, is that, "there's no vetting of the accuracy of the [health] information on the Internet." The situation is "very much caveat emptor," as one participant expressed it. The group shied away from any suggestion of censorship, but wondered if steps might be taken "to allow the consumer to have a little more knowledge about what is available, and what it means, if it's out there on the 'Net,"" the spokesperson said.

Turning to a concern directly related to privacy, the group recognized that "it's not clear what actually happens to the data that's collected," the spokesperson said. This is true of all information collected on the Internet, but it is clearly important to the Colloquium's focus on health information privacy. Of particular concern is the phenomenon of "health information leaking into other places" or the reality that personal information that a visitor provides on an Internet site, or the pattern of sites that a person visits, may be analyzed and used by advertisers or site sponsors to market products or services to the Internet visitor's perceived "needs."

Occasionally, such information may be used for malicious or discriminatory purposes. One of the breakout participants related a story of a Canadian who took a new job in the United States and, in the course of enrolling for the employer's health plan, signed a form certifying that he had no preexisting medical conditions. Within a short time the man was diagnosed with cancer. The health insurer was able to determine that the employee had ordered a book on cancer from an online bookstore and used this to argue that the employee already knew that he had cancer when he certified that he had no preexisting conditions.

Despite concerns about privacy and commercial health sites on the Internet, cyberfirms actually have done a better record of protecting individual data than have many healthcare institutions, one breakout participant suggested. For one thing, their technology is superior to the older "legacy" computer technology many health systems have invested in. Also, commercial Internet sites have economic incentives to protect the data they gather on visitors to their site. They want to prevent competitors from gaining access to their user database, and they want consumers to feel confident about providing data when they visit the firm's site. As an example of cyberfirms reacting swiftly
Appendix A

to an economic incentive, the spokesperson cited “dot.com” companies’ rapid development of software to allow secure use of credit cards in e-commerce.

Although security measures may be put in place to de-identify data and forestall unwarranted disclosures, the question, “Who decides how to treat an individual’s information?” remains the major privacy issue in cyberspace and elsewhere, the spokesperson said. That consideration led the breakout group to its final topic, a discussion of privacy policies, the covenants posted by Internet sites that tell visitors how the information they provide will (or will not) be protected—or used by the site sponsor or anyone else. As the spokesperson expressed it, “It’s about notice. What is it you’re collecting, what will you use it for, and where else might you send that information?”

The group identified three major issues in its discussion of privacy policies or privacy “notices”:

- The quality of privacy notices on the Internet;
- Technical innovations that would improve consumers’ understanding of privacy policies and enable them to play a more active role in controlling a site’s use of their data; and
- The need for more public education so that consumers have a better understanding of how information flows and is controlled on the Internet.

With respect to the quality of privacy notices, the group noted that newer sites generally post a privacy notice; many older Web sites don’t even have one. How “good” such notices are may be a question of how quality is defined, however. Many sites have extensive information about privacy, but it’s lengthy “and you can’t wade through it and pick out the important information. They’ve got it all; it’s just not always intelligible,” the spokesperson said.

That observation led to discussion of a related question, “Is there a way to hard-wire a user’s privacy preferences as he or she ‘surfs’ the Internet? In other words, can software be developed that would empower consumers as they interact with Web sites, perhaps automatically supplying personal information to sites that meet pre-established criteria while denying certain information to, or bypassing altogether, Web sites that don’t meet the consumer’s privacy preferences? The group was pleased to learn that software already is available that, to one degree or another, empowers consumers in that fashion. Given the economic incentives for cyberfirms to protect privacy, new or improved tools will be developed over time, one of the group’s participants suggested.

In view of the growing use of the Internet, and the need to boost public confidence with respect to privacy, the group considered suggestions for “baseline regulations” on Internet privacy or the establishment of privacy standards by accrediting organizations. Compliance with the standards would earn a site a “seal of approval” that would encourage consumers to visit the site and share their information. The spokesperson was quick to add that the group did not reach consensus on those proposals.

That discussion led to recognition of an information vacuum identified by a number of speakers during the course of the Colloquium—the need for public education. Whether consumers are reviewing privacy notices or interacting in Web “chat rooms,” the spokesperson reported, “The major issue we identified is that people don’t understand the accuracy—or inaccuracy—of information on the Internet, and they don’t understand what the Internet can do [with information]; they don’t understand ‘cookies,’ or ‘double-clicks.’” [Web “banner” advertisements that gather information about consumers who “double-click” to review the ad in more detail].

Balancing Protection with Legitimate Uses of Health Information

The spokesperson for the third breakout session reported that her group began with the question, “Who determines the balance between protection and legitimate use?” The group concluded that, as a general rule, the patient determines the balance. However, there are a variety of potential uses of a person’s health information that affect other segments of society, and “by affecting others,” the use of health information becomes a continuum. “There’s the patient care itself, and then as you move along the continuum, issues arise such as quality assurance, research, and then all the way at the end is public health, for example, you know, the person out there who’s infecting everybody with the Ebola virus.” (See Exhibit A, “Balancing Privacy Protection with Legitimate Use.”) Thus, while the patient is the fundamental determiner or balancer, there are public health issues at the other end of the continuum where there is a “greater good” than total privacy. “And so while there is control, which the patient exercises, there is a point where a public health concern may trump the patient,” the spokesperson said.
The group debated where quality assurance (QA) should fall on the continuum, the spokesperson said. In one sense, QA looks backward toward the quality of care that was rendered. In another sense, QA can be viewed as looking forward toward ways to improve care in the future. Research, by contrast, clearly focuses on the future, “looking at the greater good far out in the future,” the spokesperson said.

The spokesperson elaborated on the discussion of decision-makers, noting that the group did not resolve this issue. Although the patient decides how much information a provider can use, “in many cases, the decision-maker is the provider/government.” After further discussion the group concluded that the ideal approach would be to base legitimate uses on “community standards” that were developed by citizens’ groups that include “all the stakeholders,” such as patient advocacy groups, providers, researchers, institutional review boards, government, and so forth. “By the way, community standards can also be law—recognizing that law can be based on input from all the stakeholders,” the spokesperson said.

The group concluded that for two uses, QA and research, “there are issues of cost and risk and benefit that have to be evaluated.” In a peer review setting, for example, “do the doctors sitting around the table have to have the name and address of the patient whose care is being discussed?” Or, with respect to research, “How many elements of data are necessary to be able to do research in a way that doesn’t compromise the research itself?” the spokesperson asked.

Since decisions further along the continuum erode patient autonomy, “we need to make it up to the patient by ‘transparent’ behavior—meaning giving notice,” the spokesperson said. That is, the patient would be informed about QA, research, and other beneficial uses of health information. The corollary of notice is public education, a theme raised a number of times during the Colloquium.

Finally, the group tackled the difficult issue of commercial use of health information. Although participants recognized that the potential commercial use of data lies in the background at every point along the continuum, the group did not develop any recommendations for identifying acceptable or inappropriate commercial uses of health information. The group concluded that “what makes commercial use such a hot button is that there is ‘piracy,’” which the spokesperson explained meant ‘bad actors’ or ‘bad behavior’ in the use of individually identifiable health information to make money. “The existence of piracy requires law, with law being what the community has decided should be the standard for how that information should be used,” the spokesperson said. One fundamental question the group did not address was, “Does making money in the process [of using health information] automatically constitute an illegitimate use?” the spokesperson concluded.
Appendix B  Highlights of the Final HIPAA Privacy Regulations

Background
Before enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), there was no comprehensive federal law that protected the confidentiality of individually identifiable health information. Rather, a handful of federal statutes and regulations protected (i) the medical records of human subjects who participated in clinical trials, (ii) the disclosure of personal information contained in records that are maintained by federal agencies or contractors, and (iii) an individual’s substance abuse and treatment records. An individual’s general health information, like his or her medical record, insurance coverage, or financial account balances, was protected by state law, but only if a state law existed. Under HIPAA, Congress gave itself three years to pass a privacy law to protect health information. HIPAA provided that if Congress did not enact a law within that timeframe, the Department of Health and Human Services (HHS) should proceed to establish privacy standards by regulation. Congress failed to meet its self-imposed deadline, and, on November 3, 1999, HHS published proposed regulations in the Federal Register.

The proposed regulations proved controversial, attracting more than 52,000 public comments. HHS analyzed the comments, accepted some suggested changes, rejected others, and, on December 28, 2000, published final regulations. In response to protests from the healthcare industry, HHS re-opened the final regulations for an additional 30-day comment period. Contrary to industry expectations, HHS Secretary Tommy Thompson announced that the rules would become effective as published. Acknowledging industry’s continued concerns, the Secretary promised that HHS would issue extensive guidance to help covered entities comply with the requirements. The final rules became effective April 14, 2001, meaning that all healthcare organizations covered by the regulations are required to be in compliance no later than April 14, 2003. Small health plans have until April 14, 2004.

The final HIPAA privacy regulations require “covered entities” to protect all “individually identifiable health information” that is in their possession. Under the regulations, “covered entities” include health plans, health care clearinghouses, and health care providers that transmit any health information in one of nine defined HIPAA transactions: electronic claims, remittance advice, enrollment or disenrollment, eligibility for a health plan, referral certification and authorization, claims status inquiry and response, or premium payment.

The privacy regulations protect “individually identifiable health information,” (IIHI), which is very broadly defined to include past, present, or future health information, regardless of whether it is oral or electronic, whether it is or has been used to describe the individual’s treatment, or whether it did or does apply to the payment for the treatment rendered to the individual. This all-encompassing definition includes significantly more information than would be found in what is traditionally viewed as an individual “medical record.” However, if there is no way to determine the individual from the health information (that is, if the health information has been de-identified), then the health information is not protected.

As a general rule, the final HIPAA privacy regulations provide that covered entities may not use or disclose an individual’s protected health information without first obtaining the individual’s consent or authorization, as appropriate, or unless there is some exception within the final HIPAA privacy regulations or in another law, not preempted by HIPAA, that allows such use or disclosure. Although this general rule appears relatively straightforward, and is indistinguishable from what people have come to expect in their encounters with the healthcare system, the final HIPAA regulations pose a significant compliance challenge for covered healthcare organizations.

Highlights of major provisions of the final regulations are presented below. The summary describes several of the most hotly-debated issues, lists and discusses the impact of proposed-rule provisions that were significantly revised in the final regulations, and concludes with a summary of important provisions that are new to the final regulations (see table on pages 51-52), or that did not change from the version in the proposed rule.

The Most Controversial Provisions

Consents
The proposed regulations allowed covered entities to use or disclose IIHI for purposes of treatment, payment, or healthcare operations without first obtaining the individual’s consent. The final HIPAA privacy regulations, however, require health care providers to obtain a written consent from the individual that meets the requirements of the regulations before using or disclosing the individual’s health information for the purposes of treatment, payment, or healthcare operations. Neither health plans nor healthcare clearing-
houses are required to obtain the individual’s consent, although they may. Further, health care providers are allowed to condition treatment on the receipt of the individual’s consent, and health plans, if they obtain consents, are allowed to condition underwriting on their receiving consents from their members.

State Law Preemption

Federal preemption of state privacy laws is one of the most controversial issues in the debate on health information privacy. Supporters of preemption say there should be one national law that establishes privacy standards. Requiring national or regional healthcare entities to comply with a plethora of state privacy requirements, they argue, is both inefficient and costly. Opponents of federal preemption, including state governments and many consumer advocates, argue that where states have established privacy standards that are stricter than federal requirements, state laws should take precedence. Under the final HIPAA privacy regulations (and under HIPAA), a state law will be preempted if it is directly contrary to the regulations, that is, it would be impossible for an entity to comply with both the state law and HIPAA at the same time. Where the state law is contrary to HIPAA but is more stringent than HIPAA, or where the state law offers the individual greater rights as regards his or her information, the state law will prevail. In contrast to the proposed regulations, under the final rules healthcare organizations may not seek an advisory opinion from HHS to determine whether the state law will be preempted. Instead, the final regulations describe how to submit an “exception determination” to HHS for it to determine whether the state law will be preempted—a

<table>
<thead>
<tr>
<th>Provision</th>
<th>Proposed Regulations</th>
<th>Final Regulations</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope of Protection</strong></td>
<td>Protected health information that is or has been transmitted electronically in a HIPAA-related transaction.</td>
<td>Protects all health information, regardless of its form, how it is stored, or whether it is or has been communicated electronically.</td>
<td>While this is an important change, the administrative burden on covered entities is expected to decrease. No longer will the covered entity have to scrutinize each piece of paper or document in an individual’s file to determine whether all, some, or none of the health information on the document is protected. Covered entities will, however, need to define their “designated record sets,” the term HHS has chosen to mean the group or groups of an individual’s PHI that he or she may access.</td>
</tr>
<tr>
<td><strong>Business Associates</strong></td>
<td>Used the term “Business Partner.”</td>
<td>Uses the term “Business Associate.”</td>
<td>A Business Associate is an individual or entity that receives PHI from the covered entity during its services to the covered entity or in performance of its services on behalf of the covered entity. HHS extended the sphere of privacy protection to individuals and entities that do not meet the definition of “covered entity” because many non covered entities may still be able to access or receive PHI from the covered entity to or for which they provide services. Because of statutory limitations, HHS could not extend the sphere of privacy protection to non-covered entities. It could only require that covered entities have Business Associate Contracts with these non-covered entities (if appropriate) before disclosing PHI.</td>
</tr>
</tbody>
</table>
# Provisions that Changed Significantly in the Final Regulations

<table>
<thead>
<tr>
<th>Provision</th>
<th>Proposed Regulations</th>
<th>Final Regulations</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Associate Contracts</strong></td>
<td>Required that numerous provisions be included in the contract between the covered entity and its Business Partner. Also, required the individual who is the subject of the information to be named as a third party beneficiary and required the covered entity to monitor its Business Partner's compliance with the regulations.</td>
<td>No change in the number of provisions that must be included in the contract between the covered entity and its Business Associate. However, individuals need not be designated as intended third party beneficiaries to the contract, nor is the covered entity required to monitor its Business Associate's compliance with the regulations.</td>
<td>Although there will be new and different contracts to draft as a result of the final regulations, the changes made to the proposed regulations and incorporated into the final rule significantly reduce the administrative burden for covered entities.</td>
</tr>
<tr>
<td><strong>Fundraising</strong></td>
<td>Did not allow IIHI to be used or disclosed for fundraising purposes without first obtaining the individual's written authorization.</td>
<td>A covered entity need not obtain the individual's authorization to disclose his or her demographic information or the dates that the individual received healthcare services to its foundation for purposes of fundraising. The covered entity would need to obtain the individual's authorization in order to disclose more of the individual's protected health information.</td>
<td>No significant changes to a covered entity's current fundraising activities and efforts will be required.</td>
</tr>
<tr>
<td><strong>Marketing</strong></td>
<td>Did not allow IIHI to be used or disclosed for marketing purposes without first obtaining the individual's written authorization.</td>
<td>A covered entity need not obtain the individual's authorization to make a marketing communication to him or her so long as the marketing communication: (1) occurs in a face-to-face encounter with the individual; (2) concerns products or services of nominal value; or (3) concerns the health-related products and services of the health care provider or of a third party.</td>
<td>The marketing communication must include all the requisite requirements specified in the final HIPAA privacy regulations or the individual will first have to authorize the use of his or her health information. However, an individual retains the right to opt out of receiving any future marketing communications.</td>
</tr>
<tr>
<td><strong>Governmental Databases</strong></td>
<td>IIHI <strong>can</strong> be disclosed to the government for purposes of maintaining a governmental database without first obtaining the individual's written authorization.</td>
<td>IIHI <strong>cannot</strong> be disclosed to the government for purposes of maintaining a governmental database without first obtaining the individual's written authorization.</td>
<td>Many states collect IIHI from healthcare facilities within the state for purposes of informing consumers about healthcare costs, treatment outcomes, and healthcare facilities' performance. Some states have laws that require healthcare facilities in the state to submit IIHI in order for the state to abstract specific data. These laws may also specify the format in which IIHI must be submitted. Other states, however, do not have such laws. Without a specific state law to govern the submission, an individual's authorization for the release of his or her protected health information would be needed before such information could be submitted to the state.</td>
</tr>
</tbody>
</table>
process that may impose a substantial burden on the state wishing to protect its laws from HIPAA preemption. (For more information, see “State Healthcare Privacy Laws” on page 59.)

Access for Law Enforcement Purposes

Under the final HIPAA privacy regulations, a covered entity is permitted to release an individual's protected health information to law enforcement officials without informing the individual that a request for his or her information has been made, telling the individual why such a request was made, or giving the individual the opportunity to agree or refuse to authorize the disclosure of his or her health information to the law enforcement official.

Major Provisions that Did Not Change or Are New to the Final Regulations

Minimum Necessary Standard

Requests for and disclosures of protected health information must meet the “minimum necessary” standard unless the request or disclosure is related to the individual’s treatment. Essentially, a covered entity that requests protected health information is required to request only the minimum amount necessary to meet the stated purpose for the request. Similarly, a covered entity that discloses protected health information must be sure the information disclosed is the minimum amount necessary to meet the stated purpose of the request.

Individual Rights

Several of the individual rights that were defined in the proposed regulations were included in the final HIPAA privacy regulations with no major changes:

The individual has the right to receive a full and complete accounting of all disclosures made of his or her health information except those made for treatment, payment, or healthcare operations purposes. If, for example, the covered entity gives a copy of the individual's health information to a physician who is not treating the individual but instead is conducting research on anyone who has received a particular procedure, the covered entity must keep track of that disclosure. Specifically, covered entities must be able to provide an individual who requests an accounting of disclosures with the following information: who requested their information, why it was requested, what information was disclosed, to whom it was disclosed, and when it was disclosed. While this requirement will be easier for health care providers to implement than it will be for health plans (because much of the individual's health information is stored within the individual’s “medical record” at a health care provider), most, if not all health care providers will have some work to do.

There are numerous other locations within a health care provider's organization in which IIHI will be found, and these locations must also be considered and information from them included with the health care provider's response. More importantly, health plans with relatively decentralized operations, especially those plans that have geographically separate and distinct facilities or operations, will find maintaining a central “file” on each of their members a significant operational change. Each of the covered entities, however, must consider how it will best control the disclosure of individuals’ health information if there are or could be multiple entry points of entry for an individual's information request.

The individual has the right to access and/or copy his or her health information.

The individual also has the right to request an amendment of his or her health information. If the individual's request is granted, the covered entity must amend the health information. If the request for amendment is denied, however, the individual not only is entitled to receive written notice of the denial and an explanation of the reasons for it, but also is afforded a right of appeal. All related documentation must be maintained as part of the individual's health information for a minimum of six years, and must be forwarded with the rest of the individual's health information in response to any subsequent requests for it.

The individual has the right to receive a Notice of Privacy Practices (called a Notice of Information Practices in the proposed regulations) from the covered entity. This notice must describe the individual's rights as regards his
or her protected health information, how the covered entity does and will use and disclose the individual’s protected health information, and the person the individual may contact at the covered entity with questions about the Notice or in case of a problem with the use or disclosure of the individual’s health information.

**Written Authorization**

Unless otherwise permitted under the regulations, a covered entity may not disclose an individual’s confidential health information for reasons other than those associated with the individual’s treatment, payment for health services rendered, or operations of the covered entity without first obtaining the individual’s written authorization. Covered entities that maintain “family accounts” or that allow a subscriber to review the health information of the subscriber’s covered dependents will need to re-examine their policies, procedures, and practices to ensure compliance with the final HIPAA privacy regulation.

**Administrative Requirements**

In addition to designating a Privacy Official to oversee the organization’s treatment of health information, a covered entity must also designate a contact individual who can provide further information about the covered entity’s Notice of Privacy Practices and who is responsible for receiving complaints from individuals about the ways in which the covered entity uses or discloses their protected health information. Other administrative requirements include conducting workforce training classes, implementing privacy safeguards, and creating, implementing, and enforcing numerous standard privacy policies and procedures.

**Documentation Requirements**

Consents, authorizations, accountings for disclosures, and all other privacy-related documentation must be maintained, tracked, and accessible for a minimum of six years.

**Organizational Structures**

The final HIPAA privacy regulations defined several different organizational structures, most likely to accommodate affiliated covered entities, organizations that have multiple covered entities of a single type, organizations that include more than one type of covered entity, and organizations where a single department or a separate entity within the organization functions as a covered entity. Health plan sponsors, organized health care arrangements, affiliated covered entities, and hybrid entities are all specially recognized in the final regulations. Depending upon the category they fall into, these covered entities may have more or fewer responsibilities under the final regulations regarding the IIHI in their possession.
Appendix C  What Is Health Information?

The capabilities of information systems have exploded over the past decade. Where huge computers once were the norm for large American businesses, faster and more capable desktop and laptop computers now reign supreme. Americans exchange information across both wired and wireless networks, including through the Internet. The ultimate goal: access to and availability of any data at any time by anyone. As the ability to share and store information has grown, so, too, has the individual’s concern for privacy. Nowhere is that concern more evident than in the sensitive area of health information.

Despite advances in electronic storage, much of the information that physicians and other healthcare providers collect from patients is stored on paper. Whether stored electronically, on paper, or using both media, an individual’s health information is shared within a healthcare organization primarily for purposes of providing treatment to the individual or to obtain payment for the healthcare services provided. Some personal information may move outside the original setting, however, and may come back to the individual through unexpected and unfamiliar sources such as mailing lists at healthcare and non-healthcare related organizations; notations about disabilities or prescription information in personnel files; credit card invitations and opportunities; coupons for products; and notices of research projects that promise better health or longer life.

What types of personal information, if any, does the healthcare industry consider confidential? In what form or forms does the information exist? Who uses the information, and why is it used in a particular way? This article discusses personal information in the healthcare industry, and the realities of whether personal information can ever be expected to be kept completely private.

Personal Information in the Healthcare Industry

There are many pieces of information about an individual—financial, health-related, and personal—about which he or she has an expectation of privacy. Until recently, many Americans believed that their personal health information was stored on paper, with some financially-related information stored electronically. Enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) focused public attention on personal information in the healthcare industry, defining the term for the first time and establishing federal standards designed to protect the privacy of that information.

Under HIPAA, “health information” is defined broadly and includes all information related to an individual’s physical or mental condition (a.k.a., clinical information) as well as that related to payment for health services provided to the individual (a.k.a., financial information). In addition to clinical and financial information, the final HIPAA privacy regulations list and include other pieces of information about the individual (such as the individual’s driver’s license number and e-mail address) that many people would not necessarily consider “health information.” Further, regardless of whether the individual’s information is oral or “recorded,” HIPAA protects it if the information does or can be used, by itself, or in combination with other pieces of the individual’s information, to identify the individual. An individual’s health information, therefore, can be found in all sorts of places in a healthcare organization—not just in one single paper file in one specific location. The individual’s medical record, an enrollment application for insurance coverage that is signed by the person applying for coverage, a pre-admissions form that is completed prior to an inpatient hospital admission, the individual’s health insurance card—all are examples of “health information.”

Health Information Is Found in Many Forms and Places

Clinical information is the term the healthcare industry uses to describe information that relates to an individual’s physical or mental condition. Clinical information about an individual historically has been stored in a single file—traditionally referred to as a “medical record.” However, not all the clinical information about an individual is stored in a single medical record, and some information that winds up in the medical record may be only tangentially related to the individual’s treatment or condition.

While many healthcare organizations have automated some portions of the medical record so that they are accessible electronically, medical records still are primarily stored as paper files. Included in an individual’s medical record are such documents as admissions or registration face sheets, consent forms, physician’s orders for tests to be performed on the individual (and the results or reports of such tests), and progress notes about the individual written by any number and types of caregivers. Other pieces of information that relate to the individual’s condition or treatment, such as x-ray films, tissues or fluid samples taken
from the individual (usually for conducting medical tests), and video recordings or tracings, are unquestionably “health information,” but are not in a paper form. Because they are not stored on paper, and for other administrative reasons, these types of information often are stored outside the individual’s medical record. Occasionally, they may be found outside the facility in which the individual’s medical record is located.

Similarly, there are items that are not directly related to the individual’s treatment or condition, but which may be found in the individual’s medical record merely because they are stored on paper. Examples include (i) letters from the individual to the organization thanking the nursing staff for the excellent care provided during hospitalization, requesting a copy of his or her medical record, or requesting a transfer of the individual’s medical record to a new physician; (ii) letters to a continuing care facility asking about availability for the individual upon release; and (iii) letters to the individual’s previous healthcare providers requesting copies of prior medical records. What is generally unknown is that some or all of the information contained in the individual’s medical record may be released to others—both inside and outside the healthcare industry.

Financial information, the term the healthcare industry uses to describe information related to the past, present, or future payment for healthcare services rendered to an individual, is also considered “health information” under HIPAA. Financial information includes information that is shared with or by an individual’s insurance company in order to determine eligibility under the plan, authorize specific services or treatment, coordinate benefits between payors, or obtain reimbursement for services provided. Financial information may or may not be stored on paper. Even if it is in a paper form, financial information rarely is stored as part of the individual’s medical record. For example, an insurance claim form that is sent to the individual’s insurance company to obtain payment includes a detailed listing of each service that was provided to the individual during a particular healthcare encounter. This claim form also includes the individual’s diagnosis, or the problems that caused the individual to request healthcare services in the first place. While the claim form unquestionably contains “health information,” it is usually not included in the individual’s medical record. Other examples of financial information include: the individual’s account debits, credits, and balances; insurance enrollment applications and plan coverage; insurance verification; premium payments or claims history; authorizations and consents to treatment; and collection notices and notes. Usually, financial information is stored in the area of the organization that handles individual accounts and collections. It may be stored on paper in a separate and distinct financial file for each individual, included in a group file (for example, all individuals with a particular insurance coverage), or stored electronically and not kept in a paper form.

**Creation and Collection of Health Information**

It may seem logical to assume that one cannot collect health information about an individual from anyone other than that person. That is not the case, however. While each individual is the primary and major source of his or her own health information, there are other sources from which an individual’s health information can be obtained or generated. For example, symptoms of a particular illness or a person’s social or medical history often are provided to the individual’s physician by a family member or close friend, especially when the individual himself or herself cannot communicate. A test ordered by a physician for a particular reason might result in discovery of some totally unknown and unsuspected medical condition. For the most part, health information that is created while the individual is in the healthcare industry remains within the healthcare system. There are times, however, when someone other than the patient provides that patient’s health information to someone outside the healthcare industry.

Virtually every state has laws that mandate reporting of certain diseases or situations (for example, instances of abuse or neglect, evidence of domestic violence, etc.) to the appropriate state agency. If an individual is found to have a sexually transmitted disease, that information, including the individual’s name and address, must be reported. Similarly, instances of neglect and abuse must be reported to the proper authorities. In an effort to inform consumers about the most competent healthcare providers in the state, or the most customer-friendly insurers or managed care organizations, many states collect and analyze health information about individuals who receive healthcare from the state’s providers, insurance companies, and managed care organizations. In addition to various state databases, more than 800 federal databases contain individually identifiable health information.

Employers may obtain an individual’s health information as a result of pre-employment physicals or treatment for on-the-job injuries. One of
the challenges facing physicians who practice in the area of occupational medicine is how much health information can and should be provided, and to whom. If an occupational medicine physician who is employed by a company discovers an unrelated health problem while treating an individual for a job-related injury, the physician may be torn between his or her duty to maintain confidentiality under the physician-patient privilege, and the responsibility, as an employee, to report the problem to the company. Even if the physician is not an employee, he or she may have to include the health condition on the bill that is sent to the employer in cases where the company is paying for the employee's treatment.

Individuals may themselves be responsible for inadvertently disclosing confidential information. Those who participate in experimental procedures or research usually must agree to full disclosure of their health information to the pharmaceutical or device manufacturer that sponsors the research. In these cases, individuals have little or no control over the form or content of any subsequent disclosure that is made by the sponsor. An individual may also elect to complete on-line health questionnaires or health histories on an interactive Web site. Data mining programs that function behind the scenes on a Web site, or “cookies” that collect information about individuals who visit a particular site, may be hard at work but not be discovered by the individual—until he or she receives a later communication that can be traced back to that Web site.

### Accessing and Using Health Information

Even though health information about one person may be widely dispersed within a healthcare organization, it is nonetheless considerably easier to find that information within the healthcare entity than outside it. Within the healthcare industry, it is much easier to find the information at a health care provider than at a payor. For the most part, health information is stored centrally at a health care provider organization. Most of the individual's clinical information is found in his or her medical record, and most of the individual's financial information is found in the provider's finance department. At a healthcare payor organization, however, health information is rarely stored in one central file. Instead, pieces of it are stored according to their primary function (for example, membership, customer service, claims processing, utilization management, etc.). In addition, the payor organization itself may be decentralized; claims processing, for example, may take place in multiple places within one facility, be found in different facilities in the

<table>
<thead>
<tr>
<th>Entity</th>
<th>Need for Limited Access and Use</th>
<th>Potential Risks and Benefits Associated with Unrestricted Access and Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employers</td>
<td>Health information related to the individual's employment (disability, restrictions, reasonable accommodations).</td>
<td>The information may be used to the employer's advantage in hiring and promotion decisions</td>
</tr>
<tr>
<td>Researchers and research sponsors</td>
<td>Health information related to the particular study.</td>
<td>Entities may; (1) Select only those individuals who would be the best for the study; (2) Target certain groups for marketing activities; (3) Use the information to develop new treatments or technologies.</td>
</tr>
<tr>
<td>Judicial and administrative proceedings</td>
<td>Health information related to the issue(s) in the proceeding.</td>
<td>Unrelated health information could be used against the individual.</td>
</tr>
<tr>
<td>Insurance companies and managed care organizations</td>
<td>Health information for purposes of processing a claim.</td>
<td>Unrelated information may be used to deny coverage or to raise premiums, thus discriminating against those who are greater insurance risks.</td>
</tr>
<tr>
<td>State and federal databases</td>
<td>Identify efficient healthcare organizations and those with the best outcomes. Containment of disease outbreaks. Collection of health statistics and monitoring of disease trends.</td>
<td>Misuse of data by others, perhaps for inappropriate commercial use. Overcollection of data on individuals (Big Brother).</td>
</tr>
</tbody>
</table>
same city, or be located in different facilities in different cities.

Rarely is all of an individual’s health information accessible from a single location outside the healthcare industry, even though individuals and organizations outside the healthcare industry would like to be able to use all of it. The grid on page 57 provides examples of entities outside the healthcare industry that may need access to health information, the primary reasons for allowing them to access and use a limited amount of health information, and the potential risks and benefits associated with allowing unrestricted use of health information.

**Conclusion**

There is a long-standing tradition of confidentiality in the healthcare industry. In the days when an individual’s health information could be collected only from that individual, and when it was stored only on paper, there was far less risk that a person’s right of privacy would be compromised. The transition to electronic records that is occurring in the healthcare industry, combined with the reality that health information also is collected and shared outside the health industry, increases the risk that breaches of privacy will occur and that unwarranted uses of personal health information will be made. Most uses of health information are for legitimate purposes such as payment of claims, medical research, and collection of public health statistics. The challenge in the privacy debate is to find the appropriate balance between adequate protection and legitimate uses of health information—in all the forms that information may take and all the locations where it may be found.
his article provides a brief overview of developments, common elements, and trends in state laws governing the privacy of health information.

No single, comprehensive federal law protects the confidentiality of an individual's health information. Although a number of privacy bills were introduced in recent sessions of Congress, none became law. Hundreds of state laws provide varying degrees of protection, however. As noted earlier (see Appendix B, “Highlights of the Final HIPAA Privacy Regulations,” on page 50), some of these state laws will not be preempted by the final HIPAA Privacy Regulations because the state law offers greater protection to an individual's health information. There is very little uniformity in state laws across the county. Different states use various terms to describe the health information they protect, and may be somewhat limited in the type of information they protect. The individual's rights in his or her health information vary from state to state, and some laws apply only to selected components of the healthcare industry rather than to all healthcare entities.

No Single Common Term or Definition

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the term “health information” includes any information about the past, present, or future condition or treatment of an individual, that is, what has been historically maintained in a person’s “medical record” (and possibly elsewhere in the treating facility)—what the healthcare industry considers clinical information. “Health information” also includes any information that relates to an individual’s past, present, or future payment for health services. In short, HIPAA’s definition of “health information” includes both the clinical and the financial portions of an individual’s information.

No state privacy laws use the term “health information,” although some use a similar term, “health care information.” A handful of states use the older term, “medical record,” while others use terms such as “medical file,” “medical information,” “medical record information,” and even “health care records.” Where states use a term similar to the one in the final HIPAA Privacy Regulations, the definition encompasses more than just the clinical information traditionally found in an individual’s medical record. It often includes x-rays and tracings as well as the individual’s financial information. While HIPAA’s “health information” at first glance appears broader in comparison to state laws, state laws that include more than clinical information within their defined term predate HIPAA, and therefore protect the same, if not more health information. Even if a particular state’s health privacy law is relatively new, the trend is to afford greater protection to health information, not less.

Types of Information Protected

All states have laws that provide special protections for one or more types of health information. AIDS-related data is the most common type of information to receive this special protection. While every state protects the actual results of HIV tests, many states consider disclosure of the fact that an individual underwent a test for HIV just as deserving of protection. These states view disclosing that the individual received a test as serious a violation of the individual’s right to privacy as disclosing the results of that test.

More than half the states recognize the confidentiality of mental health and developmental disability records. These records are not the same as substance abuse and treatment records, which enjoy stringent protection under the Confidentiality of Records provisions of a federal public health and welfare statute (42 U.S.C. §290dd-3). State laws protect records that contain information about treatment related to an individual’s emotional well-being that are maintained by mental health providers and facilities in the state. In situations where mental health records contain information related to substance abuse or treatment, many custodians consider them doubly protected—by the state’s special mental health and general confidentiality laws and by the federal Confidentiality of Records provisions. Custodians of records that have both federal and state protection typically have implemented special procedures to ensure that mental health and/or substance abuse and treatment records are not accidentally disclosed. Increasingly, jurisdictions are enacting laws that protect genetic information and test results.

Peer review information, much of which is individually identifiable health information, is also considered extremely confidential and is protected by separate state laws. Those laws, however, are primarily designed to protect the medical personnel who created the information, not the individual to whom the data refers.

Individual Rights

There is great variety among states in the rights they grant to individuals under their confidentiality and privacy laws. Every state that has some type of statute protecting health information views that information as confidential, and the majority of those states require the individual’s prior written consent or authorization, as appropriate, before the information may be disclosed. In contrast to HIPAA, the terms “consent” and “authorization” are not distinguishable; where one state uses the term “consent,” another will use “authorization” to refer to the same process.

Many states follow a general rule that requires the individual to consent to or authorize the release of his or her information prior to its disclosure.
Most of these states also provide specific exceptions to the general rule. For example, several states allow the release of basic information (name, sex, address, age, and condition in general terms) about an individual to anyone requesting the information, provided that the individual at issue is currently receiving treatment and has not specifically prohibited the release of his or her information. Similarly, to facilitate treatment or to preserve continuity of care, some states allow one provider to disclose information to another provider without the individual's consent or written authorization.

Most states prohibit disclosing HIV, mental health and developmental disability, or substance abuse treatment records without a special authorization. Virtually every state allows providers to disclose information to the individual's health plan or insurance company in order to authorize treatment or obtain payment for services that were provided. A few states permit law enforcement agencies and authorities to access an individual's health information without the individual's consent or authorization, and most states' laws permit disclosures that are associated with subpoenas or court orders and disclosures that are required by law under the state's general confidentiality laws or elsewhere.

More than half the states allow individuals to access and/or obtain a copy of their own health information unless the individual's provider believes that the individual or some other person might be harmed if the information were disclosed. Several states that allow an individual to access his or her information also require the individual to request that access in writing. If a copy of the information is provided, the individual who requested the information is usually responsible for the reasonable costs associated with copying it and is not given a copy until those costs are paid.

Health insurers that are licensed by a particular state must provide their members and subscribers with a notice similar to the one required by the HIPAA privacy regulations. This notice requirement is a result of the Gramm-Leach-Bliley Act (also known as the Financial Modernization Act of 1999). Entities that are subject to this statute must be in compliance by the end of 2001. Health insurers currently are the only component of the healthcare industry that is included in the list of entities that must comply.

A number of states give an individual a statutory right of action for unauthorized disclosures of his or her health information. In other words, the individual has the right to sue and collect money from the person or facility releasing his or her information if the release was made without the individual's approval. The amount of damages an individual can collect varies from state to state. Some states require individuals to prove that they have suffered some harm as a result of the disclosure. In most of these cases, the laws limit the amount of money that can be awarded to the individual. Other states allow for punitive damages, but these awards are usually capped as well. In a few states, the individual can sue, but any monies awarded are paid to the state.

Inconsistent Application to Healthcare Industry Entities

It is not always easy to identify every state law or regulation that protects the confidentiality of health information. In part, this reflects the reality that state laws and regulations develop over time, often in an unsystematic fashion that may not take advantage of other states' efforts on the same issue. The result is a patchwork quilt of laws both in a particular state and across the country. Every type of healthcare organization or provider, for example, is subject to laws that apply to them because of the type of organization or provider they are. For example, certain laws are specific to insurance companies. (These laws often apply to managed care organizations as well, but in some states managed care organizations must follow a similar, but different, set of laws.) Similarly, hospitals and other healthcare institutions are subject to a different set of laws from those that govern physicians, nurses, and other healthcare professionals. Privacy requirements sometimes appear as stand-alone laws. Often, however, they appear as statutory language within more comprehensive laws, for example, as privacy provisions within medical licensing laws or other laws governing healthcare professionals and/or facilities.

Summary

State laws and regulations that protect the confidentiality of health information are numerous and in various stages of development. Some states acted long ago to recognize an individual's right to privacy and, even before HIPAA's enactment, continued to refine and enhance their confidentiality laws to address operational issues not initially contemplated as well as those raised by the increased use of electronic medical records. Other states are just beginning to draft comprehensive privacy laws. In general, recently enacted laws will more closely match the final HIPAA Privacy Regulations. Regardless of where a state is in its development of confidentiality laws, each state's legislature is keenly aware of the public's growing interest in health information privacy. State legislatures face a daunting challenge in drafting laws that are flexible enough to address changes occurring in the healthcare industry itself, broad enough to allow for the rapid advances in technology, and comprehensive enough to give individuals a sense of security that their health information is, and will be kept, confidential.
About the American Health Lawyers Association

Vision
To lead health law to excellence through education, information, and dialogue.

Mission
To provide a forum for interaction and information exchange to enable its lawyer members to serve their clients more effectively; to produce the highest-quality, nonpartisan, educational programs, products, and services concerning health law issues; and to serve as a public resource on selected healthcare legal issues.

History
Created by a merger of the National Health Lawyers Association and the American Academy of Healthcare Attorneys on July 1, 1997, the American Health Lawyers Association is the nation’s largest nonpartisan 501(c)(3) educational organization devoted to legal issues in the healthcare field, with a history of 31 years* of providing resources to health attorneys. The association’s 9,000 active members practice in law firms, government, in-house settings, and academia. They represent the entire spectrum of the health industry: physicians, hospitals and health systems, health maintenance organizations, health insurers, managed care companies, nursing facilities, home care providers, and consumers.

* American Academy of Healthcare Attorneys was founded in 1968.
2000–2001 Board of Directors

Beth J. Schermer, Esq.
President
Coppersmith, Gordon, Schermer, Owens & Nelson PLC
Phoenix, AZ

Douglas A. Hastings, Esq.
President-Elect/Chair, Programs Committee
Epstein Becker & Green
Washington, DC

James Roosevelt, Jr., Esq.
President-Elect Designate/Chair, Finance Committee
Tufts Health Plan
Waltham, MA

Michael F. Anthony, Esq.
Immediate Past President
McDermott Will & Emery
Chicago, IL

Robert A. Griffith, Esq.
Griffith & Associates
Boston, MA

Gail P. Heagen, Esq.
Sentara Health System
Norfolk, VA

Daniel B. Higgins, Esq.
Paul, Hastings, Janofsky & Walker
San Francisco, CA

Mark A. Kadzielski, Esq.
Akin Gump Strauss Hauer & Feld, LLP
Los Angeles, CA

Gregory M. Luce, Esq.
Jones Day Reavis & Pogue
Washington, DC

Thomas W. Mayo, Esq.
Haynes and Boone, LLP
Southern Methodist University
School of Law
Dallas, TX

Mark G. Mishek, Esq.
Allina Health System
Minnetonka, MN

Peter M. Leibold, Esq.
Ex-Officio
American Health Lawyers Association
Washington, DC

Susan O. Scheutzow, Esq.
Ulmer and Biever, LLP
Cleveland, OH

Nancy J. Severson, Esq.
Denver, CO

James G. Sheehan, Esq.
Assistant US Attorney
Philadelphia, PA

Jennifer A. Stiller, Esq.
Haverford, PA

T. J. Sullivan, Esq.
Gardner Carton & Douglas
Washington, DC

James L. Touse, Esq.
Blue Cross Blue Shield of Tennessee
Chattanooga, TN

Adele A. Waller, Esq.
Bell Boyd & Fordyce
Chicago, IL

Ivan Wood, Esq.
Strasburger & Price LLP
Houston, TX

Health Lawyers Staff

Executive Department

Peter M. Leibold, Esq.
Executive Vice President/Chief Executive Officer

Rita Brinley
Executive Assistant

Operations

Wayne Miller, CAE
Deputy Executive Vice President/Chief Operating Officer

Eileen M. Bantel
Manager of Special Interest and Substantive Law Committees

Clara M. Woodall
Financial Assistant

George Mair
Network Administrator

Yolanda Smith
Database Administrator

Robert Wilson
Office/Fulfillment Assistant

Membership Services & Marketing

Kerry B. Hoggard, CAE, PAHM
Director of Strategic Planning, Membership & Marketing

Franklin Boyd
Manager of Member Services

David E. Sharpe
Manager of Marketing

Mary Boutsikaris
Art Director/Graphic Designer

Emilee Simmons
Membership/Editorial Assistant

Carine Brice
Senior Member Service Representative

Marianne Schrupp
Member Services Representative

Donna Swann
Receptionist

Professional Resources

Blair Dobbins, JD
Director of Professional Resources

William B. Harvey, Esq.
Manager of Non-Dues Publications and Acquisitions Editor

Joseph C. Salerno, Jr.
Manager of Internet Services

Elizabeth S. Turman, Esq.
Editor in Chief

Lisa C. Weltsch, JD
Managing Editor

Marshall M. Burkes
Internet Services Coordinator

Robert C. Truhil II
Production Editor

Programs

Anne H. Hoover
Director of Programs

Valerie Burrows Eshleman
Manager of Programs

Rachel Nelson
Programs Assistant

Sharn A. Robertson
Faculty Assistant

Public Interest

Joseph A. Kuchler
Director of Public Interest

Directors

Gail B. Agrawal, Esq.
University of North Carolina
School of Law
Chapel Hill, NC

Jerry A. Bell, Jr., Esq.
Fulbright & Jaworski, LLP
Houston, TX

Elise Dunitz Brennan, Esq.
Doerner Saunders Daniel & Anderson, LLP
Tulsa, OK

Gail P. Heagen, Esq.
Sentara Health System
Norfolk, VA

Mark A. Kadzielski, Esq.
Akin Gump Strauss Hauer & Feld, LLP
Los Angeles, CA

Almata E. Cooper, Esq.
Ohio State Medical Association
Hilliard, OH

Douglas J. Hammer, Esq.
At-Large Member of the Executive Committee
Intermountain Health Care, Inc.
Salt Lake City, UT

Anthea R. Daniels, Esq.
Secretary/Chair, Professional Resources Committee
Cleaveland, OH

S. Allan Adelman, Esq.
Chair, SISLC Committee
Godard West Adelman Sheff & Smith
Rockville, MD

Wayne Miller, CAE
Deputy Executive Vice President/Chief Operating Officer

Eileen M. Bantel
Manager of Special Interest and Substantive Law Committees

Clara M. Woodall
Financial Assistant

George Mair
Network Administrator

Yolanda Smith
Database Administrator

Robert Wilson
Office/Fulfillment Assistant

Kerry B. Hoggard, CAE, PAHM
Director of Strategic Planning, Membership & Marketing

Franklin Boyd
Manager of Member Services

David E. Sharpe
Manager of Marketing

Mary Boutsikaris
Art Director/Graphic Designer

Emilee Simmons
Membership/Editorial Assistant

Carine Brice
Senior Member Service Representative

Marianne Schrupp
Member Services Representative

Donna Swann
Receptionist

Professional Resources

Blair Dobbins, JD
Director of Professional Resources

William B. Harvey, Esq.
Manager of Non-Dues Publications and Acquisitions Editor

Joseph C. Salerno, Jr.
Manager of Internet Services

Elizabeth S. Turman, Esq.
Editor in Chief

Lisa C. Weltsch, JD
Managing Editor

Marshall M. Burkes
Internet Services Coordinator

Robert C. Truhn II
Production Editor

Programs

Anne H. Hoover
Director of Programs

Valerie Burrows Eshleman
Manager of Programs

Rachel Nelson
Programs Assistant

Sharn A. Robertson
Faculty Assistant

Public Interest

Joseph A. Kuchler
Director of Public Interest
CONTRIBUTORS
Godard West Adelman Sheff & Smith
Joanne F. Goldberg and
Alan S. Goldberg, Esq.
Kerry B. Hoggard, CAE, PAHM
Kelly Law Firm, PC
Joseph A. Kuchler
Peter M. Leibold, Esq.
Kathleen McDermott
Margaret M. Manning, Esq.
William H. Maruca, Esq.
David E. Matyas, Esq.
James Roosevelt Jr., Esq.
Nancy J. Severson, Esq.
Michael L. Silhol, Esq.
Dr. Richard F. Tompkins

FRIENDS*
Franklin Boyd
Joanne Byars
Hollowell Peacock & Meyer, PA
Michael G. Jones, Esq.
Anne Mac Arthur
Robin S. Martinez
Heather McKenzie
Mark Mishek, Esq.
Peter A. Pavarini
Emilee Simmons
Robert Truhn II

LEVELS OF GIVING
Patron – $1,500 or more
Benefactor – $500 - $1,499
Contributor – $101 - $499
Friend – up to $100

*Space does not permit listing the many Health Lawyers members who contributed through the $10 donation check-off on their membership renewal form. Health Lawyers also acknowledges and appreciates their support. Please see our Web site (www.healthlawyers.org) for a listing of all member contributors.