July 1998

NATIONAL HEALTH POLICY FORUM

Protecting the Confidentiality of Health Information

■

A background paper prepared by
Lise Rybowski, *Consultant*

The George Washington University
WASHINGTON DC

How best to protect the confidentiality of health care information is a complex and contentious issue that raises some of Americans' greatest fears about unimpeded, "Big Brother"-like intrusions into personal areas and unchecked abuses of sensitive information. Resolution of this issue, however, is key to the health care industry's use of information technologies to evaluate quality-improvement and cost-reduction efforts in the delivery of health care.

Concerns about personal privacy in the context of health care information are not new, nor is this the first time that they have demanded the attention of Congress. But recent changes in the health care environment have heightened public awareness that much personal information is widely available and beyond the control of the individual. Polls by Louis Harris/Equifax have found that, while many people take a pragmatic approach to the impact of information technologies on their lives, they are also anxious about the rapid pace at which information is being exchanged and eager to see some restraints put on the ways and the circumstances in which their personal information can be used.

At the same time, those who use this kind of information to deliver, improve, research, track, and evaluate health care-related services, in both the private and the public sectors, are equally anxious to ensure that any such restraints—assuming they are necessary—do not interfere unduly with their ability to function. Specifically, they worry about the effect of privacy protections on their ability to share information and, therefore, their ability to provide care appropriately and efficiently.

Consequently, the debate about the confidentiality of health care information is often framed as a conflict between the privacy interests of individual consumers of health care and the information needs of the private and public health care entities that deliver these services. But the reality is not so cut and dried. There is a surprising degree of consensus among the various stakeholders—including consumer advocates, providers, payers, and researchers—regarding the importance of respecting and enforcing health information confidentiality rights, at least in principle. Thus, disagreements are occurring not at an ethical level but at a practical one; it is over the details that the different parties and their competing interests collide. The controversy centers on the difficult question of where to draw the line between appropriate and inappropriate uses of identifiable information. That is, what information must be available, to whom, and for which of many possible purposes?

The purpose of this paper is to lay out the issues that have to be resolved, the perspectives of the stakeholders, and some of the options available to legislators, regulators, and the health care industry.

THE IMPETUS FOR LEGISLATION

While the issue has been debated off and on for many years, the call for congressional action to resolve the controversies surrounding health information confidentiality results from the confluence of several factors. The most obvious stimulus is the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[1] which requires that Congress act to protect personal privacy. The second factor is the notable progress in information technologies over the last several years and its impact on the usefulness and ubiquity of health care data. A third issue is growing awareness of the use of personal medical data by various health care corporations for commercial advantage. A fourth is the growth of managed care in the 1990s; the associated increase in the number of entities with access to personal health information has accentuated both clinician and patient concerns about privacy, particularly with respect to how that information may be used to create barriers to care and coverage. Finally, the need to legislate on this issue is driven—albeit to a lesser extent—by international pressures, as concerns about health information confidentiality are not unique to the United States.

Legislative Requirements

HIPAA, the biggest political change spurring action with respect to health information confidentiality, required the secretary of health and human services to make recommendations to Congress on ways to protect individually identifiable information and to establish penalties for wrongful disclosure for health care transactions. The secretary presented those recommendations on September 11, 1997. Congress now has until August 1999 to enact a privacy law. If Congress fails to meet this deadline and does not vote to extend it, the legislation obliges the secretary to promulgate regulations with standards for the confidentiality of electronic administrative and financial transactions by February 2000. However, there is some question as to how such regulations would play out in the absence of legislation. One key issue is that HIPAA specifically addresses only electronic media and limits regulatory oversight to administrative and financial data, creating distinctions that are problematic. It would be difficult for the

secretary (or Congress) to protect the confidentiality of information in claims systems but not that in medical records; also, regardless of how the law is currently written, it is unclear how the Department of Health and Human Services (DHHS) would be able to devise protections that pertain to data maintained and transmitted in electronic media but not to data maintained on paper or other forms of media or to data transmitted by telephone or fax.

Since neither the health care industry nor the privacy advocates want to see Congress cede responsibility for the law to the administration, they are largely united in their desire to seek a mutually satisfactory solution through legislative channels before the deadline. It remains to be seen, however, whether Congress will be able to resolve competing interests in the allotted time.

Some pressure is also arising from the perceived inequity between health information, which many people believe contains the most personal data, and other common records, such as those maintained in the context of credit reporting, banking, electronic mail, cable television, and video rentals. While federal legislation safeguards the confidentiality of these kinds of data, it does not extend similar protections to medical records, which are widely circulated and used with varying degrees of oversight, depending on the applicable state law. In fact, both federal and state laws have authorized disclosure of records for a variety of purposes, including fraud and abuse investigations, public health, peer review, accreditation, and licensing.

The Growth of Information Technologies

There is little question that the speed and functionality made available by information technologies have created and will continue to generate tremendous benefits for the health care industry. But computers are a mixed blessing, because the ease with which they can make data widely available poses new risks to individual privacy. Compared to paper-based records, electronic information is more easily manipulated and linked and is certainly more portable. Computerization also raises the specter of a huge, national database of identifiable, comprehensive health information. Although development of such a database is unlikely, many people find such a notion threatening (and some wrongly believe it is required under HIPAA). Finally, the capabilities of database software programs make the information they access more valuable commodities. Thus, although the risks to privacy are not new, the accelerating use of these technologies in and across health care institutions is forcing society to reconsider and revise its policies vis-à-vis the protection of personal health information.

However, very few of the relevant stakeholders are actually arguing against computerization in the health care industry—which has been one of the industries slowest to adopt information technology. It is widely acknowledged that computers can increase the ability to protect, disguise (by stripping indicators as well as by encrypting), and track the disclosure of information. Moreover, abuses can and do occur, regardless of whether the information is in electronic or paper form. For most privacy advocates, the problem is not the technology itself but the likelihood that entities will amass huge amounts of personal data, simply because they can rather than because there is a true need to do so.

Secondary Uses of Personal Health Information

The growth of information technologies has led to increased use of personal health information for purposes other than those for which they were originally collected. Disease management strategies, for instance, often depend on the ability to identify individuals with specific conditions for more intensive treatment or care management. The use of personal health information for commercial advantage also has become increasingly common. Pharmaceutical companies, for example, often rely on identifiable pharmacy prescription data to target customers who might be interested in their new products or services. Baby formula manufacturers often use hospital admissions data to target new mothers. And, while consumers could conceivably benefit from this unsolicited information, many privacy advocates object to the availability of this information without the patient's consent. Furthermore, commercial insurers have historically used claims data for medical underwriting, often to the detriment of potential subscribers.

The Spread of Managed Care

In the course of transforming the delivery of health care in the 1990s, managed care has brought about major changes in the ways in which information is gathered and used. The health care delivery system now has a seemingly unquenchable need for information. One result has been that, in addition to collecting data at the individual patient level, providers, payers, employers, and others are pooling substantial amounts of data in order to understand what is happening at the level of populations (or relevant subsets). While this is contributing to significant new knowledge about the

delivery and outcomes of care, it also implies a dissemination of personal information far beyond the walls of a doctor's office. Although there is little hard evidence to support the view that personal health information is being widely misused as a result of this population-based approach to care, the press has heightened the public's fears by broadcasting numerous anecdotes about individual instances of confidentiality breaches.

The practices associated with managed care also raise serious questions about the responsibilities of the various employees, contractors, and vendors with access to personally identifiable information. While the duty of health care providers to protect the confidentiality of patient records is established in some federal and state statutes, case law, and professional codes of conduct, the duty of many third parties has yet to be legally defined.

For some stakeholders (usually physicians), the fight for privacy protections has become part of a broader battle against the expansion of managed care and demands for more explicit accountability. However, most parties to the debate recognize that the legislation must be sensitive to the current structure and operations of the delivery system, even as it confronts the system's flaws. In particular, proposals must acknowledge the existence and impact of integrated systems, which cannot function without an unimpeded flow of information among the providers of care.

International Pressures

Concerns about the confidentiality of health care information are widespread in other countries. Canada, New Zealand, and the members of the European Union, among others, have enacted a variety of strict policies, procedures, and penalties to ensure that data collected for health care purposes remain confidential.[2]

Some experts have noted that public concern in other countries does not appear to be as palpable as it is in the United States. One attributes the relative calm in Europe, for example, to the availability of guaranteed health care coverage; Americans are much more anxious about the impact that inappropriately disclosed information could have on their health care coverage or jobs (and therefore their ability to afford insurance and care). But other nations also appear to be acting more quickly to respond to their citizens' fears. It is not clear why this would be the case, although peer pressure from neighboring countries has certainly been instrumental in pushing the European nations towards the adoption of specific protections. In the United States, on the other hand, people have not transformed their concerns into popular support for any initiatives. Congress is also facing the powerful force of inertia and mixed signals from various parts of the health care industry.

While some of the new policies of other nations have no implications for the United States, of particular concern to American companies and agencies are provisions that organizations covered by the privacy protection rules of a given country may not disseminate information to organizations outside the country that do not provide an adequate degree of protection. For example, a directive of the European Union explicitly states that member nations must adopt this policy by October 1998. If the United States fails to reach a consensus on how to address the privacy issue, international restrictions on the flow of data could quickly become a serious problem for private firms and government agencies involved in research, public health, and other information uses where data routinely cross international borders.

UNDERSTANDING TERMINOLOGY

Before launching into a discussion of the issues that Congress will have to resolve, it may be helpful to review the terms that are commonly tossed around in the context of this debate. Since there are numerous ways to interpret and define these terms, this section is not meant to be definitive but is merely intended to provide a common ground for the reader.

The word used most often is *privacy*, which has been defined in its broadest sense by U.S. Supreme Court Justice Louis Brandeis in 1928 as the right to be left alone.[3] According to the National Committee on Vital and Health Statistics, privacy in the health information arena—which is also called records privacy, information privacy, and data protection—refers to the interests of patients in knowing and controlling how their personal health information is collected, maintained, used, and disclosed.[4]

Many stakeholders argue that the issue is not really one of privacy, since the nature of health care demands that patients reveal personal information in order *not* "to be left alone." Rather, the problem is *confidentiality*: How do we ensure that information disclosed by an individual is protected from unauthorized use or redisclosure? To privacy advocates, who believe that information represents and is owned by the individual, any disclosure without consent would be a breach of confidentiality. Others argue that confidentiality is

maintained as long as the identity of the individual is protected from disclosure, even if information is shared without consent. (As a general rule, it is useful to think of privacy as belonging to a person, while confidentiality is a property of information.)

To maintain the confidentiality of health information, participants in the health care arena rely on a variety of *security* measures, which are the policies, procedures, and technological tools that protect the use and disclosure of information. Security is responsible for ensuring authorization (that is, who can see the information?), integrity (that is, did it arrive in the way it was sent?), and authenticity (that is, can the user's identify be verified?). While the use of such measures can be encouraged or even compelled by law, a specific approach to implementing security cannot be legislated, especially in light of the rapid changes in the technologies available for these purposes.

DISSECTING THE CONTROVERSY

This section examines the concerns of the various stakeholders on the health information confidentiality issue and discusses some of the options that legislators may consider. To the extent possible, this paper will point to the areas in which there appears to be some agreement among stakeholders: primarily with regard to those uses of information that are either distinctly linked to patient care and payment for services or clearly outside of the boundaries of health care, such as marketing. Areas of disagreement, on the other hand, occur mainly in the gray areas—those uses of information that are not necessarily of direct benefit to the patient but can be argued to be related to the provision of health care.

As noted previously, competing interests do agree on the broad principles at stake. They also recognize that the lack of minimum standards for the use of health information in the United States is a serious problem. Since information flows between states, there is a growing consensus regarding the need for ground rules for maintaining confidentiality so that people —regardless of the type or location of their organization—know what is expected of them. Thus, on the whole, people concur on the need for rules (especially with regard to the downstream users of information, many of whom currently have no constraints on their activities), limits on the ways in which information is used, and procedures for controlling use and disclosure. There is also a growing respect for the idea that society will have to make some tradeoffs between privacy and other social values, although that concept is certainly not universally accepted.

The Spectrum of Views

Although there is an "us against them" theme to much of the privacy debate, the issue clearly has many sides; neither the advocates nor the representatives of industry speak with one voice. Moreover, like many health care issues, strong beliefs tend to cross party lines. However, in the interest of imposing simplicity on a complex subject, it is helpful to review the basic philosophies shaping the perspectives at each end of the spectrum.

Privacy as a personal right. To many privacy advocates, privacy is a personal right attached to an individual. The implication of this idea is that individuals own the information in their medical records and have a right to know where their information is going and why. From this perspective, violations of that right can undermine the trust between doctor and patient that is fundamental to the quality of the clinical relationship. Without that trust, privacy advocates maintain, people will not be honest about their information, particularly if there are risks associated with disclosing sensitive data (such as genetic predispositions or unhealthy behaviors). In the HIV field, this kind of behavior has already been exhibited: Because the diagnosis is so stigmatizing, patients afraid of how their information might be used tend to censor themselves, sharing only as much as they believe necessary. Similarly, the fact that providers have had to offer anonymous testing in order to draw people in demonstrates the extent to which individuals fear exposure, even at the risk of their own health.

Advocates also argue that distrust of the "system" will eventually undermine even the most benevolent of social goals; for instance, clinical research will have little value if the credibility and completeness of the original data are in question. Thus, they argue, society has an ethical and social interest in preserving the privacy rights of individuals.

"Life Is Not Risk-Free." Standing at the other end of this relatively narrow spectrum are representatives of the pharmaceutical and other research-based industries and agencies (such as government health departments)—most of whom respect and support the values associated with individual privacy rights. However, their emphasis is on striking a balance between these rights and other laudable goals. In their view, confidentiality should not be maintained at the risk of information uses with high social value, such as research,

public health, and quality improvement. Although they want reasonable protections regarding the access and use of individually identifiable information, they believe that it is not possible or practical to protect everything absolutely.

Industry representatives and researchers are also concerned that privacy advocates are characterizing the use of information as a net negative for consumers, implying a need to specify precisely which uses should be allowable. Not only does this approach send the wrong message to consumers (that is, that all uses of information are "bad"), but it also creates an unduly restrictive environment for information dissemination and use. Moreover, it requires that each acceptable use be thoroughly and accurately defined, which is a particular problem in a health care environment that is constantly changing. Taking what they see as a less negative view of the value of information, those who conduct research would prefer to focus on defining those uses that should be prohibited—such as the use of personal information for marketing purposes, disclosure to the press, or discrimination—leaving a fairly broad circle of legitimate uses. While these proscribed uses may also be hard to identify and define, proponents of this view argue that it will be easier to reach a consensus on the ways in which information should not be used and the strong penalties that should be imposed on those who cross the line.

From the perspective of the provider community, perhaps the biggest concern is that the legislation recognize how the delivery of care has evolved over the past ten years. An unimpeded flow of information is critical to cost containment efforts, outcomes studies, disease management projects, and many other functions that characterize today's delivery system. Despite their differences, the components of the health care industry are not likely to accept a bill that fails to strike a balance between the rights of the individual and the ability of providers and researchers to deliver care effectively and improve upon its quality.

THE REALM OF SOLUTIONS

Many of those seriously committed to working towards a resolution believe that pitting privacy interests against the effective delivery of health care is a no-win situation. They argue that the first step is to reframe the model so as to emphasize the ways in which the protection of privacy rights serves—rather than competes with—the interests of industry. By focusing on the benefits associated with enforceable guarantees of confidentiality, these advocates hope to nourish a more constructive debate regarding what needs to be done to protect data from misuse and inappropriate disclosure, thereby improving the quality of information available to the industry.

Generally speaking, the protection of privacy requires a variety of measures, including administrative and management techniques, education of information users and patients regarding rights and responsibilities, and disciplinary sanctions for misuse (that is, criminal penalties for the intentional, improper disclosure of information or misrepresentation to obtain data). It is important to note that these measures are not specific to electronic health information but apply to all data regardless of the media in which they are maintained or communicated. However, the slate of potential legislative solutions to the problem will certainly include requirements or incentives to harness the capabilities of the many technological tools that can be used to protect information.

Many experts have pointed to a set of principles known as "fair information practices" as the foundation of any legislative solution. Essentially, these principles state that an individual ought to have rights with respect to any kind of information about him or her and that other people should have responsibilities towards that information. They do not necessarily guarantee complete privacy or confidentiality, but they do suggest that personal information will be treated fairly.

Fair information practices are based on the following notions:[5]

- *Openness and transparency*—People should know what records exist about them, how the records are maintained, where they can get the records, and how to use the information.
- *Access and correction*—Individuals should be able to view their records and amend them as needed to correct any errors in the information they contain.
- *Data quality*—Information should be timely, accurate, relevant, and complete for the purpose for which it is maintained.
- *Collection limitation*—Information should be collected by lawful and fair means; in addition, some limitations should be placed on the extent of information that can be gathered for a given purpose.
- *Disclosure limitation*—Those who have access to personal information should not be able to disclose it to others without the consent of the data subject or other legal authority.

- *Use limitations*—Personal information maintained in health records should be used only for the purposes specified at the time of collection.
- *Security*—The system for maintaining information should be reasonably secure.
- *Accountability*—Recordkeepers should be held accountable for adhering to these principles.

These concepts were first articulated in 1973 in a government report that set the stage for future efforts to limit access to and use of personal information.[6] One of the first applications of this code was the Privacy Act of 1974, which imposes constraints on the federal government's use of personal information. Since that time, these principles have served as the basis for similar rulings and laws in both the United States and abroad,[7] including the various legislative proposals currently on the table. However, there is no question that some are more relevant than others and/or enjoy more widespread support. For instance, while nearly everyone would agree that legislation should not rein in a physician's ability to collect information, many people would argue that it ought to restrict insurers' and employers' ability to engage in the same activity. The principles regarding disclosure and use limitations tend to draw the most controversy.

In discussing these principles and their implications, privacy experts on various sides of the debate are often quick to point out that legislation is only part of the solution; nothing is stopping people from doing what they can and should do now to protect the confidentiality of personal information. For instance, organizations should have policies and procedures to accomplish the following:

- Discourage gossip.
- Keep people from looking at or disclosing records for inappropriate reasons.
- Ensure that computer systems are designed in a way that maintains confidentiality.
- Provide physicians and other providers with the information they need to deliver care effectively but no more (for example, a pharmacist needs to know what other drugs a patient may be taking but not the mental health diagnosis underlying a particular prescription).
- Provide payers with the information they need to process claims efficiently but no more.

The latter two examples highlight the dilemma of determining where to draw the line between what is and is not necessary; experts point out that this is not an easy question and cannot necessarily be legislated.

KEY ISSUES

With that caveat in mind, there are several specific, controversial issues that Congress will have to address in the context of health information confidentiality legislation:

- Providing patients access to their information.
- Controlling the access of others to information.
- Segregating information.
- Conducting research.
- Allowing the use of information beyond the realm of health care.
- Preempting state laws with a federal bill.

Providing Patients Access to Their Information

One of the least controversial questions is whether individuals should have a right to their own record. A key element of the fair information practices, the right of a patient to access and amend his or her record, is regarded as the bedrock of confidentiality legislation. Roughly 30 states already have laws allowing patients access to their records, but since these laws are not consistent, it is difficult for a user of information to know what state law is controlling.[8]

Thus, most stakeholders agree that this right should be guaranteed in federal law, which would make access to information uniform across all states. However, there is talk of a few controversial exceptions that complicate the issue. Some elements of the health care industry would like to limit access in the following circumstances:

- Where access poses a risk of harm to the patient.
- Where access could reveal personal information about others; for example, a child's record could contain information about a parent's previous drug use.
- Where access could undermine the validity or integrity of a clinical trial.

Also, while most people agree in principle with the idea of allowing patients to amend their records, providers, researchers, and others in the health care field are concerned that the original records be preserved. Thus, they would prefer to see legislation that gives patients

the right to correct their records by marking errors and appending any necessary information.

Controlling the Access of Others to Information

The next issue concerns the access of everyone other than the patient to individually identifiable information. It raises a number of questions, none of which have easy answers:

- Who should have access to personal information?
- How much access should they have? For what purposes?
- Who should control that access and how?

Wrestling with these questions requires some consideration of the many ways health information is currently used—typically without authorization from the patient—and the number of people who must see that information in the process. Common applications of personal information include the following:

- Delivering and managing care.
- Paying for care (adjudicating claims).
- Assessing the effectiveness of care.
- Managing the health of a population.
- Measuring and improving health status.
- Marketing pharmaceutical and other health products.
- Practicing medical underwriting.
- Conducting medical research.
- Performing oversight activities (including credentialing, accreditation, licensing, and investigations of fraud).
- Tracking and protecting the public health.
- Supporting law enforcement activities.
- Confirming hiring decisions.

While some of these uses are more widely accepted (or decried) than others, the critical point is that these information-intensive activities occur everywhere, all the time, and that no uniform standard exists to control the disclosure and use of health information in the United States. Public attention tends to concentrate on those uses associated with the wrongful, unauthorized disclosure of information, which can be legitimately categorized as a security issue (that is, health care organizations must implement specific tools, policies, and procedures to limit leaks). To many privacy advocates, the greater concern is that individuals are often compelled to authorize disclosure of information to employers not functioning as payers or providers, insurers other than those providing health coverage, and other entities not involved in the delivery of care.

On the theory that continued uncontrolled disclosure will eventually have a chilling effect on the flow of information between physicians and patients, most of whom do not yet realize how many people see their sensitive information, proposed legislation gives patients greater control over the linkage and dissemination of information. Both privacy advocates and industry representatives agree on the need for ground rules for confidentiality so that everyone knows what is expected, especially in the context of information flowing freely across states. Many stakeholders (particularly in the medical community) would like to see standards for how much and what kinds of information outsiders can see and for what happens to information after disclosure—specifically, under what circumstances it may be redisclosed, especially if it was only authorized for a certain purpose.

Unfortunately, the consensus does not extend much further. While there is general agreement regarding the need for information to be readily available for the central purposes of delivering and paying for care, the stakeholders disagree—often passionately—about how best to decide who can see what. The debate centers around three overlapping issues:

- The value of informed consent.
- The role of individuals in determining who can see their information.
- The definition of identifiable information.

Informed consent and the role of the individual. Generally speaking, any use of health care information is appropriate as long as it has been authorized by the patient, that is, as long as the subject of the information has consented to that use. Privacy advocates argue that the concept of informed consent with respect to data is analogous to informed consent for a medical procedure. They argue that, like the performance of a procedure without a patient's consent, the disclosure of medical history without consent should be considered a serious breach of individual rights.

In theory, consent requires that the subject be fully informed of the implications of authorization; in reality, however, people regularly authorize disclosures of their information without understanding what they are allowing. The problem is that, in most cases, patients

have to authorize disclosure in order to get their care paid for. This practice among insurers and employers is so common that some advocates question whether records can ever be truly private; even if access is exclusively limited to providers, the patients themselves can be compelled to bring or send their own records. As a result, some policy experts have given up on the idea of informed consent, believing it better to establish a broad set of health care-related entities that will have access to personal data under legal controls.

The insurance industry echoes this view; rather than engaging in a debate about limiting access, industry representatives would like to see an effort to define exactly which behaviors and uses are appropriate and which are not. In general, they would like to see a broad definition for the realm of legitimate uses related to care (that is, where specific consent would not be required) that would encompass those activities that enhance the ability of integrated systems and managed care organizations to provide cost-effective care. However, the changing nature of the health care environment makes it difficult to design legislation that lists every possibility. Based on the ways in which health care is delivered today, stakeholders can agree that all activities associated with the actual delivery of care should be considered appropriate and that any uses based on unauthorized disclosure are not, but all the rest lies in a gray area.

Given their position as stewards of health information, many health care providers believe that patients should not be signing blanket authorizations. They would like to see legislative language that sets both standards for what providers and others need to do to protect confidentiality and penalties for not doing so. However, they emphasize that the threat to personal information tends to occur outside of the provider's office, not in the doctor's presence. Furthermore, since most abuses are said to stem from people who have "legitimate" access to information, not outsiders (for example, computer hackers), they want external users of information to have to make a strong case to justify the information they want, the amount they claim to need, and how they intend to use it.

This position is especially strong among a minority of physicians who believe they should serve as the sole gatekeepers of information, as well as among mental health professionals, who are concerned about how and why their patients' records are used for administrative purposes. Mental health organizations believe that, in order to maintain the level of trust that is critical to the patient-therapist relationship, they should not have to disclose records absent patient consent unless the need for patient information outweighs the patient's rights and that the scope of exceptions must be narrowly and clearly defined. On the other hand, from the perspective of those concerned about provider accountability, the unavailability of information about mental health services would also serve to limit oversight of the mental health field.

Other segments of the health care industry, including insurers, are less sure about the patient authorization issue. They are concerned about giving patients "veto power" over who sees their information. By withholding information from specific parties, patients could inadvertently undermine the quality of care they receive, bias the results of outcomes studies, or even create a risk to their own health. Insurers, in particular, are adamant about having access to the complete record in order to know exactly what they are reimbursing; however, while they want their employees and contractors to be able to see records, they are not opposed to reasonable limits beyond that sphere. For instance, payers would defend the appropriateness of using data for the purpose of targeting patients for improved care, but not for marketing purposes (for example, to create and sell a list of people with incontinence to adult diaper manufacturers).

While various players in the health care industry suggest that marketing may not be an appropriate use for personal health care information, especially in the absence of consent, there is little question that the use of such information for this purpose by providers, pharmaceutical companies, health plans, and others is becoming increasingly common. Even for those organizations that do not use it themselves, the demand by outside entities has made health-related information a valuable–and profitable–commodity. As a result of news reports in early 1998 regarding the unauthorized purchase and use of identifiable pharmacy prescription data by a database firm on behalf of a drug company, this issue has recently aroused the ire of consumers (some of whom have filed class action suits) and attracted the attention of policymakers at the state and federal levels. While consumers are not necessarily opposed to learning more about possible treatment options, they objected strenuously upon learning that their personally identifiable information could be sold by their local pharmacy without their consent, regardless of the potential value of its purpose. From a policy perspective, the potential for abuse in this context is alarming; while legislatures are not expected to outlaw such marketing practices altogether, it is likely that they will establish requirements with respect to explicitly

informing consumers and obtaining their consent to such uses.

Another contentious issue regarding the use of personal information, in this case by insurers, is the practice of pooling information in a shared database known as the Medical Information Bureau. For the purposes of underwriting, insurers (primarily life insurance companies) may contact the bureau at any time to determine whether an applicant has been refused coverage in the past or suffers from a pre-existing condition. This common activity raises serious concerns about the lack of informed consent on the part of applicants, since most people do not even know that their information is being used in this way. In addition, critics say, the insurers do not impose adequate safeguards to protect the confidentiality of personal information.

Some privacy advocates are disturbed enough about this kind of situation to suggest that consent be obtained every time information changes hands. The health care industry dismisses this idea as costly and overly burdensome for both the provider and the patient, who is likely to just sign everything blindly. (However, this suggestion does draw attention to the practical issue of how to link authorizations to the information so that subsequent recipients are aware of restrictions.) Still, most advocates seem focused on fixing and strengthening the informed consent process so that information flows freely in the clinical area directly related to patient care but cannot be used outside that realm unless specifically authorized. They are particularly concerned that the individual, not the government, should decide who has access to personal information. For instance, patients could be given a standard waiver for billing information that would provide insurers with basic codes for the care to be covered. If the insurer needs more detail, the patient would be told and given an opportunity to consent to that disclosure. This approach allows the patient to refuse further disclosure, thus taking back responsibility for paying the claim. While this may not be an easy decision to make, at least it would be an informed one. In addition, privacy advocates would like to protect personal information that has been released by permitting disclosure only to people who are at an appropriate clinical level to understand the information and take ethical responsibility for it.

Individually identifiable information. The issue of informed consent is entangled with the debate surrounding "individually identifiable information," which refers to any information that can be traced back to its subject. Obviously, records with names, addresses, and Social Security numbers are identifiable. However, some privacy advocates argue that even records from which all this information has been stripped can sometimes be associated with a person. The question of when information is identifiable becomes especially important in the context of legislative proposals requiring that no identifiable record may be used without informed consent. Not surprisingly, researchers are very concerned about the ramifications of this idea.

In addition to researchers, others in the managed care industry note that they need identifiable information for the coordination of care and payment, utilization review, quality assurance, outcomes research, and risk stratification for disease management (that is, to identify people most in need of care)—all of which they regard as legitimate health care activities that enhance the industry's progress toward the provision of coordinated care.

One way to address this issue is through the use of patient identifiers, which can enable researchers to use and link records without knowing the actual identity of their subjects. Among HIPAA's requirements is the development of standards for a unique patient identifier. However, the creation of identification numbers is very controversial, with some advocates expressing fears that it will only make information more accessible to those without authorization. And even proponents recognize that this idea is likely to result in a political quagmire because it is commonly perceived as a national identification card.

The more likely resolution lies in the use of encryption, which could be used to hide the identity of the subject from everyone except the individual who holds the key to the code. Given the sophistication of today's encryption systems, most stakeholders agree that encrypted information should not be considered identifiable, which is good news for the research community. At the same time, however, there is a strong demand that the keyholder be held legally liable for maintaining the secrecy of the key.

Segregating Information

Closely linked to the issue of informed consent is an even more hotly debated proposal to allow individuals and/or their providers to segregate information, which means that they can decide what elements of their information to reveal or hide. Thus, rather than consenting to the release of their complete medical records, patients would be authorizing disclosure of specific parts of that record to specific parties.

Under the philosophy that no one is entitled to know anything about a person unless he or she chooses to disclose it, some privacy advocates are pushing draft legislation that would seriously limit access to information, even by providers. They argue that the individual patient should be able to determine which information is sensitive or important (such as mental health treatment notes or a history of abortion) and limit access accordingly. Driving this argument is a common fear that sensitive information will be used against the individual, most likely by an insurer or employer. Our growing knowledge of the genetic map is particularly threatening because it arouses people's anxieties about not being able to get coverage because of a statistical predisposition, possibly based on information they did not want disseminated.

One variation on this approach would include the suggestion by a handful of advocates that individuals be able to exercise control over their information by keeping some information out of computerized records. They believe that the individual should have the right not to become part of a computerized information system —even if the intent of such a system is completely benevolent. Most privacy advocates question the feasibility of this strategy, recognizing that it is not realistic to exclude information from computerized records and concerned that it deflects attention from the real issue, which is that abuses are committed whether data are in electronic form or on paper, usually by people who already have access. Also, computers offer protections and information-masking capabilities that cannot be duplicated in hard copy files. However, the issue for proponents of this position is not that a computerized system is good or bad in itself but that people should have the choice of opting out. Recognizing that this approach may be inefficient, these stakeholders contend that few people will actually opt out, but all people will feel freer to share personal information, knowing they have some control over how their data are maintained.

Among the strongest proponents of this proposed approach are members of the mental health community who believe that psychiatrists and other therapists should have the option of keeping their notes out of the computer and thus out of the reach of the managed care organizations, which should only have access to the minimum level of information necessary to do their job. Operationally, supporters argue that this approach is no different from maintaining different folders for notes and other records, which many providers already do now.

One complication to the computerization backlash is that, if anything, computers make it easier to mark and track the dissemination of records that have been designated as sensitive in order to minimize distribution. It is generally not feasible to segregate some parts (such as the mental health history) from the rest of the medical record when it is maintained on paper, as most still are, especially in provider offices. The British Medical Society, which has adopted this segregation approach as its policy, is relying on computers to make it possible; to that end, it is developing a security system that will enable patients to set access levels and grant permission for specific disclosure. In addition to the technological complexity, this strategy will require a great deal of education of patients to explain their options and the limitations of the system.[9]

The opt-out idea is meeting with strong opposition from the health care industry and the research community, which find it impractical and especially troublesome. Arguing that this approach should not be necessary if all information is sufficiently protected, providers and managed care organizations claim that individual decisions to opt out would weaken their ability to provide high-quality, well-coordinated care in a cost-effective manner; they would not be able to easily track the care of those patients who are not in the computerized system, share information about patients, or get access to information about them on a timely basis. Providers also worry that members of the groups that could most benefit from the results of studies made possible by computerized information might be the ones who refuse to share their information. Researchers argue that an opt-out provision would limit their ability to conduct population-based research. The results of a study based on computerized medical records may be biased, inconclusive, or seriously flawed if the information about the population is not complete (for example, if it does not include all those who should be in the sample or if individual records are incomplete, thereby limiting the ability of researchers to address complicating factors). For instance, a study of the health status of all adult women would be missing a significant segment if a number of people with similar characteristics—say, young women diagnosed with HIV—opted out, and there would be no way for researchers to identify and adjust for their absence. Those favoring the right to opt out counter these arguments by noting that researchers can still do controlled studies (in contrast to population-based research) and that those patients who most need care want to participate in clinical research trials and are unlikely to deny access to medical records.

While they may oppose such a strong enforcement of individual rights, providers and researchers insist

that they are not turning a blind eye to the problem but simply want to propose an alternative approach based on security rather than on privacy principles. That is, they claim that patients would not feel a need for total control over access to records if they knew that security measures were in place to protect the information from inappropriate use and that anyone breaching patient confidentiality would be subject to substantial penalties. Advocates counter by pointing out that this approach assumes that all violations will be caught before they result in any harm, whereas their strategy enables patients to be proactive in protecting their data. From a policy perspective, industry representatives also argue that the problem here is not one of confidentiality but of fear of discrimination. Rather than denying access, the industry would like to see strong prohibitions of any use of personal health information—whether computerized or not—for discriminatory purposes. They also point out that when all information is not treated the same, the fact that information is missing in itself raises flags.

This response is echoed in the industry's position vis-à-vis a second meaning of segregation, which also refers to the idea that the law would treat dissimilar kinds of information differently, possibly by providing stronger protections for more sensitive information. The pressure for this kind of proposal comes from the various consumer groups seeking special protections for certain kinds of data, such as HIV status, alcohol or drug dependency, and genetic information. However, most advocates and industry representatives agree that they want not different categories of information and protection but strong protections for all information.

One problem is that the proposed solution (that is, special treatment for certain kinds of information) can inadvertently create new problems by revealing the information; for instance, in states where HIV status does not have to be disclosed without a court order, the provider is revealing the patient's status simply by asking for the court order. Segregating genetic information also presents problems. Many people claim that most health information, such as family history, can be considered to be genetic, so how would legislation differentiate between genetic and non-genetic data? The current controversy surrounding the use and disclosure of genetic information, such as a predisposition to breast cancer, illustrates an additional complexity: are some pieces of information more valuable than others?

A number of stakeholders on all sides concur that the concerns raised by specific kinds of sensitive information should be addressed through laws that mete out strong penalties for using such information for discriminatory purposes. (HIPAA makes some progress toward reining in discrimination by requiring that insurers offer coverage despite preexisting conditions, although the costs of that coverage may be prohibitive.) Also, although the genetic issue is politically "hot," few parties want to handle it as a separate privacy issue, if for no other reason than to maintain uniformity in the treatment of medical records (that is, they do not want different rules governing the same records). With anti-discrimination laws in place, the health care community believes that it can address other concerns by restricting disclosure and use of identifiable information and implementing strong security measures for all records, regardless of what media are used to create, transmit, and store the data.

Conducting Research

While no one would argue with the importance of health care research, everyone seems to be debating the need to balance the social benefits of health research with the social good of personal privacy. The differences in opinion revolve around the need for patient consent in the context of identifiable information. Despite the paucity of evidence to support fears of abuse or misuse of personal information, some believe patient fears and mistrust may pose a threat to the accuracy and completeness of the information contained in medical records.

At the same time, it is important to acknowledge that the common use of non-identifiable information is not considered controversial from a privacy perspective. The issue is the identification of the individual more so than the ability to access health information. Questions are often raised regarding how to make records anonymous so that no one can determine the identify of the subject. But to a large extent, this is a technical question rather than a legislative problem, since there are ways to control what can and cannot be seen in a computerized medical record.

In the context of identifiable information, however, the privacy advocates universally favor requirements for informed consent by the subject. Some point out that privacy protections may actually benefit the research community because people may feel more free to make their information available. In addition, the trade-off between confidentiality and research may not be as significant as it was thought to be, because developing technologies strengthen both by improving access to information and making it increasingly possible to "anonymize" data. Finally, privacy protections offer

value to the research community to the extent that they facilitate the flow of data internationally; again, by October 1998, American health care organizations that do not adequately protect personal data will not be able to access information maintained in member countries of the European Union.

But researchers claim that the process of obtaining informed consent for every subject is inefficient. For instance, as required by Minnesota law, the Mayo Clinic has embarked upon an extensive and costly effort to get consent from all of its patients. According to a recent article in the *New England Journal of Medicine,* researchers at Mayo found that less than 5 percent of patients objected to the use of their data for research purposes.[10] In some cases, where patients are dead or out of contact, getting consent is impossible. Finally, informed consent requirements threaten to degrade the quality of large databases due to missing data. As noted earlier, problems arise if that 5 percent who declined consent represent a significant cluster, such as all of the people with a particular disease relevant to the study. In that case, omitting this group from the research could have an impact on its validity or integrity. Of course, it is possible that data could be missing now because people are afraid to share information.

The overriding concern of those in the research community is that any federal legislation will be overly strict or narrow. Already subject to numerous requirements, they fear that new legislation would add layers of regulations over the process already in place but would not add meaningfully more protections. Those engaged in DNA-based research are especially concerned about their ability to use preserved samples for secondary research beyond the use for which the samples were obtained; others are worried about their ability to conduct follow-up studies after a drug is approved, should they need to track patients over time. Not wanting to limit this kind of research, the pharmaceutical industry argues that general consent of the subjects—who often cannot be located again—should be good enough. Fortunately, much of this information is not identifiable. But privacy advocates counter that, unless the original consent was sufficiently broad, the subject's consent should be required for identifiable information.

The research community also argues that research itself is not the source of abuse and that advocates are overblowing the extent to which individuals care. Expressing concerns about the practical and financial burden that consent requirements would place on the research community and on the individuals who would have to authorize uses and users, researchers claim that such legislation could hinder useful investigations, which would not serve the interests of individual patients or the general population. They also stress that different kinds of research require different levels of information protection. Rather than lumping all research into one category, they want to discuss how to apply the law fairly to different kinds of researchers—such as public health, private, university, government, provider-based, and health plan-based—and different kinds of research—such as epidemiological, clinical, outcomes, and disease management. Some segments of the medical community disagree with this approach: Mental health organizations, for instance, believe that identifiable information related to mental health should not be available for research without specific consent. But other providers argue that access to such information is necessary to understanding what is happening to the research subject.

The research community's position is essentially that the use of information for research purposes requires that society make trade-offs between individual privacy interests and the need for sound information on medical and public health issues. Because of the nature of the clinical and epidemiological research process (for example, the need to link records from different sources or follow up with subjects), it is simply not possible to "clean" records perfectly and still retain all useful data. Therefore, identifiable information is sometimes necessary.

The question thus becomes how to determine the necessity of using identifiable information for this purpose and under what circumstances the requirement for consent may be waived. Some industry experts have suggested expanding the use of institutional review boards (IRBs), which are organizations established both within and outside of health care institutions to decide whether the use of identifiable information is critical and unavoidable. Under IRB regulations promulgated in the 1980s, researchers are already subject to informed consent requirements for clinical trials. If the research is federally funded, the institution with the grant must use an internal IRB to review and oversee trial design and methodology to ensure that participants are protected; if the research is non-federally funded, the organization must contract with a commercial IRB. For records-based research, researchers are exempt from the regulations if the project is totally anonymous; if not, they can get a waiver giving them the right to use identifiable information without consent only if they meet specific criteria (for example, the research poses minimal risk to the subjects, will have no adverse

effects, and cannot be done without the waiver). Privacy advocates point out that the waivers do not typically consider privacy risks.

The IRBs are already overtaxed, so it is not clear whether they can take on responsibility for even more studies. In addition, while the quest for IRB approval would succeed in forcing clinical researchers through the requisite number of hoops needed to maintain confidentiality, it would have no impact on inquiries that do not meet the formal definition of research but use the same techniques. These are common and becoming increasingly more complex. If, for example, a hospital administrator chooses to investigate the cost-effectiveness of its clinics, there are no restrictions on that person's access to the institution's records, other than policies adopted by the hospital itself—which vary from institution to institution.

In its recommendations, DHHS has taken a status quo position with respect to research. The recommendations reflect a view that, assuming no harm to the individual, the social good of research outweighs privacy rights. Surprised by some misunderstandings of the likely impact of the secretary's recommendations on this topic, administration representatives note that, as a research agency itself, DHHS is unlikely to propose anything detrimental to the research community. However, for some people, the department's research responsibilities raise the question of whether it can be unbiased on this point; some advocates argue that the oversight of health information confidentiality issues should reside in a separate and independent authority that has no stake in the outcome.

The use of personally identifiable information for research is expected to be a controversial issue for Congress; while no one can point to specific abuses or violations, some people question why researchers need identifiable information once they have linked files and "anonymized" the records. Since the effects of the status quo on individuals are not yet clear, this area is likely to require more investigation before legislators will be able to make informed policy decisions. Some states have dealt with the issue by saying that consent is revoked automatically after a certain number of days. But the research community claims that this imposes too much pressure on researchers and distracts them from their work. That said, this is one situation in which technology is likely to come to the rescue; the ability to maintain records in electronic form will make it much easier to protect the privacy of subjects because no one will have to leaf through entire medical records to find specific information and, for some purposes, researchers will be able to easily use arbitrary identifiers rather than names.

Most stakeholders agree that the public health and research communities must take responsibility for conducting an education campaign that helps consumers make informed decisions by explaining how their research benefits the public and how sharing personal information allows them to achieve socially valuable goals. They also have to do a better job of explaining how they use information and how they protect it. The current controversy makes it clear, however, that the industry will also have to fix the system to protect the confidentiality of information and show evidence that their systems are secure.

Those seeking to resolve the controversy suggest that, in addition to public education, system fixes could include incentives for an increased reliance on non-identifiable, coded, or encrypted information whenever possible; a broader application of the federal IRB requirements; and strong sanctions for violations of confidentiality.

Allowing the Use of Information beyond the Realm of Health Care

For many people, the threat to personal privacy arises not from the use of their information in the context of health care delivery but from the many uses that occur outside of that realm. As noted earlier, health care data are made available for a number of purposes, such as law enforcement, employment, marketing, public health, and oversight, that have nothing to do with delivering personal health care. This raises obvious questions about how to protect the confidentiality of information that passes into the control of secondary and tertiary users. The dilemma lies in determining what the legitimate uses of information are, how they should be authorized, and how they should be limited. Since it is not possible to do justice to each of the possible uses of identifiable health data, this section illustrates the issues at stake by focusing on the two uses that evoke the strongest reactions and arguments: law enforcement and employment.

Law enforcement. At present, law enforcement agencies enjoy fairly easy access to personal health information, although some state laws do impose limited restrictions. From the perspective of both privacy advocates and the health care community, this ease of access by law enforcement authorities is far and away one of the most contentious and challenging issues that will have to be resolved through legislation.

This is also a difficult issue for the administration, as illustrated by the fact that it is the primary area in which the secretary's proposal differed from the recommenda-

tions of the National Committee on Vital and Health Statistics, which had been tasked by HIPAA with providing advice to DHHS on how to proceed in the privacy arena. It is also the area in which the proposal met with the most vocal objections. The recommendations were criticized for allowing law enforcement officials wide authority to access patient records for investigations or prosecutions.

Administration officials emphasize that the secretary's recommendations were not intended to be any less restrictive than current law—despite the way in which they were portrayed in the media. The current law has no specific requirement for providers to cooperate with law enforcement authorities; any provider can refuse to submit a requested medical record unless and until the authorities obtain a court order. That said, others argue that the absence of constraints on information access and use for law enforcement purposes is inconsistent with the restrictions imposed on all the other parties who can be said to need this kind of data to operate effectively.

Those who must deal with requests from law enforcement officials on a regular basis want to limit the accessibility of the information by putting in place a standard process requiring a warrant or subpoena as well as notification of the subject—which would enable the patient to seek to quash the subpoena before the information is released, rather than finding out about it after the fact. Advocates point out that privacy bills in other areas (such as financial records and video rentals) have offered protection from the free rein of law enforcement agencies by (*a*) setting up procedural requirements for anyone wanting the information, (*b*) establishing standards for determining that information disclosure is necessary, and (*c*) placing limits on the use of the information.

Employers. Some polls suggest that what members of the public are most concerned about is having data used against them, particularly by employers. Currently, many employers have access to a great deal of health-related information, sometimes because of workers' compensation or employee assistance programs but most often because they are self-insured, which means that they—rather than an insurer—are financially responsible for paying the medical claims of employees and their families. Like insurers, they are entitled to review medical data for the legitimate purpose of settling claims and administering benefits; the problem arises if that information is used to discriminate against people in the workplace. There have been cases, for instance, in which employees claimed to have been denied promotions or even fired because their positive HIV status became known to their supervisors.

Employers, whether self-insured or not, also may gain access to health information to the extent that the employees's health status is relevant to the ability to perform a given job. While the Americans with Disabilities Act (ADA) affords certain protections, experts in this area argue that it is an inadequate deterrent against the misuse of voluntarily provided information.[11]

Although few employers would publicly admit to using personal information, the health plans that administer coverage on their behalf indicate that requests for data are commonplace. Participants in recent meetings of provider and health plan associations suggest that some health care organizations are favoring a statutory change that would prohibit employers from demanding personal information.

Some employers have reportedly used health information in making hiring decisions. Several states have tried to deal with this issue by denying employers the right to ask for genetic information, but that raises the issue noted earlier regarding the fine line between genetic and non-genetic information. In an effort to avoid that debate, Minnesota enacted a law that states that prospective employers may ask only for information specifically related to the functions of the job for which the applicant is being considered, thus drawing a distinction between job-related information and unrelated information. For instance, an applicant for a job that requires heavy lifting may be asked for an orthopedic history, but not for a complete medical record. Unfortunately, it can be difficult to provide segments of a medical record when the information is maintained in paper form, but this obstacle vanishes when data are kept electronically. One expert pointed out that the easiest way to protect the confidentiality of health information in this context may be to amend the ADA to say that prospective employers may request only health information that is job-related but predicted that this option would be politically impossible.

As with most issues regarding patient confidentiality, employer access to personal health information becomes more complex as the uses of this information become more visible. While most agree that employers should be prohibited from using the information for hiring or firing decisions, determining "appropriate" uses for employers can be more problematic. For example, an employee's HIV status should be irrelevant to an employer, but when the employer also acts as the payer of health care services, the patient's condition

could determine appropriate treatment. If, for example, a routine outpatient procedure should be performed in a hospital due to the patient's HIV status, the payer needs to know this information to make the correct coverage decision.

At the same time, many large employers are moving more aggressively to implement worksite disease management strategies for a variety of conditions ranging from diabetes to depression. They argue that these strategies will provide patients with information and treatment that will lessen the severity of illnesses. Privacy advocates, on the other hand, fear that employers who gain access to disease-specific information may use it against their employees.

Most experts in this area agree that this issue calls for two kinds of legislative action: first, Congress could take steps to erect strong protections for the health information legitimately possessed by employers. The chief component of such protection would be requirements for a "firewall" between the medical records maintained by benefits staff and the personnel records maintained by management staff, as well as serious penalties for violating confidentiality. The second action relates to strengthening anti-discrimination laws to discourage the use of such information for inappropriate purposes.

Preempting State Laws with a Federal Bill

The final key issue that Congress will have to resolve is whether federal law should preempt existing state laws. At present, state laws related to health information confidentiality are not uniform; some have strong and well-enforced protections in place, while others have very few or very weak rules. The problem posed by this patchwork quilt is that many participants in the health care industry cross state lines or contract with vendors and other organizations in multiple states, which makes it difficult for them to determine what law is controlling. Corporate headquarters, for instance, may not be where the patient is, and the patient may not be where the information is stored.

The question of preemption is likely to be difficult to legislate. Given few areas of agreement and strong merits to the arguments on both sides, it will be quite a challenge to strike a balance between valid but competing interests.

In essence, the preemption issue revolves around whether to set a floor of minimum standards for privacy protection, which individual states could exceed, or to establish a "ceiling" of high standards that everyone must meet but could not be required to exceed by the states. Neither privacy advocates nor the Clinton administration are in favor of broad preemption, partly because some of the existing state laws are very well crafted. Most elements of the health care industry, on the other hand, favor federal preemption—with privacy protections high enough to relieve people's fears and low enough to be workable—because it would give them a single set of rules to follow. Monitoring legislation and tailoring activities to 50 different legal environments can be expensive. Multistate enterprises are also concerned about the complexity of implementing the requirements of a federal law in the absence of preemption.

Not surprisingly, most providers (such as group practices) are not nearly as concerned about the preemption issue as are the national health plans, pharmaceutical companies, and big hospital systems that would like to see standards on a national level. The many payers that operate in multiple states, for instance, have indicated that they would be unwilling to support a bill that does not include preemption of state laws. They want standards that would allow information to flow through the system as it does now, but with punishments in place to keep people from flaunting the law. In recognition of the public's demand for extra protections for particularly sensitive information (such as HIV status, mental health problems, or substance abuse history), some in the industry suggest that the federal legislation could be modeled after the strongest state laws. This is consistent with the views of some provider organizations, which do not want people to be left with less protection than they already had under state law. On the other hand, this "high ceiling" approach to legislation creates a possibility that researchers will not be able to obtain information they need; as a result, members of the research community want to ensure that legislators understand what kinds of research could be lost under different scenarios.

Once again, the dissenting voices come from the public health and mental health communities, which feel strongly about imposing a floor of minimum requirements that establish rights and duties for all parties across state lines, while also preserving the ability of states to pass stronger laws; at the very least, they want to incorporate some exceptions into a federal preemption. The problem with specifying exceptions, however, is that it is very complicated to identify what individual states are doing to protect mental health information, since they can do so through statute, common law, licensing requirements, and other means. Moreover, isolating mental health information from an

individual's medical record can have unintended consequences. For example, if a primary care provider is unaware a patient is being treated for depression, he or she may prescribe inappropriate treatment or medication. Also, if mental health information is the only information that is isolated or handled differently, it would be possible to reveal personal information about a patient simply by refusing access to the full record.

It is important to recognize that federal preemption is unlikely to cover everything; for instance, virtually all stakeholders agree that preemption should not interfere with public health functions, which should continue to be the responsibility of the states. In addition, a statute would preempt only those laws that pertain to patient confidentiality in the context of the flow of information for specific activities; for example, issues such as communications with next of kin would not necessarily be covered by this kind of law.

Moreover, preemption does not have to be absolute. One option that has been proposed is to preempt all state laws except those that protect mental health and public health issues—although it would likely be difficult to determine which laws qualify. Some experts have suggested that the legislation could preempt only those laws dealing with uses of information that are truly in the national interest, such as investigations of fraud and abuse in health care.

Conclusion

This paper presents the issue of health information confidentiality in terms of the need to strike a complex balance of competing interests. In some cases, the interests and values of privacy can complement the interests and values of health care delivery, including research, by minimizing patients' anxieties about the potential misuse of their information. But in others legislators will have to make hard choices that favor one set of values over the other.

ENDNOTES

1. P.L. 104-191, Section 164. Available: http://aspe.os.dhhs.gov/admnsimp/pl104191.htm, February 26, 1998.

2. William W., Lowrance, "Privacy and Health Research: A Report to the U.S. Secretary of Health and Human Services," Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services, Washington, D.C., May 1997. Fact Sheets Nos. HC 3.1-3.5 explaining the Health Information Privacy Code 1994, issued by the Privacy Commissioner of New Zealand, June 1994. Available at http://www.knowledge-basket.co.nz/privacy/health/hc0.htm, March 3, 1998. David H. Flaherty, "Privacy and Data Protection in Health and Medical Information," presentation of the Information and Privacy Commissioner of British Columbia to the 8th World Congress on Medical Informatics, July 27, 1995. Available at http://www.oipcbc.org/publications/presentations/health.html, March 3, 1998.

3. Louis D. Brandeis in his 1928 dissent in the first wiretapping case to reach the Supreme Court: "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the 4th Amendment." *Olmstead v. United States,* 277 U.S.438 (1928).

4. Health Privacy and Confidentiality Recommendations, National Committee on Vital and Health Statistics, June 25, 1997, 5, 6.

5. The concept of a "code of fair information practices" was recommended in early studies of privacy and is embedded in the Privacy Act of 1974. It is also derived from several sources, including codes developed by the Department of Health, Education, and Welfare (1973); Organization for Economic Cooperation and Development (1981); and Council of Europe (1981).

6. U.S. Department of Health and Human Services, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, (Washington, D.C.: DHHS, 1973).

7. Janlori Goldman and Deirdre Mulligan, "Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality," Center for Democracy and Technology, Washington, D.C., 1996.

8. Telephone interview with Kathleen Frawley, J.D., M.S., R.R.A., vice president, legislative and public policy services, American Health Information Management Association, January 6, 1998.

9. Telephone interview with A.G. Breitenstein, JRI Health Law Institute, November 23, 1997.

10. L. Joseph Melton III, "Sounding Board: The Threat to Medical-Records Research," *New England Journal of Medicine,* 337 (1997), no. 20: 1466-69.

11. Telephone interview with Mark Rothstein, professor of law, director of Health Law and Policy Institute, Law Center, University of Houston. November 24, 1997.