MEDICAL PRIVACY AND CONFIDENTIALITY

Policy Issue Analysis 1998

Table of Contents

MEDICAL PRIVACY AND CONFIDENTIALITY

Executive Summary

Strategic Health Policy International, Inc. surveyed health care industry policy players to determine the level of knowledge, concerns and involvement in issues of medical privacy and confidentiality. It is clear from this assessment that the factors that drive national policy decisions are in place and shaping up for what may well be one of the most complex and contentious policy debates since the Clinton Health Reform. While many people will agree to principles of medical privacy, the specific programmatic implementation of those principles will generate considerable controversy. All three branches of the Federal Government, but particularly the Legislative, will have the greatest role in shaping this issue in the future. It will serve as the field on which all of the players will jockey for position and wage political warfare.

The environment is only being shaped in a way that will predict the players and point to possible outcomes. The outrage in the media and among the public about the recent CVS/Giant/Elensys pharmaceutical compliance and marketing program was built on a foundation of increasing concerns for patient rights and privacy. Beginning in 1995 with the European Directive on Data Privacy, Congress has been spurred to recognize privacy protections as an issue. The passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) placed a privacy protection deadline on the Congressional calendar. Individual states pressed ahead, not waiting for national legislation and proposed and passed a patchwork of record-protection legislation. President Clinton's Commission on Patient Rights echoed concerns and established medical privacy as an important right, but one that balances with responsibilities. Congress is beginning to act, and bills are now introduced in both Houses.

This study included reviews of literature and discussions with important players to examine the policies and politics of different factions likely to engage in the warfare. We have learned that it is far too early to predict the outcomes, but we have determined that the most likely battles will be in six areas:

- What will be collected, in terms of data and how will it be used?
- How will data be managed to preserve privacy and confidentiality?
- What rights will patients have to view and correct medical records?
- How will lines be drawn to require consent and prior authorization?
- How will intentional and unintentional violations be punished?
- Will federal laws preempt state laws?

Our analysis is one of *breadth* rather than *depth* at this stage. It is our belief that this arena will become increasingly active, will create additional opportunities for attacks on health

providers (particularly in pharmaceuticals), that the Congress will miss its HIPAA deadlines and that the medical privacy may well become an election issue because of the health care, civil rights, Constitutional protections and States rights issues it engenders. In the midst of the nature of the risks, this issue should be one of careful consideration for health care providers.

Background and Definitions

Real examples of medical privacy violations demonstrate the risks that some people have already experienced when private medical data is made public. For example:

- The medical and mental health records of a congresswoman from New York were faxed to a local newspaper during her campaign.
- A Massachusetts HMO kept extensive notes of psychotherapy sessions on a central computer, accessible to all clinical employees.
- Sales representatives of a managed care company in Maryland were able to purchase, illegally, computer records of Medicaid recipients from Medicaid clerks.
- A purchaser of a second-hand computer discovered that the hard drive contained a grocery store's pharmacy records including patient names, addresses, Social Security numbers and prescription medicines.
- Members of U.S. Congress, at the start of the AIDS epidemic, threatened to embarrass AIDS patients and leverage anti-gay sentiments at that time by reading medical records of AIDS patients treated at the National Institutes of Health Clinical Center on the floor of the Congress.

The Center for Democracy and Technology proposes that "privacy encompasses the values of individual autonomy, freedom and dignity. Individuals invoke privacy when they seek to retreat from the outside world; keep thoughts, actions, words, and facts out of the public eye; and limit the disclosure and use of personal information that they have given to another person." Webster's Third International New Dictionary (1976) defines confidentiality as "communicated, conveyed, acted on or practiced in confidence, known only to a limited few, not publicly disseminated." Privacy, in other words, is the right to keep some information secret from others. Confidentiality is the protection that is afforded that otherwise secret, sensitive and personal information from disclosure. For example, the right of privacy ensures that when patients provide blood samples for routine laboratory testing those same samples will not be used to assess HIV status, to conduct genetic tests or to determine illegal drug use for employment or law enforcement purposes without the patient's permission. The right to confidentiality assures that once the patient has agreed to those tests, that the information is maintained and used only by those deemed by the patient to have reason to use that information for his or her benefit.

The earliest health-related privacy legislation was the Federal Privacy Act of 1974. This act allowed individuals rights to medical files maintained by federal agencies. Individual agencies were allowed to establish additional policies if they believed there was a need and

many agencies, such as the Public Health Service (PHS) in the U.S. Department of Health and Human Services (DHHS), did just that. The law had no impact on medical records in the private sector.

Throughout the '80s the DHHS continued to study medical privacy issues and react to privacy policy as needed (as in the case of the threatened Congressional subpoenas of patient data from the NIH Clinical Center mentioned above), but the next major effort of the Department was in the testimony of Secretary Donna Shalala before a Senate Committee on Labor and Human Resources on September 11, 1997 concerning the DHHS response to the HIPAA requirement that national uniform privacy policy be developed either through legislation or regulation.

Forces Shaping Public Policy in Medical Privacy

Three principal driving forces shape national government action on any topic of debate: policy, politics and precipitating events. It is *policy* that creates the "way" or the direction that decisions or actions will take. It is in policy debates that we identify problems, define the terms and limits of the debates and seek solutions. It is *politics* that creates the "will" or the energy for change. Politics establishes those who have the power to enact the changes that come from the policy-level considerations. It is *precipitating events* that "catalyze" the interaction between the other two. Precipitating events are those forces outside the policy and political arenas that force change because they are so extraordinary or pervasive that they cannot be ignored. Issues related to medical privacy are no exception. Medical privacy is increasingly a topic of discussion—though not yet a topic of widespread debate—precisely because those three driving forces are ripening. As we will describe here, those forces have not yet crystallized sufficiently to produce the kind of focused, national debate that will shed light as well as heat on the issue, but we predict that they are lining up and momentum is gaining daily.

In the case of medical privacy, a set of precipitating events are already numerous and growing. Some precipitating events are found in the actions of other governments, whose policy decisions will affect the commercial operations of American business. Some of these precipitating events are found in the violation of personal medical privacy that have been reported in major news stories of the past year. These events will provide the examples to consumer activists and politicians alike to demonstrate the need to move forward with legislation or regulation. Particularly in the upcoming Presidential Election cycle and its projected focus on health care and patient rights, we anticipate that breaches of privacy and confidentiality that might otherwise have gone unnoticed will become rallying cries for tough protections and tougher sanctions.

Unfortunately, the level of understanding of privacy and confidentiality issues within the health policy community is limited. Few organizations are well enough acquainted with the issues and the implications for their members' operations to participate in a reasoned policy

debate; many look to coalitions comprised of similar organizations for expertise and leadership in this area. In the course of this assessment of data privacy policy, we identified 50 key associations that would be players in the national policy debates. Of the 41 associations that responded to our requests for interview, only one-quarter of the groups had formulated any policy position on privacy; one-third were tracking the issue and formulating policy; and the remainder were either unaware of this issue or aware but unconcerned about its impact on their organization or its members. In addition, we could identify only a few coalitions and think tanks that have taken the lead on this issue, taking a hand in writing proposed legislation and authoring much of the debate. The majority of the organizations we surveyed knew about the issue and its importance, but few were ready to subscribe to any specific legislative initiative.

The same "watchful waiting" is occurring among those players with political portfolios. With few exceptions, political players—at each end of Pennsylvania Avenue and on any side of Main Street—have yet to declare their positions and intentions. It is our assessment that politicians are waiting for more data, clearer signals from their voting and special interest constituencies and greater demonstration of need before they step into what may well be the next major civil rights battle.

Policy Force: Precipitating Events

In today's high-technology, information-driven, managed care environments, confidential health, and medical data is collected, stored, analyzed, distributed, and accessed for many different purposes by many different entities. Innovative, high-capacity technology, coupled with increasing health care costs and demands for accountability, creates a thirst for patient medical information to address everything from patient registration and recall systems to clinical encounter recording, clinical disease management, claims processing and payments and contract negotiations. This unprecedented demand for health care data creates concerns about the erosion of medical privacy in the minds of both consumers and providers.

These opportunities and the need for data have captured the attention of legislators at state, national and international levels. A number of key events have focused on issues of patient privacy and are about to bring them to the forefront of politics and legislative initiatives in the coming months:

European Directive on Data Protection. In 1995, the European Parliament and the Council of the European Union (EU) issued a directive that will take effect on October 25, 1998. This directive is a widespread privacy policy for each EU member nation. A section of this policy will prohibit electronic transfer of personal information about European citizens to countries with privacy protection laws that are deemed inadequate by the EU. As a result, unless the U.S. develops and implements privacy protections that meet the requirements of the EU, some U.S. companies with European operations could find their commercial

activities disrupted by the inability to transfer information. For example, pharmaceutical companies conducting clinical trials in Europe for submission to the U.S. Food and Drug Administration for drug marketing approval could have difficulty transferring information on European citizens to the U.S. for analysis. The EU Directive does allow for some industry-sector exceptions if the industry has self-imposed privacy protections. Knowledgeable observers agree that the pharmaceutical industry will develop those protections, so it is unlikely that pharmaceutical operations will be disrupted. The fact that such a Directive was passed by the EU is indicative of the seriousness with which the Europeans have deliberated on the issues of individual privacy.

Health Insurance Portability and Accountability Act of 1996. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress must enact healthcare privacy and confidentiality legislation by August 1999. This provision was intended to ensure that as Congress created more access to care through coordinated services it protected patients from unauthorized disclosure of personal data. Included within HIPAA are three recommendations related to individually identifiable health information:

1) The rights that an individual who is the subject of individually identifiable health information should have,
2) The procedures that should be established for the exercise of such rights, and
3) The uses and disclosures of such information that should be authorized or required. (HIPAA, Sect. 264)

If Congress fails to pass legislation by August 1999, HIPAA requires that DHHS promulgate healthcare privacy and confidentiality regulations regarding the handling of electronic records.

Also, under HIPAA, health care system providers and payers must adopt uniform information transaction standards and use electronic health information data systems to process transactions by February 2000. Fully computerized data systems will allow instantaneous access to each patient's medical information. With movement toward national electronic health care information systems, incorporating clinical data will become more visible. Even the progress towards implementation of this HIPAA provision will generate opportunities for broader policy-focused debates.

Department of Health and Human Services. In September 1997, DHHS Secretary Shalala issued a report recommending that Congress enact those national standards called for in HIPAA that provide fundamental privacy rights for patients and define responsibilities for those who serve them. This report was based on a study commissioned in 1996 to analyze the implications for the U.S. of the new European Union Directive and related policy and legal changes. It was intended to serve as the basis for recommended policy and a technical approach to ensuring privacy, as research proceeds to enhance the health of the public. An earlier draft of the report was met with objections from the Department of Justice, principally because the report appeared to restrict its access to medical information. Unable

to reach a consensus within the Administration, DHHS is encouraging Congress to enact legislation, and in doing so, shifting the focus for resolving differences of opinion in medical privacy rights to the legislature. Key to the handling of prescription information, this report recommends that Pharmaceutical Benefit Managers (PBMs) be prevented from selling patient prescription data to pharmaceutical companies.

CVS/Giant Pharmacies & Elensys, Inc. On February 15, 1998, and again on February 18, 1998, the *Washington Post* published front page stories on an agreement between CVS Corporation, Giant Food, Inc. pharmacies and Elensys, Inc., a Massachusetts firm that manages electronic records and provides services to support prescription drug compliance. The article reported on a Glaxo-Wellcome-supported program, similar to others in the industry and in place in pharmacies across the nation. This widely publicized story led readers to believe that Glaxo-Wellcome had access to patient records, although they did not, and sparked a debate on the issue of patient privacy related to medicines. Giant Food Inc. and CVS, Inc. officials responded to the deluge of complaints from customers by limiting or severing their relationship with Elensys, Inc.

Consumer Bill of Rights & Responsibilities Deliberations. In late 1997 and early 1998, the President's Advisory Commission on Consumer Protection and Quality in the Healthcare Industry resulted in recommendations to the President on medical privacy and other matters. As a result, President Clinton proposed a Consumer Bill of Rights and Responsibilities, now proposed in Congress as HR3605 by Congressmen John Dingell (D-MI) and Richard Gephardt (D-MO) and as S1890 by Senators Thomas Daschle (D-SD) and Ted Kennedy (R-MA). These bills propose other patient rights, including access to needed health care providers, access to emergency services and allowances for grievance and appeal processes, but also include privacy and confidentiality provisions. Under the bill, individually identifiable information could be used without written consent, with very few exceptions. In return for "rights," including access to and payment for healthcare, patients are deemed to be willing to exercise some "responsibilities", including relinquishing some personal privacy. Therefore, permitting the availability and use of identifiable information is one of the "responsibilities" of the patient.

State Legislation. Finally, states have increasingly considered privacy and confidentiality legislation in the course of their legislative calendars in recent years. In the 1998 Legislative sessions, more than 250 bills have been introduced in the States, 63 have passed at least one house and 7 have been enacted. As States proceed with their own considerations of medical privacy, there is the potential for disruption of interstate commerce and the internal business interruption of companies, including in health care, with research and commercial operations that require the interstate transfer of information. This disparate State activity alone will drive the need for a Federal-State debate on the preemption of State law by Federal policy.

Policy Force: Key Policy Issues and Principles

It is likely that two elements will frame the key policy issues that will be a focus of future debates. The first is a set of principles developed by DHHS Secretary Shalala in her 1997 report on medical privacy (mentioned above). The second is a set of the practical and programmatic considerations that must be considered in the collection, use and management of data.

Shalala Principles. The 1997 DHHS final report, as amended to account for inter-Administration policy conflicts, established principles for medical privacy. These principles related to boundaries, security, consumer control, accountability and public responsibility:

- ***Boundaries Principle***. This principle states that an individual's health care information should be used for health purposes and only those purposes, subject to a few carefully defined exceptions. It should be easy to use information for those defined health care purposes, and very difficult to use for other purposes. Four situations arise in which health information is collected, disclosed, or used and should be addressed by Federal health privacy legislation. First, provision of and payment for health care should be dealt with in terms of a uniform privacy law, regardless of the location where services were received. Information obtained for payment purposes should only be used for this payment transaction and all other requests should require further disclosure legislation. Second, all entities working within healthcare, including service organizations, should be held to the same level of privacy restrictions. Third, limited disclosures for national priorities (such as public health research needs) should be allowed in order to balance national priorities for public health and personal privacy. Fourth, disclosure with patient authorization should be allowed.

- ***Security Principle***. This principle requires that organizations entrusted with health information should protect it against deliberate or inadvertent misuse or disclosure. Federal law should require security measures.

- ***Consumer Control Principle***. This principle gives patients the right to view their records, obtain copies, correct errors, and learn who has accessed them. DHHS recommendations significantly strengthen the ability of consumers to understand and control personal health information.

- ***Accountability Principle***. This principle requires that those who misuse personal health information should be punished. Those who are harmed by its misuse should have legal recourse. Federal law should provide new sanctions and new avenues for redress for consumers when privacy rights have been violated.

- ***Public Responsibility Principle***. In this principle, an individual's claims to privacy are balanced by a public responsibility to contribute to the common good through

disclosure of personal information for important, socially useful purposes. This would be done with the understanding that their information will be used with respect and care and will be legally protected. Federal law should identify those limited arenas in which our public responsibilities warrant authorization of access to medical information and should sharply limit the uses and disclosure of information in those contexts.

Practical and Programmatic Considerations in Medical Privacy. We have identified six practical and programmatic considerations we believe will be the focus of the national policy debates concerning medical privacy legislation or regulation. They include: 1) the way that data is collected and used, 2) the way that data is managed to preserve privacy and confidentiality, 3) the rights of patients to view and correct medical records, 4) the limits of consent and authorization to view records, 5) penalties for intentional and unintentional breaches of privacy rights, and 6) the degree to which federal government policy will preempt policies of the States.

- ***Data Collection and Use***. Patient medical data is coveted by a number of entities. Managed care uses information to track utilization and structure negotiations with payers and physicians. Insurance companies use the information contained in medical records to determine treatment and/or claims coverage. Pharmaceutical companies partner with physicians, pharmacies and hospitals to create compliance with drug regimens and to support product marketing. Courts subpoena medical records for use in competency hearings and custody determinations. Employers use health data about prospective employees to make hiring decisions and occasionally to make promotion and placement decisions.

  The policy-level debates concerning data collection and use address:

  - What data will be collected? Who will be allowed to collect it?
  - What existing personal identifiers will be collected (or what new identifiers will be created) and how will those be "filtered" as they are transmitted to data users? Which personal identifiers should be filtered for specific purposes?
  - Who will determine the appropriate uses of data? What will those appropriate uses be? Even if the data is de-identified, will personal medical record information be used without the knowledge and consent of the patient?
  - What if patients must consent for medical records use in research? If some patients do not consent, will that invalidate population-based research and limit the utility of the database?
  - Will failure to grant consent create a new stigma for patients? Will it create the impression that the patient has "something to hide?"
  - Should law enforcement agencies be allowed to gain access to medical information?

- ***Data Management to Preserve Privacy and Confidentiality***. Privacy is the right of an individual to limit *access to* information about themselves. Confidentiality is a form of

protection of private information that the individual chooses to disclose. It is characterized by a special relationship between people (i.e. between physician and patient). Security encompasses *technical and organizational procedures* that protect electronic information and data processing systems from unauthorized access, modification or misuse.

Privacy, confidentiality and security are each an important focus in the medical privacy policy debate. Each is proving more difficult to manage as health care information moves over electronic networks, making it accessible to more people at widely scattered locations and institutions with different policies and procedures in place. Unauthorized uses of information by authorized users are difficult to monitor. Patients are usually unaware of how their medical information can be used, to whom it may be released and what rights they may have to access or correct it, particularly once it is in the hands of a secondary user.

The policy-level debates concerning privacy, confidentiality and security will address:

- Does a patient have a right to privacy in all medical matters? For example, can a hospital or insurance company order HIV or genetic tests on blood samples collected for other purposes without the consent of the patient?
- Must all patient releases be in writing?
- Once the patient discloses private information, how and where will data be maintained in order to assure security and confidentiality?
- Does the responsibility for maintaining security and confidentiality extend not only to a corporate entity storing the data (including providers), but also to all employees as individuals?
- Should penalties for violations be assessed to corporations or also the individual employees?
- Should criminal background checks for medical data storage operation companies (including provider groups) be required for all employees?
- Should data vendors and users be allowed to transmit data over the Internet?
- Should all those who store medical data be required to have a minimum level of system security, including passwords, authorization levels and audit logs?
- How frequently should passwords be changed? How long should audit logs be kept?
- Should the government outlaw certain types of encryption technology?
- Should government license data vendors and users? Should government limit the number of licensed data vendors and users to better assure security?
- Should ERISA companies providing healthcare coverage assure that medical information used in claims payment and medical benefits transactions are not available to company supervisors and managers of personnel?
- Should companies be allowed to require data disclosure to the company in return for medical benefits coverage?

- ***The Rights of Patients to View and Correct Medical Records***. Medical information—especially if automated—can be easily shared, altered and manipulated. Because personal data can be disseminated so easily, privacy advocates emphasize the need for information to be fully available to the individual patient to review, challenge and correct. This process is analogous to the viewing and correction of consumer credit records.

  The policy-level debates concerning viewing and correcting medical records will address:

  - Will patients be allowed to view and correct medical records, including psychiatric records? Should patients have access to diagnosis and prognosis information?
  - How long should a patient have to wait for a response to a medical records review request?
  - Should a patient be allowed to correct the record? What are the limits of the patient's ability to correct records? Will medical oversight be required if patients wish to alter diagnoses, for example? If a patient and physician disagree, who will prevail?
  - How will patients be allowed access to records? At the point of care? Within a data warehouse?
  - How often may patients correct the record? Should a patient be charged for accessing the records? For correcting the records?
  - If uncorrected records are shared and the patient later learns of inaccuracies and makes corrections, must corrections be shared with all prior data users?

- ***The Limits of Consent and Authorization***. Because privacy is a Constitutional right, advocates will most likely prevail in arguments that organizations making claims to information in an individual's medical record should be obliged to respect the wishes of that individual concerning the use of the information.

  The policy-level debates concerning consent and authorization will address:

  - How detailed should a consent form be? How many potential specific uses should be listed on the form? Should the consent expire? Should consent be periodically re-authorized? If so, how often? How should consent be revoked? Does consent extend beyond the life of the person?
  - Can a person refusing authorization for medical record sharing be denied care?
  - Should patients be allowed to withhold consent for data collection, sharing and use and yet be allowed health care reimbursement? Will capitation plans create more opportunities for patients to receive care and halt data disclosure at the doctor's door?
  - Should prisoners and military personnel be allowed the same consent and authorization rights as other citizens?
  - Should patient data release consent be required each time a patient's data is used?

- At what point does the patient grant consent, at the point of the medical service? At the point the information is transmitted to any user? When the data is re-sold or re-cycled?
- Should patients be compensated for the use of their information?

- ***Penalties for Intentional and Unintentional Violations of Medical Privacy***. Under HIPAA, a person who knowingly uses or causes to be used a unique health identifier to obtain individually identifiable patient medical information or who discloses this information to another person is subject to penalties. These penalties include fines of not more than $50,000 and imprisonment of not more than 1 year, or both. If this offense is committed under false pretenses, the fine is increased to not more than $100,000, and imprisonment of not more than 5 years, or both. If the offense is committed with the intent to sell the individual's information for commercial advantage, personal gain or malicious harm, the fine goes up to $250,000, and up to 10 years in jail, or both. In addition to high monetary penalties and incarceration, enforcement of state or federal health privacy laws may also include prohibition from further participation in the health care reimbursement under Medicare and Medicaid programs.

  The policy-level debates concerning penalties for violations will address:

  - What are adequate penalties for violations of security, privacy and confidentiality?
  - Should penalties be assessed at the federal level, the state level or both? Should civil penalty remedies also be available?
  - Should penalties differ for intentional and unintentional violations?

- ***Federal Preemption of State Laws***. A patchwork of State legislation in any arena creates difficulties in commercial activities conducted across State borders. The health data vendor and user industries already face those difficulties and, as a result, are proposing that the federal government preempt laws passed by State legislatures and enact uniform legislation to create a national environment to support electronic commerce and computer-based patient records unhindered by local differences in regulations.

  The National Conference of Commissioners of Uniform State Laws (NCCUSL), which assists the States in crafting laws that are consistent across State lines, attempted to address this issue with the States a number of years ago. In an effort to engage the States in joint of laws, NCCUSL sought greater consistency across the States, which would have avoided the need for federal preemption. The NCCUSL drafted medical privacy legislation in 1985 that has been passed in only two states. They are not active in this arena at this time, except to monitor State activity. It is unlikely that any effort they would mount at this time would prevent the move towards federal preemption already underway. The lack of NCCUSL effort in this arena increases the chances that federal preemption will be seriously addressed in the Congress.

While there appears to be a growing consensus among the various interest groups about the elements that will constitute a successful Congressional measure, there remains strong disagreement about whether a Federal law should supersede stronger State laws. This is the single most distinctive difference between the two strongest contenders for legislative passage to be drafted to date—SB1921 introduced by Senator Jeffords that would lay a "floor" and allow stronger state laws to stand, and a measure still to be introduced by Senator Bennett that would preempt all existing state laws.

Blanket generalizations are risky and inaccurate but, overall, it is true that providers and consumers favor stronger state laws taking precedence over a federal measure because it is easier to protect personal medical information turf with state laws. Data handlers, information systems professionals and researchers, on the other hand, prefer a single federal law that would facilitate the ease of use and protection of information in ventures that cross State lines.

The advantages of stronger state laws, according to proponents of that approach, are that they would allow for the differences in state populations and needs. For example, New York and California have a large HIV/AIDS population that some would argue might call for stronger protections than a state like Iowa, for which AIDS is not a great concern.

The advantages of a preemptive Federal measure are that federal law superseding all state laws would ensure that all data would be handled in the same manner. This approach would greatly reduce the errors that could result from confusion about the prevailing statutes that govern the confidentiality of certain bits of information. For researchers, whose projects frequently span the nation, all patient information would be protected in the same way. For multi-state health plans and employers, consistent rules would encourage compliance with laws regarding disclosure.

The policy level debates concerning federal preemption will address:

- Should laws passed by the U.S. Congress supersede existing State laws? (Many states currently have stringent laws concerning HIV, mental health, genetic testing, and these will be three main battle grounds.)
- Should a Federal law lay a "floor" on which States may overlay stricter laws?
- Should laws treat all classes of information with the same degree of confidentiality, or do some diseases or conditions require a greater level of security, such as HIV/AIDS, genetic information and mental health treatment?
- How will the conflict between state insurance regulation and federal privacy legislation be resolved?
- Will federal level penalties for violations suffice, or will state professional practice acts and licensing boards also have the ability to punish violations?
- Should data centers be regulated by State as well as Federal law?

Politics of Medical Privacy

Consumers, data users and commercial vendors of data and technology will drive the politics of medical privacy. In the course of this assessment, we contacted 50 organizations and succeeded in interviewing 41 of them about their positions, concerns and expectations regarding medical privacy, confidentiality and security legislation. Our contacts included a spectrum of interest groups that are monitoring and participating in medical privacy issues development. We targeted our interview efforts to the provider, consumer and research communities for this report. Each of those groups note that they and others, such as the criminal justice system, child welfare agencies and the commercial data sectors, all have varying stakes in how much and in what form personal healthcare data information will become available to them.

Consumer/Advocate Groups. The general public is still largely unaware of the issues in medical privacy policy and they remain unengaged in the early debates and is only very recently learning about the issue from the press. Most obvious and most active are the consumer groups for whom this issue cuts closest to the bone. These groups are comprised of people who identify strongly with a subset of the general population, either by virtue of their age (AARP for the seniors, Families USA for children), their disease (AIDS Action Council) or their disability (National Mental Health Association). In particular, the mental health consumer and HIV/AIDS communities are concerned with the confidentiality of their medical records and have been very active in debates on this issue for at least 10 years. The groups we interviewed represent the leading edge of consumer knowledge and activism. They are the most aware of the implications for lost privacy, having suffered discrimination in education, housing, insurance and employment. In response to these fears, some patients seek treatment for certain conditions, such as sexually transmitted diseases and mental health problems, outside their usual providers and without seeking reimbursement. According to a 1993 Harris/Equifax survey (cited in Janlori Goldman and Deirdre Mulligan, *Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality*), it has been estimated that nearly 11% of healthcare is now private pay for such reasons.

Another activist and concerned group of consumers are those within the American Jewish community. In recent years, advances in genetic testing have identified a mutation in a particular gene, BCRA1, related to breast cancer in young women. That, as well as other genetic conditions, have been studied more extensively in the Jewish population because the patterns of intermarriage have made it easier to conduct genetic studies than in other homogenous ethnic groups or in heterogeneous groups. The prevalence of the genetic studies and the calls for data registries to track carriers of genetic mutations has raised concerns among community leaders. Although Jewish women are no more likely to be carriers of the defective gene than other women, the establishment of registries may lead to perceptions that American Jews are "genetically-defective" as compared to others, a fear that is fueled by memories of the Nazi Holocaust.

The activist consumer groups would resist the development of national data systems as well as legislation requiring reporting of all patient transactions. This is demonstrated in the recent controversy about the HIPAA requirement that a unique health identifier be designated for every U.S. citizen. Activist consumers will oppose any such proposal as too threatening to individuals' privacy concerns. More limited legislation is laying the groundwork which may progress towards acceptance of identifiers. For example, a bill in the Maryland legislature proposes that all health care transaction information, including those of self-pay patients, be included in a statewide database. The Maryland Health Care Access and Cost Commission recommends such a move to better understand how people use healthcare resources. In a related move abroad, a pan-European electronic health passport has been proposed which would carry a baseline of information about citizens including blood type and allergy information for emergency use. In France, the Health Ministry has announced that doctors must submit all their bills electronically by 1999.

In addition to the consumer groups, one of the most visibly active players in the consumer-protection camp is Janlori Goldman, author of the Center for Democracy and Technology report and a former ACLU privacy attorney. She is now Director of the Georgetown University Health Privacy Project (HPP). The HPP produces a handbook for the protection of the confidentiality of patients' records which has been endorsed by both the AIDS Action Council and the American Health Information Management Association. In conjunction with Georgetown University Law School, it provides students with medical privacy *pro bono* assignments with consumer group clients. It also assists in drafting legislation.

Providers. Providers as used here refers to any individual or institution involved in the delivery of health care services, such as nurses, doctors, dentists, physical therapists, mental health therapists, hospitals, clinics and nursing homes. Healthcare providers, primarily physicians under the auspices of medical associations, are the most active in medical privacy issues to date and share a concern for patient privacy second only to consumers themselves. The key concern of physicians is that patients will withhold vital information for fear that it will become public, and that incomplete information will be detrimental to an accurate diagnosis and the provision of optimal care. Philosophically, they base their interest on the preservation of the historic doctor-patient privilege as embodied in the Hippocratic Oath. This relationship and the historical adherence to confidentiality by physicians gives patients the freedom to divulge all aspects of a health history without fear of public scrutiny or reprisal. The American Medical Association is currently formulating a more formal policy, using as its foundation the work done by the Massachusetts Medical Society, considered the leader among state medical groups in formulating policy on medical privacy.

Payers. Payers have always had an interest in tracking health care information. In the earliest days of fee-for-service medicine, accurate tracking created the basis for billing, and the information captured was used to support higher reimbursements from insurance companies. With the advent of Prospective Payment and Diagnosis Related Group (DRG)

billing in hospitals, the incentive was to accurately capture information to support the patient's categorization within a higher-, rather than lower-, cost DRG. Under managed care, where the insurer assumes the financial risk for care, current capitation reimbursement methods demand even more accuracy and adequacy in data collection. If capitation rates are not calculated accurately, it could spell demise for the provider. Access to data, particularly outcome measurements, is the lifeblood of HMOs. It is the premise upon which all subsequent decisions are made regarding which populations to cover, which providers to include and which treatments and therapies to reimburse. The recent experience of Oxford Health Plans of Norwalk, Connecticut in the mismanagement of its data system is indicative of the kinds of problems that HMOs will have if data does not support the financial, as well as the clinical needs, of care. Because large portions of its database were inaccurate, Oxford had incorrectly projected its potential exposure, which resulted in large, nearly catastrophic, losses. At last reporting, it had filed a first quarter 1998, $45.3 million loss, suffered management shake-ups and anticipates major restructuring to recover from the outcome of mismanaging data.

While it is well-accepted that accurate data is necessary for the smooth operation of a modern, automated healthcare system, there is still some debate about the level of detail insurers need, or are entitled to, in order to determine the validity of a claim. For example, mental health consumer advocates do not want the details of therapy sessions to be divulged to justify payment. Further, under ERISA (Employee Retirement Income Security Act), employers have the option of self-insuring. Since employers are payers, they have access to confidential health information to which they might not otherwise be privy.

Researchers. Currently, some research is skewed because data is largely derived from populations who are more willing or more easily measured (such as volunteers or the indigent, public health population) or who have limited authority over their health information (such as prisoners and military conscripts). Many researchers would prefer to have access to all medical data, not prejudiced by payer, illness or patient choice, because the most accurate conclusions result from data extracted from the whole population, rather than a subset that, it could be argued, is not a representative sample. The strongest voices representing the research community, such as the Biotechnology Industry Organization (BIO) which incorporates over 770 organizations dedicated to research and development worldwide, believe that unrestricted access to all information gleaned from all populations is unlikely. Therefore, they are crafting ways to frame the debate to gain access to as much clinical information as possible, specifically by calling for broad national confidentiality laws that will confer uniformity to all patient authorizations for consent. That objective is best achieved by removing identifiers. Some researchers, however, want the ability to “unlock” encryption keys to trace disease patterns in families, within ethnic groups and across geographic regions. As an example, in the case of babies born in the 1950s to mothers who took DES, researchers would like to be able to track specific people to monitor the impact of the drug.

The Commercial Healthcare Sector. Pharmaceutical and medical device companies have a financial stake in their ability to retrieve and manipulate data. Access to medical records provides patterns of use for research and development, manufacturing, marketing, warehousing and distribution. Presently, the industry's interests are being promoted by the Pharmaceutical Research and Manufacturers of America (PhRMA) and several individual manufacturers who have joined in roundtable discussions. Other policy players generally consider the interests of the pharmaceutical industry to be the least critical of all the players. In polling various interest groups, we discovered that pharmaceutical companies are perceived as the worst offenders in violations of patient privacy, a view that does not square with reality and which is most likely media reporting driven. An AARP policy spokesperson expressed a view typical of several of the groups we interviewed when he stated that the organization did not want pharmaceutical companies directly contacting its members and considered such contacts to be overt violations of privacy.

In response to the press reports of the CVS/Elensys relationship, the National Association of Board of Pharmacy developed a set of draft guidelines that defines the role of patient compliance and intervention programs within the pharmacy setting. NABP draft guidelines recommend that compliance and intervention programs only be used to monitor a patient's drug therapy regimen, and expressly may not be used to switch a patient's medication or course of therapy for economic or financial gain. The guidelines also recommend that such programs be voluntary and that patients be allowed to opt-out of any compliance program. It also recommends that any information that is used for research must be de-identified.

Criminal Justice. The benefit to the common good is the rationale for criminal justice claims to unfettered access to identifiable medical records. Criminal justice includes the courts, which can access records via a court order; the penal system, with access to records of prisoners for the safety of prison personnel; the juvenile justice system, with access for proper disposition of cases and safe handling of children and adolescents; and local, state and federal law enforcement, who need immediate access to information during emergencies. Criminal justice advocates argue for access to otherwise private or confidential information, and their rationale is strongest in cases of threats of imminent danger. Its interests to unauthorized access are protected in Secretary Shalala's recommendations to Congress. This view is not universally held, however. In contrast with the DHHS recommendations, current legislative proposals require that law enforcement entities be subject to some form of due process before records can be released to them. The American Hospital Association, in its testimony before the U.S. House of Representatives in May, criticized the DHHS proposal and supported legislative efforts to hold law enforcement agencies accountable to provide proof by showing probable cause in their efforts to gain access to health records.

Technology. The technology sector is a conglomerate of firms that develop the software, provide the hardware and manage the health data archives. This group is primarily concerned with the art of the possible, rather than with the constraint of progress towards

information and technology development, management and manipulation. Its concerns run the gamut from developers of encryption and other technologies which are data-neutral (that is, their work could apply to any data, not just to the medical data arena) to health data vendors, such as members of the American Health Information Management Association (AHIMA). There is agreement across the spectrum of technology companies that some national standards are necessary and desirable. From the perspective of the information technology developers, a preemptive federal standard makes development, deployment and management of products more uniform and efficient. From the perspective of AHIMA, a federal standard eases the responsible handling medical records from a variety of sources, each of which currently is governed by different State laws and institutional policies.

Shared Medical Systems Inc. (SMS), the second-largest healthcare information systems vendor in the world, explained that technology has the capability to install any of the currently envisioned levels of security now being considered in policy debates. Literally, anything is possible, though the cost to achieve some of the levels of security may be prohibitive and would greatly restrict access to data because of the costs that will be added to data system management. In addition, certain security technologies are slow and would be inefficient to run. In the view of SMS, it is more cost-effective for healthcare providers to invest in and train people who know and abide by the laws, and for government to enact stiff penalties in place for violators than it is to try to achieve optimal levels of security using technology.

Media. The media has not yet emerged as a major player in the debates, although as the issue heats up it is likely to become a force. Mainstream articles so far have warned people about the threat that electronic data poses to their privacy, and future media is expected to elaborate on that theme. There is some emotional appeal in stories that elaborate on the conspiracy theory that "Big Brother Is Watching," and the media is likely to latch onto that singular theme. It is a simplistic approach and therefore has soundbite appeal.

Philosophically, the media will come at this debate from two angles. Americans have a Constitutional right to privacy; yet, the press has a Constitutional right to freedom of expression, which has been extended to gathering and broadcasting information in an unfettered way.

As individuals, journalists are likely to write missives of the type published by William Safire this spring in the *Washington Post*. The opinion piece ended with the statement: "We must demand the government set the example in snoopery restraint. If Americans allow us to lose our expectation of privacy, we will then lose our privacy itself—and the essence of our personal freedom is the right to be let alone."

However, the media is in the unique position of perhaps getting caught in its own crossfire, having an institutional bias toward access to information. News organizations frequently

pursue information on individuals under the Freedom of Information (FOI) Act. It will continue to protect its position that all information about public officials and public figures should be made available for general consumption under the presumption that the public has the right to know about the character and habits of its political and cultural leaders. It may find itself arguing that the government does not have a right to know about every detail of an individual's life, while the press does.

Government Focus

The States. States have historically been stronger and more active than the federal government in privacy protection. Gostin, in 1996 in the *Journal of the American Medical Association*, reported that 49 states had some statutory protection for public health information in general; 42 states for communicable diseases reporting; 43 states for sexually-transmitted diseases; 42 states permitted disclosure of data for statistical purposes; 39 states allowed disclosure for contact-tracing in communicable diseases; 22 states for epidemiological investigations, and 14 states for subpoena or court order.

Most recently, State laws have focused on medical record protection for mental health, HIV/AIDS and genetic testing information. States have most recently acted to protect confidentiality of pharmacy records, but in a limited way. For example, in most states, to date, pharmacists are not covered by the same confidentiality regulations as other health care providers despite efforts in that direction. Layered on this patchwork of legislation is a constant flow of new proposals. According to Jacob Herstek of the National Conference of State Legislatures (NCSL), more than 250 bills containing medical record provisions were introduced in 1998 alone. Of those, 63 passed one house and 7 were enacted. The complexity of the laws makes it difficult to conduct a comprehensive analysis of the laws at this time, and more experience will be required to determine if there are trends at the State level.

It is no surprise, then, that attention returns to Washington as the most likely solution for a comprehensive privacy strategy. It is also no surprise that some observers see the federal government as the setting for what is likely to be next major civil rights battlefield.

A few states have tackled laws that regulate pharmacies, pharmacists and the records they keep. The Pennsylvania Pharmaceutical Association (PPA) believes that while that state's Pharmacy Act covers pharmacist behavior, it does not go far enough. A spokesperson for the PPA believes stricter laws are needed to protect patient records in PBMs and managed care organizations. In Virginia, the state enacted a law in 1998 that names the pharmacy as the owner of patient records. Another law that would have made patient pharmacy records a part of the medical record, and subject to the same confidentiality laws, passed both houses but was vetoed by the governor. The governor vetoed the law saying the attorney general advised him it was unenforceable as written, but that he would revisit it next year.

Florida entertained a law in 1998 that establishes ownership of the pharmacy record with the pharmacy or corporation that owns the pharmacy. Since it is the pharmacist, and not the pharmacy, that is licensed, such laws protect the pharmacist from personal and professional liability resulting from misuse or mishandling of records when those decisions are made by the owner or corporation. In Massachusetts, a legislative proposal that would have protected patient rights regarding general medical records never left committee.

The Executive Branch. In addition to the activities of DHHS devoted exclusively to medical privacy, other branches of government are addressing information and privacy needs overall. Most recently, the Clinton Administration has put forth its proposal for a "unique health identifier" —a computer code that would create a national database to track every citizen's medical history. This specter of this womb-to-tomb database has elicited concern from consumer privacy advocates. DHHS hearings are underway on this issue and some observers believe the proposal will die due to public opposition.

Leadership also has come from Vice President Al Gore, who has taken a particular interest in technology and in its data security component. This interest extends to records security, calling for an Electronic Bill of Rights. The Executive Branch is interested in advancing the development and sale of encryption technologies that will allow codes to be unlocked for security and law enforcement purposes. It also contemplates a National Information Infrastructure (NII) with the capability to overlay data from disparate sources to create a multi-dimensional snapshot of every citizen. Executive Order #13010 advances the establishment of Chief Information Officers at each agency and encourages "cross-agency cooperation" by establishing Government Information Technology Services that would link data gathered by the Federal Emergency Management Administration (FEMA), the Department of Defense (DoD), the Department of Commerce (DoC), the Department of Transportation (DoT), Department of Energy (DoE), the Department of the Interior (DoI), the Department of Education (DoE), the Department of Health and Human Services (DHHS), the Department of Labor (DoL), Housing and Urban Development (HUD), the Armed Services, the National Aeronautics and Space Administration (NASA) and the Agency for International Development (AID), to name an extensive, but not all-inclusive, list.

The Courts. A few cases have come before the courts. The cases have been too few and not yet significant enough to define the public policy debate. As noted by Justina A. Molzon, M.S. Pharm., J.D. in "Pharmacists, Patients and Privacy: The Foundation of Pharmaceutical Care", technology is developing faster than the law can keep up with it. While the courts hand down decisions on a case-by-case basis, no major trend has emerged, nor single case set a standard. It is more likely that the courts will play a major role later, after either federal legislation is passed or regulations are issued that will spawn lawsuits to challenge them.

According to David Weber, founder of the AIDS Law Project and author of *AIDS and The Law*, case law comes from two arenas—challenges to statutory law and challenges to

Constitutional law. Most of the legal challenges that arise are challenges to specific state statutes, usually the result of workplace violations. Constitutional challenges are rarer, but they occur. One such case is *Doe v. SEPTA*. In this case, a SEPTA employee with HIV claimed his Constitutional right to privacy was violated when his employer, a State transit agency and a payer for prescription drug coverage, attempted to get pharmacy information regarding the identity of which of its employees were taking the HIV drug Retrovir. SEPTA had discovered the Retrovir prescription during its audit of a prescription benefit plan. In overturning a lower court ruling that awarded damages to the employee, the Third Circuit Court of Appeals in 1995 sided with SEPTA, saying the transit system's right to monitor its drug costs outweighed the employee's right to confidentiality.

The U.S. Supreme Court also has weighed in on the debate. In *Roe v. Whalen*, Supreme Court justices allowed New York State to keep a computerized list of prescription records for dangerous drugs and to require physicians to disclose the names of patients for whom those drugs were prescribed. In a reference to the state's "vital interest in controlling the distribution of dangerous drugs", it tipped the scales in favor of the state statute. However, in doing so it still acknowledged the individual's right to privacy which includes "the individual interest in avoiding disclosure of personal matters." It clearly left open the option for further Constitutional volleys.

The U.S. Congress. All of the major players presently engaged in privacy policy debates have turned their focus toward the U.S. Congress—even the Executive Branch views the federal legislature as the most appropriate setting for determining the national public policies and standards which medical privacy requires. Current activity in the House is still limited, in particular, for an issue with Constitutional and economic ramifications, such as the case in medical privacy. Most activity is in the Senate, where three bills are vying for primacy, one each by James Jeffords (R-VT) and Robert Bennett (R-UT) and another by Edward Kennedy (D-MA) and Patrick Leahy (D-VT). One bill headed for introduction in the House of Representatives, "The Consumer Protection and Medical Record Confidentiality Act", slated for introduction by Congressman Chris Shays (R-CT), is currently in draft. None of these bills has clear frontrunner status, and none of the stakeholders has taken a position favoring any one bill to the complete exclusion of others.

The Jeffords Bill (S.1921 "Health Care PIN Act") requires that separate consent authorizations be obtained for any purpose other than treatment, payment or health care operations. The bill protects health information, defined as any information (including demographic information) that relates to past, present or future physical or mental health or conditions of an individual, provision of health care to an individual; or payment for the health care services provided to an individual. It allows for exceptions for public health reasons or reporting of vital statistics or abuse and it preempts weaker state laws.

The Jeffords bill is considered a compromise between the two extremes in the debate—those with strong right-to-privacy views on the consumer side and those with broad access

views on the commercial and information side. Jeffords lays a “floor” in the privacy debate, establishing bare minimum safeguards that include a two-tiered consent system. The two-tier system includes one consent to authorize primary service delivery and payment and a second authorization for research and other secondary uses. It allows stricter state laws to stand, something desirable to consumer and advocate groups.

The Kennedy/Leahy Bill (S. 1368 "Medical Information Privacy and Security Act") deals with issues of patient-identifiable information and creates stricter disclosure rules, allowing patients to indicate that particular entities may not receive their information. It does not preempt other Federal or State laws. The Kennedy/Leahy bill is favored by right-to-privacy advocates. It defines a personal right to control information and is closer to the positions of groups such as the American Medical Association and the American Association of Retired Persons. It may not be politically viable because it is too restrictive for commercial interests, however.

The current draft of the Bennett Bill circulating within Congress would require providers to obtain a single disclosure form for treatment, payment or healthcare operations and another for any other purpose. It regulates individually identifiable health information, but allows reporting of vital statistics, abuse or neglect, and the reporting of an individual's mental or communicable disease status. It preempts State laws. Not yet formally introduced as of this writing, Bennett is considered a contender as the frontrunner among the all the proposals to date. While it accomplishes many of the same compromise positions as Jeffords, it goes one step further by superseding all State legislation, the preferred position of the data and health care commercial sectors.

In the House of Representatives, Chris Shays (R-CT) has introduced H.R. 3900, "Consumer Health and Research Technology (CHART) Protection Act", a bill intended to protect the availability of information for research purposes. The bill provides for medical information to be provided to researchers without the consent of the patient if a formal review board has approved the research project, if confidentiality protections are in place within the research setting, if the researcher agrees not to disclose the information to any other data user and is informed of the legal consequences for doing so. The bill preempts State laws.

None of the above laws addressed the handling of pharmacy records. A separate piece of legislation, H.R.3756, entitled the “Prescription Privacy Protection Act of 1998”, introduced by Rep. Jerrold Nadler (D-NY) and precipitated by reports of the CVS/Elensys patient compliance program, addressed the need for written consent for disclosure of pharmacy records. Significantly, it held the pharmacy owner, pharmacist or other pharmacy employees liable to a civil monetary penalty of not more than $10,000, but clearly did not hold the pharmacy or the corporation that owns the pharmacy accountable for improper disposition of the records.

Table 1.

Organization	Uninformed	Informed, Unconcerned	Concerned, Tracking	Formulating Policy	Policy Determined	Active in Policy
State						
Assn. of State & Territorial Health Officials			x	x		
Massachusetts State Medical Soc.			x		x	x
Nat'l Assn. of Ins. Commissioners			x			
Nat'l Conf. of State Legislators			x		x	
Nat'l Conf. of Uniform State Laws (Chicago)					x	
Nat'l Governors Assn. Health Policy Studies Div.	x					
Providers/Medical						
American Academy of Pediatrics			x	x		
American Assn. of Health Plans: Merger of Group Health Assn. of America & American Managed Care & Review Assn.			x	x		x
American College of Physicians			x		x	x
American Hospital Assn.			x	x		x
American Medical Assn.			x	x		x
American Psychological Assn.			x			
Assn. of Physicians & Surgeons			x			
Health Leadership Council			x	x		x
Nursing						
American Nurses Assn.			x	x		
Pharmacy						
Academy of Managed Care Pharmacy			x		x	x
American Assn. of Colleges of Pharmacy			x	x		
American Pharmaceutical Assn.			x	x		x
American Society of Consultant Pharmacists			x			
Nat'l Assn. of Boards of Pharmacy			x			
Nat'l Assn. of Chain Drug Stores			x	x		
Nat'l Community Pharmacists Assn.			x			
Pharmaceutical Care Management Association			x	x		
Pharmaceutical Research & Manufacturers of America			x	x		
Insurance						
Alliance of American Insurers		x				
American Council of Life Ins.			x			x
American Managed Behavioral Healthcare Assn.			x		x	x
Health Ins. Assn. of America			x			x
Nat'l Assn. of Ins. Commissioners			x	x		x
Consumers/Advocates						
AIDS Action Council			x			x
American Assn. of Retired Persons			x		x	
Consortium for Citizens with Disabilities/ Nat'l Assn. of People with AIDS					x	x
Families USA		x				
Nat'l Mental Health Assn.			x		x	x
Nat'l Organization for Rare Disorders			x			x
Medical Information						
American Medical Informatics Assn.			x			x
Shared Medical Systems, Inc.			x			x
Attorneys						
AIDS Law Project of PA			x			
Other Groups						
American Public Health Assn.			x			
Health Privacy Project					x	x
U.S. Chamber of Commerce			x			x