HEALTH INFORMATION CONFIDENTIALITY: ARE WE SLEEPING WHILE TECHNOLOGY ERODES OUR PRIVACY?

November 1998

Underwritten by a grant from
THE ROBERT WOOD JOHNSON FOUNDATION

TABLE OF CONTENTS

I.	THE ISSUE	1
II.	INTRODUCTION	1
III.	HEALTH INFORMATION -- WHAT IS IT, WHO NEEDS IT AND FOR WHAT PURPOSES?	1
IV.	MEDICAL PRIVACY -- IT'S NOT REALLY A "NEW" ISSUE	3
V.	MEDICAL PRIVACY AND HEALTH INFORMATION CONFIDENTIALITY -- PINPOINTING THE MAIN ISSUES	4
VI.	NATIONAL EFFORTS - - DHHS AND THE SECRETARY'S RECOMMENDATIONS	5
VII.	CONGRESS AND MEDICAL PRIVACY BILLS	6
VIII.	STATE LAWS -- MEETING THE CHALLENGE	7
IX.	SUMMARY REMARKS	8
X.	POLICY IMPLICATIONS	9
XI.	REFERENCES	10

ISSUE BRIEF No. 28

New Jersey Policy Forums on Health & Medical Care

101 Campus Drive, University Square, Princeton, New Jersey 08540• v (609) 720-0136 • f (609) 720-0134

Jamie Harrison, Executive Director • Joanne T. Fuccello, Associate Director/Writer Researcher

Sponsored by The Forums Institute for Public Policy

Underwritten by a grant from

The Robert Wood Johnson Foundation.

HEALTH INFORMATION CONFIDENTIALITY: ARE WE SLEEPING WHILE TECHNOLOGY ERODES OUR PRIVACY?

ISSUE: For public policy makers, the issue of medical privacy and the confidentiality of health information cuts across legal, regulatory, ethical and practice lines. In a health care system offering new approaches to managing health care delivery, financing and research, advances in information technology have allowed for the sharing and distribution of health information to multiple players -- including providers, insurers, employers, payers, and new third parties. How do policy makers balance the individual right to privacy with the demands of health data collection and sharing to meet the goal of improved health? At present, there is no comprehensive federal medical privacy law, and the states have a varied "patchwork" of laws, in most cases addressing only parts of the broader issue. With several federal bills pending which may preempt state laws, what options are available to policy makers?

INTRODUCTION

The end of the 20th century has been described as a "post-humanist" era. The tenets of humanism, in the purest sense of the word, emphasize the central importance of human values and extol the wonders of the human mind and spirit and their accomplishments. In the post-humanist world, technology is the center of the universe, and from our hearts to our DNA, we are decoded and digitized, distilled into bytes of information. The subject of medical privacy forces the issue of analyzing how the core values of ethics, privacy and confidentiality of our individual and collective health care will be balanced against the technological imperative to "use" information to better our health care system.

As with most discussions regarding the state of health care, the medical privacy issue is comprised of many views and components. Through electronic data information systems -- in both the public and private sectors, through insurers, providers, public health networks, and employers in massive corporations and small businesses -- information regarding our health care and medical information is being more easily collected and shared.[1] What types of are lines are being crossed for the sake of information-gathering and how will confidentiality be ensured? What steps are the "purveyors" of information taking to meet the goals of establishing a reliable database of health information to inform policies and planning in such areas as public health and epidemiology, while at the same time preserving the integrity of each individual's privacy?

The benefits and power of information technology -- to organize, store, analyze and share information quickly and efficiently -- have evolved in tandem with the ability to retrieve and deliver this information to a diverse group of users located at multiple sites. Compared to other sectors, the health information industry is considered by many analysts to "lag behind" in its degree of advancement and sophistication, yet growth in the industry is occurring at an exponential rate. These technological advances represent a double-edged sword, which on one side offers sophisticated tools for medical research, clinical practice, research and education; yet, on the other side raises significant concerns about breaching the security, privacy and confidentiality of health information. At the current crossroads, some industry observers believe that technology is "moving too fast" and the erosion of privacy has already taken place. Others believe that policy makers may not have to choose one over the other, i.e, individual privacy rights vs. the use of sophisticated health information systems and data warehouses, but must be informed about the issues in such a way so as to synthesize the two without sacrificing the benefits of either one.

HEALTH INFORMATION -- WHAT IS IT, WHO NEEDS IT AND FOR WHAT PURPOSES?

A deadline has been set -- through the Health Insurance Portability and Accountability Act of 1996 (HIPAA) -- for Congress to enact a comprehensive law in order to create a privacy framework to protect personally identifiable health information.[2] HIPAA gives Congress until August 1999 to do so; if it does not meet this deadline, the federal Department of Health and Human Services (DHSS) is authorized to step in and promulgate regulations relating to the privacy of health information within 42 months of HIPAA (February 21, 2000) (Jones, 1998).[3]

[1] In 1997, the National Research Council estimated health information technology spending to be at between $10-$15 billion per year. A May 1998 feature article in *Medical Economics* reported on the continued growth of the industry, noting that health care providers alone are investing approximately $2 billion a year to create new information networks to support activities such as disease management.

[2] HIPAA contained a section setting forth administrative simplification requirements in an attempt to improve standardized electronic transmission of health information and medical records, both administrative and financial. The administrative simplification requirements raised privacy concerns because of potential breaches in privacy through the electronic exchange of sensitive health information.

[3] There are also "global" pressures coming to bear: a European Union directive, effective October 1998, prohibits member organizations

What type of personal and sensitive information can medical records include? Such confidential information as an individual's medical, psychiatric, or psychological history, diagnosis, condition, treatment, evaluation and drug prescriptions (Herstek, 1998). In the present system, these medical records are available to a wide range of individuals and organizations, which may in turn have access to personally identifiable health information. This health information is collected and used for a range of activities. Those entities collecting health information include:

- Health Plans/Managed Care Organizations
- Providers (Physicians; Hospitals; Health Care Facilities)
- Employers (Private and Public Sector)
- Health Insurers
- Researchers (Clinical; Academic)
- Pharmaceuticals
- Standards and Accreditation Organizations
- Peer Reviewers
- Federal, State, Local Governments - as employers, payers, insurers and researchers

Health care activities for which information is being collected and utilized:

- Payment of health care services
- Provision of health care services
- Determinations of health coverage
- Reviews of utilization activities
- Public health research activities
- Research on disease and treatment protocols
- Analysis of outcomes
- Tracking of overall health care costs
- Tracking of other health-care related activities, such as workers' compensation claims

Health care stakeholders are responding in various ways to the complex issues raised by efforts to create and implement a medical privacy "standard." While individual patients and physicians are concerned about the potential effects that breaches in confidentiality may have on their relationship and the delivery of health care, researchers and policy makers fear that too stringent a privacy law may damage the integrity of their research, which includes public health activities, tracking studies, and health care evaluation studies. The public at large is also concerned about the possible ramifications of the health information being "negatively" interpreted, such as by employment or insurance discrimination. What if an employer saw a genetic predisposition to depression in a potential employee's file, wouldn't the candidate without this risk factor make a more attractive employee? Or insurance risk?

Health plans and insurers have various insurance management issues that are a concern: how might proposed legislation affect their ability to conduct utilization reviews or to perform provider performance measurements? As states continue to move forward with legislation targeting "pieces" of privacy issues, businesses with multi-state operations are pushing for some type of uniformity in privacy laws and regulations (Kahn, 1998). These organizations are concerned about the potential increased costs associated with conforming to different laws and administrative requirements in every state in which they conduct business.

In the absence of a comprehensive federal privacy law and with wide variation among state laws, large amounts of health data at present fall somewhere between identifiable and fully anonymized. For the most part, personal health information is used for the "right" reasons. But there has been considerable growth in the business of "buying and selling" such information for commercial purposes. For example, pharmaceutical companies are using pharmacy prescription data to "advertise" related products to consumers -- such as glucose level monitors to diabetics; and direct-mail advertisers offer baby formula coupons to new mothers, through hospital birth registry records (Herbert, 1998; O'Harrow, 1998; Rybowski, 1998).[4] The same technology that has allowed for the development of large, multi-purpose databases of information, has also simplified and facilitated access to and analysis of this information, across all fields.

The growth of managed health care with its administrative imperatives for better quality assessment and outcomes measurement has also added to the exponential increase in large-scale information systems and data "warehouses."[5] This trend is evident in both private sector managed plans, as well as in Medicaid and Medicare managed care initiatives. The resulting "easy access" to this information makes each of us vulnerable to its getting into the "wrong" hands for the "wrong" purposes. Confidentiality of personal health information is a precious commodity and one, which if misused, can have an impact on employment, housing, insurance coverage and quality of life.

Confidentiality between and among medical professionals and patients lies at the ethical core of the

from sharing and transferring information to entities outside of their country that do not have in place an "adequate" degree of privacy protection. (Jones, 1998).

[4] For a detailed discussion on the issue of protecting the confidentiality of health information, reference is made to Rybowski's July 1998 National Health Policy Forum Background Paper.

[5] A 1997 Peat Marwick survey found that 82 percent of Americans receiving health benefits from their employers are part of a managed care plan (Health Insurance Association of America, 1998).

profession, whether the health care provider be a physician, nurse, social worker, psychiatrist or facility, such as a hospital, pharmacy or clinical lab. An emerging trend involves behaviors by individual patients who are admitting to "doctor-hopping" or withholding information from their doctors about their health, because they fear the information my be used in a negative way. A 1993 Louis Harris survey found that 11 percent of the public have, on occasion, chosen not to file an insurance claim, and 7 percent have chosen not to seek care because they did not want to harm their employment prospects or other life opportunities. Not only do such behaviors have a negative impact on the individual involved, but "missing" health information or unreported health conditions will affect research, disease management and public health studies.

The managed care delivery system requires sophisticated coordination and information sharing among health plans, hospitals, physicians, purchasers and others in the health care market. The architects of sophisticated electronic and data exchange systems are currently faced with the issue that unless they can create "tamper-proof" secure systems, they run the risk of the public and health care professionals turning away from using the technology. How can the confidentiality of health care information be ensured without making these records so secure that health care providers and researchers do not have access to information when they need it? For example, an emergency room physician points out that "Not knowing that patients have a drug allergy when they hit your emergency room unconscious could kill them" *(American College of Physcians - American Society of Internal Medicine, Newsletter*, September 1998).

MEDICAL PRIVACY -- IT'S NOT REALLY A "NEW" ISSUE

A 1997 survey conducted by the Center for Public Integrity found that 92 percent of respondents reported they were "concerned about threats to their privacy," and 64 percent said they were "very concerned" about ensuring it (Lewis, 1998). It is a routine finding on patient satisfaction surveys in hospitals that privacy is one of the highest-ranking concerns among patients who are being cared for in hospital settings (Gesensway 1998).[6]

How is privacy defined? Rybowski (1998) points to U.S. Supreme Court Justice Louis Brandeis' 1928 definition of privacy, in which he wrote that the makers of our Constitution "conferred…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. U.S*., 277 US 438 (1928); the first wiretapping case to reach the Supreme Court). In more recent times, according to the National Committee on Vital and Health Statistics, in its Health Privacy and Confidentiality Recommendations last year, health information privacy refers to the interest of patients "in knowing and controlling how their personal health information is collected, maintained, used and disclosed" (ibid.).

The issue of medical records privacy and related measures to ensure the confidentiality of health information has been a national issue for decades. In 1971, Congress first heard testimony on the issue, although in the mid-1960s proposals for national "data centers" raised concerns about the emerging growth of data collecting and statistical research activities (Bennett, 1992). Over 250 legislative bills relating to privacy were introduced between 1965 and 1972 (from the 89th to the 92nd Congresses); however, only two privacy laws were enacted: the Omnibus Crime Control and Safe Streets Act of 1968 (regarding use of wiretaps) and the Fair Credit Reporting Act of 1970 (regulating credit agencies) (ibid).

In 1974, the Federal Privacy Act was enacted; yet the act covers only personally identifiable data held by the federal government (it does not cover data held outside the federal government); this data includes Food and Drug Administration data, National Center for Health Statistics' data and the Centers for Disease Control's public health surveillance data (Benjamin & Kennan, 1997). The U.S. Office of Technology Assessment reported in 1993 that "the patchwork of state and federal laws addressing privacy in personal medical data is inadequate to guide the health industry to protect privacy of medical information in a computerized environment" (U.S. Congress, Office of Technology Assessment, 1993).[7]

A recent Op-Ed piece in *The New York Times* entitled "What Privacy Rights?" addressed the erosion of patient confidentiality by pointing to the practice of the "selling" of medical information, such as prescription drug information, for financial gain among businesses (September 28, 1998). The author voices the view of privacy advocates -- who have been calling

[6] Concern about privacy has not escaped the popular media, as reflected in both *Newsweek* and *Time* magazines' cover stories over the past two years, titled respectively: "Naked Before the World: Will Your Medical Secrets Be Safe in a New National Data Bank," and "The Death of Privacy: You Have No Secrets" (June 30; August 27, 1997).

[7] Congress passed the Americans with Disabilities Act in 1993, which provided comprehensive civil rights protection for people with disabilities. Case law continues to address and interpret the rights of infected people, physicians, dentists and other health care providers, including confidentiality issues (Tamborlane & Kunz, 1998).

on Congress for years to enact legislation to "spell out and guarantee a citizen's basic right to privacy" -- that the opposing view of industry players has made Congress slow to act in this regard (ibid.).

Janlori Goldman, Director of the Health Privacy Project at the Institute for Health Care Research and Policy at Georgetown University Medical Center, notes that: "Reports of the last twenty years are unanimous in concluding that a comprehensive national health privacy law is critical to ensuring both the integrity of the doctor/patient relationship and the continued development of this nation's health care system" (May 19, 1998, testimony before the U. S. House of Representatives).[8]

MEDICAL PRIVACY AND HEALTH INFORMATION CONFIDENTIALITY -- PINPOINTING THE MAIN ISSUES

There are several key issues that emerge in grappling with the implementation of medical privacy standards, underscoring the complexity of the issue. According to Goldman (1998), they can be categorized under discrete substantive areas: (1) Access; (2) Notice; (3) Consent; (4) Research; (5) Security; (6) Law Enforcement; (7) Remedies (Penalties/Sanctions) and (8) Preemption. Each of these areas carries with it multiple issues/questions. For example, in the area of access, who should control access and how; what role should people have in having access to their own information and in deciding on who can see and use it? Issues concerning notice and consent include identifying what kinds of notice must be given to patients and how and when consent will be obtained. An issue especially significant to states is how broad should federal preemption of state laws pertaining to confidentiality be.

Research issues include questions regarding the use of personally identifiable information and the analysis of instances when information will be used for research purposes without patient authorization. At present, there is no consensus as to how much patient-identifiable data should be available to medical researchers without specific patient authorization. The American College of Physicians-American Society of Internal Medicine (College), for example, has offered its position on instances in which individually identifiable patient health information may be used for medical research projects without patient authorization. The College supports this disclosure only if the research cannot be done in any other way and if an institutional review board (IRB) has determined that the research project "is so important it would outweigh any intrusion into a patient's privacy and if the research would be of minimal risk to the patient" (Gesensway 1998)[9]. Such a position represents a balance between what the medical profession needs to do to protect the rights of an individual patient vs. their "obligation to create new knowledge that will further protect the health of the public" (Lavizzo-Mourey, 1998). Within the College's ethics manual, it is stated that "physicians, recognizing that confidentiality is a fundamental tenet of medical care, have an obligation within their own institutions to advocate policies and procedures to secure the confidentiality of patient records" (Ibid.). As chair of the College's Ethics and Human Rights Committee, Dr. Lavizzo-Mourey points out the ongoing privacy debate comes at a time in the health care environment where more research is required in order to evaluate and assess quality of care and the efficiency and effectiveness of new health care delivery systems.

An industry has emerged among computer technology firms to develop global data protection programs for large-scale corporations and businesses, and medical records management systems for health care providers, health plans and insurers. Throughout the country, there is wide variation as to how such "information-sensitive" entities as hospitals are addressing the issues of balancing medical privacy and technological advances. Some are moving forward into such areas as Internet transfer of patients' health information from multiple offices, to labs, nursing homes and radiology clinics. Privacy is ensured by the utilization of sophisticated security measures such as encryption and password reassignments. Among other hospital systems, there remains caution about using the Internet to transfer confidential patient information until a national privacy law is adopted (Gesenway 1998). There is also a growing awareness of how "lapses" in human behavior and judgement often can create just as much a threat to potential breaches in medical privacy than "unfettered technology." In both the private and public sector, there are significant efforts to offer training to staff -- from doctors and nurses to administrative assistants and billing clerks -- in the area of confidentiality and privacy. For the most part, all involved parties are exploring ways to use technological

[8] The Health Privacy Project's work is focused in three areas: it is creating a compendium of state health confidentiality laws; it is staffing a Health Privacy Working Group to reach common ground on "best principles"; and it is identifying models within the health care community for health privacy "best practices." (Goldman Testimony, May 19, 1998).

[9] There has been an increased concern over the status of the institutional review board (IRB) system, which developed in the 1970s. Many analysts believe it is not structured to effectively protect "patients' rights and patients' interests" in the rapidly evolving world of electronic technology. Critics of the IRB system are calling for a re-structuring to meet the privacy demands of the new health care delivery system, and it is expected that the National Bioethics Advisory Commission will recommend a more thorough informed consent process, among other changes. (Edgar & Rothman, 1995; Katz, 1995; Silberner, 1998; Woodward, 1998).

and human resources in a positive way to ensure and safeguard medical privacy.

NATIONAL EFFORTS - - DHHS AND THE SECRETARY'S RECOMMENDATIONS

Under the requirements of the Health Insurance Portability and Accountability Act (HIPPA), Department of Health and Human Services (DHSS) Secretary Donna Shalala presented recommendations to Congress in September 1997 regarding the development of medical privacy standards.[10] In her report, she called for the creation of a basic national standard of protection, which would include defined security measures and explicit penalties for misuse of information. Her recommendations included five principles upon which a privacy standard would be based:

1. The principle of boundaries -- consumers' health information should be disclosed only for health care purposes;

2. The principle of security -- those who collect, store, transmit or maintain health information must take steps to safeguard it;

3. The principle of control -- consumers must have control over their health information and should have the right to access their health information;

4. The principle of accountability -- individuals who have access to individually identifiable health information will be liable for abuse;

5. The principle of public responsibility -- privacy must be balanced with public responsibility to support public health initiatives, research and initiatives to combat fraud and abuse.

While many industry groups support these principles as set forth, consensus regarding their actual implementation remains elusive. How these principles will be fostered and applied in creating a national privacy standard is a work in progress. One example of the contentious debates surrounding one of the Secretary's recommendations was summarized in an opinion piece in the Journal of the American Medical Association (JAMA) (1998). It presented the degree of opposition to what has been described as a type of "unfettered" access to medical records that may be accorded to law enforcement agents and members of the U.S. intelligence community if certain pending DHHS medical privacy recommendations are adopted as law.[11] In particular, the American Psychiatric Association is strongly opposed to such access, believing that it would "pose a serious threat to the welfare of patients, especially those with mental illness" (Skolnick, 1998). The APA, the National Alliance for the Mentally Ill and the National Association of Mental Health have joined other groups to support legislation that would instead require law enforcement and government intelligence officials to get court permission before they can view patients' records, just as a warrant is required to search and remove records from a person's property. Skolnick points out that in many states, law enforcement officers are allowed to search through a person's medical records without legal process. In pointing to the Hippocratic oath -- the structural integrity of medical practice -- he raises the concern that medical information technology is allowing access to medical and health information to those who have "taken no oath to protect either the privacy or well-being of patients" (ibid.).

In addition to specific concerns regarding the sensitive nature of medical records for those who are being treated for mental illness and substance abuse problems, the issue of genetic information also holds special significance. "Genetic" information such as a person's genetic predisposition to disease, or family history of diseases, may make an individual vulnerable to employment or insurance coverage decisions. Certain privacy advocates contend that because the “misuse” of genetic information could be especially damaging, it should be subject to "higher" privacy standards and be treated separately from other medical records (International Society for Pharmacoepidemiology, 1998; Skolnick, 1998). How can a compromise be reached to balance the specific needs of each affected group in creating a privacy standard?

[10] Over time, DHSS, in consultation with the National Committee on Vital and Health Statistics (NCVHS), will be proposing a series of regulations related to the administrative simplification requirements set forth in HIPPA. In discussing one set of proposed rules created to promote the greater use of electronic transactions (Federal Register, May 7, 1998), Shalala cautioned that while some security standards for electronic health data were included in the proposed rules, "They are not enough" (Jones, 1998).

[11] Reference is made to http://aspe.os.dhhs.gov/admnsimp/ for DHHS secretary Shalala's recommendations for protecting the confidentiality of patient information.

Bills Introduced in the Senate	Bills Introduced in the House
▪ Health Care Personal Information Nondisclosure Act of 1998(S. 1921): Introduced by Senators Jeffords (R-Vt.) and Dodd (D-Conn.)	▪ Consumer Protection and Medical Record Confidentiality Act of 1998 (HR 3900): Introduced by Representatives Shays (R-Conn.) and Barrett (D-Wis.)
▪ Medical Information Privacy and Security Act (S. 1368): Introduced by Senators Leahy (D-Vt.) and Kennedy (D-Ma.)	▪ Medical Privacy in the Age of New Technologies Act of 1997 (HR 1815): Introduced by Representative McDermott (D-Wash.)
▪ Medical Information Protection Act of 1998 (S. 2609): Introduced by Senator Bennett (R-UT)	▪ Fair Health Information Practices Act of 1997 (HR 52): Introduced by Representative Condit (D-Ca.).

CONGRESS AND MEDICAL PRIVACY BILLS

At present, several bills are being considered at the federal level, but no comprehensive law has been passed. While past medical privacy and health information confidentiality statutes may have been sufficient in scope and scale at the time they were introduced, the dynamic changes in the health care delivery and financing system during the past few years have changed the playing field: particularly with the inclusion of so many additional third-party players. The growth of managed care has brought with it the inclusion of many additional players such as contractors, vendors and employees responsible for medical records management and claims review. As Rybowski points out: "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" (National Health Policy Forum, *Background Paper*, July 1998). A summary of current medical privacy bills is below.

At Congressional hearings held in spring 1998 on the medical privacy bills, most stakeholders who testified -- from providers and insurers to researchers and employers -- agree that the country needs comprehensive legislation to protect the confidentiality of health care records, but consensus about what the law should contain seems not to be easily reachable.[12] Currently, no national law exists that makes it a criminal offense for people to access health care information they are not entitled to see, and state laws vary widely on the subject (Gesensway 1998).

There is differentiation among the bills regarding the central issues of patient consent; how access to both federally and privately funded researchers will be controlled and monitored and the level of federal preemption. Specifically, should the federal law establish a "floor" of minimum privacy protection standards -- in which case, states could exceed federally-set standards; or should federal law create a "ceiling" of standards, under which all entities must be in compliance and which cannot be exceeded by the states? (Jones, 1998). In her 1997 recommendations to Congress, Secretary Shalala addressed the preemption issue by asserting that the federal health privacy legislation should supersede state law that is less protective than the federal law; i.e., the federal law should provide "floor preemption." However, during the past year, the preemption of state laws is the trend that has emerged amongst all of the majority party bills on medical privacy: all would preempt state law.

The Jeffords, Condit and Shays bills allow preemption exceptions for state laws that cover mental health and public health activities (Jones, 1998). The Medical Information Protection Act of 1998 (S.2609), introduced by Sen. Bennett (R.-Utah) in early October 1998, carries no exception to preemption of existing state laws, not even for laws regarding HIV status or mental health records.

Also at the federal level, all of the pending major "patient protection" bills contain confidentiality provisions.[13] The House Patient Protection Act of 1998 (H.R. 4250) includes specific provisions related to

[12] The National Association of Insurance Commissioners has, in draft form, a "Health Information Privacy Model Act," which includes such privacy elements as: definitions of protected health information, disclosures of protected health information; conditions for scientific, medical and public policy research and sanctions for the unauthorized collection, use or disclosure of protected health information (September 14, 1998, draft).

[13] Reference is made to several "patient protection" bills currently pending, including S. 2330 (Senate Republican bill); S. 1890/H.R. 3605 (Kennedy-Dingell) and S. 2416 (Chafee).

medical records privacy and the confidentiality of health information and addresses certain parameters for the disclosure of health information.[14] Privacy advocates believe that establishment of confidentiality provisions is better served under a separate law, rather than as part of the patient protection law (Jones, 1998; Rybowski, 1998).

STATE LAWS -- MEETING THE CHALLENGE

Although it still remains to be seen as to what specific actions Congress will take, the states have a range of state medical records laws, most of which are not comprehensive in nature.[15] In general, medical privacy protections are contained in medical and other professional practice acts, and in hospital and other institutional licensure laws. Many reporting and confidentiality laws are condition-specific, i.e., laws that focus on confidentiality based on diagnosis (such as HIV/AIDS, mental health), or they relate to the activities of specific entities (such as hospital or public health department records). The scope of the laws and applicable sanctions vary widely across the states. Robert Gellman, a privacy and information policy consultant reports that "most but not all states impose a duty to maintain confidentiality on physicians. Fewer impose a similar requirement on other health care providers; nine have confidentiality requirements for employers and only four impose requirements on insurers" (Skolnick, 1998).

At present, all states have separate statutes providing confidentiality of information for those infected with HIV; each state also has a statute addressing the confidentiality of general health care information; and most have a separate statute defining the confidentiality of mental health and substance abuse treatment records and information (ibid.).[16] Service provision by physicians, dentists and other health care practitioners is directly affected by the variation in state laws, especially in border states such as New Jersey and New York. Currently, for example, a provider practicing in both New Jersey and New York and treating HIV/AIDS patients is faced with meeting different state law requirements: while New York's AIDS statute primarily deals with confidentiality, New Jersey's statute focuses on the reporting of diagnosed cases of AIDS or HIV infection, as well as the maintenance of confidentiality (Tamborlane & Kunz, 1998).

Over 250 bills that refer to medical records have been introduced at the state-level in 1998. Thirty-five states identified the issue as a focus for legislative consideration during the past year. The state of Minnesota's comprehensive privacy law (effective January 1997) received national attention with requirements which include that: providers notify (in writing) all patients seeking medical care that medical records may be released for research and that the patient may object; and on request, providers must inform subjects whose records were released and tell them how they can contact investigators. According to Herstek (1998), there was physician-provider concern that the Minnesota law created difficulties for providers and research entities when trying to access medical information for research purposes (*New England Journal of Medicine*, 1997).

In their legislative activity, most states are trying to target the confidentiality issue, but with an awareness that medical research requires access to the same information. The state of Vermont is an example of one in which much focus has been on creating a comprehensive medical privacy law that "has the right balance" so as not to compromise the needs of medical researchers. The bill did not pass through the last legislative session because consensus could not be met as to "the amount of access to medical records given to law enforcement" (ibid.). In 1998, the state of Maine did pass a comprehensive medical records law, which establishes confidentiality and security safeguards, including informed consent provisions.

In a January 1998 interview in *New Jersey Medicine*, Dr. Leah Ziskin (deputy commissioner with the New Jersey Department of Health and Senior Services) identified the "use of technology, and especially computerization, as a tool for information and monitoring," as one of the major accomplishments in the area of public health in the state (Berlin, 1998). She cited the state's electronic birth certificate program, and its AIDS and HIV registries as examples of this accomplishment.[17] While pointing out that registries are used with non-identifiers and congregate numbers, she acknowledges that confidentiality emerges as a major issue.

[14] Reference is made to New Jersey Policy Forums Issue Brief No. 26, "Free Market or "Free-For-All": Competition, Regulation and Consumer Protections," for information on patient protection legislation (June, 1998).

[15] Rep. William Thomas (R.-CA), chairman of the House Ways and Means Health subcommittee, in speaking at Congressional hearings on records privacy stated that a "crazy quilt" pattern of state privacy laws will emerge if states are given the authority to pass their own laws (Gardener, 1998).

[16] Federal laws do cover the privacy of drug and alcohol treatment centers that receive federal funds, but only a small number of health records are protected in this way (Skolnick, 1998, quoting R. Gellman.)

[17] A specific law regarding the testing of persons believed to be infected with the AIDS virus and the reporting of such test results to public health agencies was passed in New Jersey in the early 1980s. The law addresses how records of such persons should be kept and who would have access to this information. (N.J.S.A. 26:5C-5 through 26:5C-14.)

New Jersey is a state with statutes regarding the confidentiality of health care information for specific health conditions, such as AIDS and mental health, as well as provider confidentiality laws and medical reporting requirements for public health activities. Current legislative activity in the state of New Jersey includes Senate Bill No. S323 (Senator Littell), a medical records bill aimed at promoting the development and use in New Jersey of health care information electronic data interchange (EDI) technology. The bill was introduced in January of 1998; the Assembly Health Committee report was released on October 5, 1998. Under the bill, recommendations of the Healthcare Information Networks and Technologies (HINT) report would be implemented.

On the front of consumer protection bills, Senate Bill No. 766 (Senators Codey and Sinagra) was introduced in February 1998. The "New Jersey Health Care Consumer Information Act" would require that the State Board of Medical Examiners collect specific information to create a profile of each physician and podiatrist licensed to practice in the state, including any criminal convictions or malpractice judgments. On request, the Board may distribute the profile information to the public. The purpose of the bill "is to enable health care consumers to make informed choices about their physicians and podiatrists in a way that is not prejudicial or unfair to physicians or podiatrists." The bill amends the confidentiality provisions of P.L. 1983, c. 248 (C.45:9-19.3) and P. L. 1989, c.300 (C.45:9-19.10) to allow the Board to release this information to the public.

SUMMARY REMARKS

As one analyst noted when discussing the complex issues of medical privacy in the dynamically evolving health care system: "Technology is the right arm of health care and its Achilles' heel" (Skolnick, 1998).[18] The fundamental challenge confronting policy makers and health industry players is to identify how to use the tools of sophisticated technology to design efficient health information systems that safeguard privacy and the confidentiality of health information. And while doing so, to preserve the rights, values and professional and personal ethics that are essential components of a functional health care system. At present, with several national medical privacy bills in motion, it is still to be seen which course will be taken for a national standard. Unknown as well is how decisions at the federal level will affect state laws concerning privacy and confidentiality.

[18] Richard Harding, MD, member of Presidential Committee to develop legislation for protecting the confidentiality of medical records (Skolnick, 1998).

POLICY IMPLICATIONS

The enrollment of exponential numbers of Medicaid, and to a somewhat lesser degree, Medicare beneficiaries, into HMO managed care plans has exposed already-vulnerable clients with even more exposure to contract vendors and providers. Most analysts agree that for Medicaid managed care "to work," a comprehensive and tightly monitored clinical case management system must be in place. A system of this type demands detailed record-keeping, including medical management and information sharing with multiple players. How will these large public programs – on both national and state levels -- ensure that privacy and confidentiality safeguards are being employed to the protection of their beneficiaries? How can situations like the widely publicized Maryland case -- in which Medicaid clerks in Maryland were prosecuted for selling computerized records of recipients' financial resources to sales representatives of managed care companies -- be avoided?

The industry of pharmacy benefit management companies has established electronic links to most pharmacies throughout the country. A recent *Washington Post* article offered an analysis of the industry, which monitors prescriptions and prescription card usage in the over $81 billion prescription drug industry (September 27, 1998). Privacy advocates point out that "a growing number of patients, doctors and pharmacists complain that they never gave explicit approval for personal information to be collected and analyzed." Several states, including Ohio, New York and Virginia are focusing on laws that would give states more control over pharmacy benefit managers (several of which are owned by pharmaceutical companies), who have been known to contact patients on anti-depressant medication and offer them alternative medications or mental health programs. Is this a trend that should be monitored in New Jersey as well?

Sociologist Amitai Etzioni has written about the issue of HIV testing of newborn infants framed by the privacy rights of the mother, on the one hand, to the care of the newborn and the benefits of public health, on the other. He points out the many oppose the unblinding of HIV testing on newborns, because it would violate the mothers' legal right to privacy. Keeping the blind testing, he argues, would "directly contribute to the death of a significant proportion of infants born to mothers who have HIV," as the infants would not receive beneficial treatments early (in addition to other public health reasons) (1998). How are these ethical values and legal rights to be ranked in the broader public policy debates of nonidentifiable health data collection and usage? Where should the conversation begin?

In his statement during Congressional hearings this spring, Health Insurance Association of America[19] president Charles N. Kahn, asserted that proposed federal laws must not add another "layer" of administrative requirements on industry activities, but should "preempt most state laws affecting the insurance industry." He elaborated that uniform national standards for confidentiality are necessary to avoid a dual regulatory structure for medical records, pointing out that "state authority should remain paramount with regard to areas that do not conflict with national uniformity and consistency, such as state reporting requirements for public health and safety." How does this industry view "fit in" with state policymakers' positions on states' authority and federal preemption?

Based on a 1994 American Civil Liberties Union (ACLU) survey, which found that 75 percent of the public is concerned about health insurers' ability to put medical information about them into databases accessible by others, the group advocates that the public should be able to have "paper-only" records of its health care services, rather than being included in large computerized databases. Is this a viable alternative to be considered by policymakers?

Groups on both sides of the privacy issue -- that is advocating for either more stringent or less stringent mandates -- are in agreement that they oppose a proposal to create a national patient identifier, as had been described under HIPPA[20]. Such an identifier would be able to track each individual "from cradle to grave." Critics believe it would make access to personal health information too easy for anyone to review and interest has, at present, waned on pursuing such a unique health identifier. Is there a way to make such information secure in New Jersey as a means to facilitate public services and conduct public health research?

[19] The Health Insurance Association of America has over 250 member companies that provide health, long-term care and disability-income to their covered lives.

[20] Reference is made to a July 30, 1998, Washington Post article by Robert O'Harrow, Jr., "White House to Delay Health ID Plan on Privacy Concerns."

REFERENCES

Allen, Arthur. “Medical Privacy? Forget It!” *Medical Economics*. May 11, 1998.

Benjamin, Georges C. and S. A. Kennan. “Health Data Privacy.” *The Physician Executive*. November-December 1997.

Bennett, Colin J. Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Cornell University Press. 1992.

Berlin, Bill. “Interview with Leah Z. Ziskin, MD, MPH.” *New Jersey Medicine*. January 1998.

Edgar, H & D. J. Rothman. “The Institutional Review Board and Beyond: Future Challenges to the Ethics of Human Experimentation.” *Milbank Quarterly* 1995.

Etizioni, Amitai. "HIV Testing of Infants: Privacy and Public Health." *Health Affairs*. July/August 1998.

Frawley, Kathleen & D. D. Asmonga. "Privacy and Confidentiality Issues Dominate Federal Legislative and Regulatory Agenda." *Journal of AHIMA*. October 1997.

Gardener, Jonathan. "Congress Split on Patient Privacy." *Modern Healthcare*. March 30, 1998.

Gesensway, Deborah. "How to Keep Electronic Records Private? New Laws and High-Tech Solutions Might Work, But What is The Downside?" *ACP-ASIM Observer*. September 1998.

Goldman, Janlori. Director, Health Privacy Project. Testimony on “The Consumer Protection And Medical Record Confidentiality Act of 1998” authored by Congressman Chris Shays (R-CT); before the U.S. House of Representatives. Subcommittee on Government Management, Information and Technology of the Committee on Government Reform and Oversight. May 19, 1998.

Herbert, Bob. "What Privacy Rights?" *The New York Times*. Op-Ed. "In America".September 27, 1998.

Herstek, Jacob. "Issue Brief: Medical Records."National Conference on State Legislatures. Health Policy Tracking Service. October 1998.

International Society for Pharmacoepidemiology. "Data Privacy, Medical Record Confidentiality and Research in the Interest of Public Health." September 1997; amended August 1998.

Jones, Nora S. “Protecting the Confidentiality of Health Information.” *Issue Brief No. 724*. National Health Policy Forum. The George Washington University. September 18, 1998.

Kahn, Charles N. Health Insurance Association of America. Chief Operating Officer. Testimony on “The Consumer Protection And Medical Record Confidentiality Act of 1998” authored by Congressman Chris Shays (R-CT); before the U.S. House of Representatives. Subcommittee on Government Management, Information and Technology of the Committee on Government Reform and Oversight. May 19, 1998.

Katz. J. “Do We Need Another Advisory Commission on Human Experimentation?”*Hastings Center Report*. 1995; 25(1).

Lewis, Charles. Statement. July 1998. On "Nothing Sacred: The Politics of Privacy." The Center for Public Integrity.

Lowrance, William W. Privacy and Health Research. A Report to the U.S. Secretary of Health and Human Services. May 1997.

National Association of Insurance Commissioners. *Health Information Privacy Model Act*. Draft. September 14, 1998.

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

O'Harrow, Robert. "Plans' Access to Pharmacy Data Raises Privacy Issue. Benefit Firms Delve Into Patient Records." *The Washington Post*. September 27, 1998.

Olson, Lee A., S.G. Peters & J. B. Stewart. "Security and Confidentiality in an Electronic Medical Record." *Healthcare Information Management*. Spring 1998.

Rybowski, Lise. "Protecting the Confidentiality of Health Information." Background paper. National Health Policy Forum. The George Washington University. July 1998.

Silberner, Joanne. "Remodelling IRB's." *Hastings Center Report*. July-August 1998.

Skolnick, Andrew A. "Opposition to Law Officers Having Unfettered Access to Medical Records." *JAMA*, January 28, 1998.

Talley, C. Richard. "Confidentiality of Patient Records." *American Journal of Health-System Pharmacists*. May 1, 1998.

Tamborlane, Theodosia A., and D. A. Kunz. "UPDATE: New Jersey AIDS Testing, Reporting and Confidentiality Requirements." *Journal of the New Jersey Dental Association*. 68-2. 1998.

United States. Congress. Office of Technology Assessment. "Protecting Privacy in Computerized Medical Information." 44. 1993.

United States. Department of Health and Human Services. Testimony of Donna E. Shalala before the Senate Committee on Labor and Human Resources. September 11, 1997.

Woodward, Beverly. "Letter to the editor, *New England Journal of Medicine*; re: medical research." *New England Journal of Medicine*. April 9, 1998.

The New Jersey Policy Forums acknowledges the help of Zoe Hudson, Policy Analyst, Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, for her assistance in researching this issue brief.
