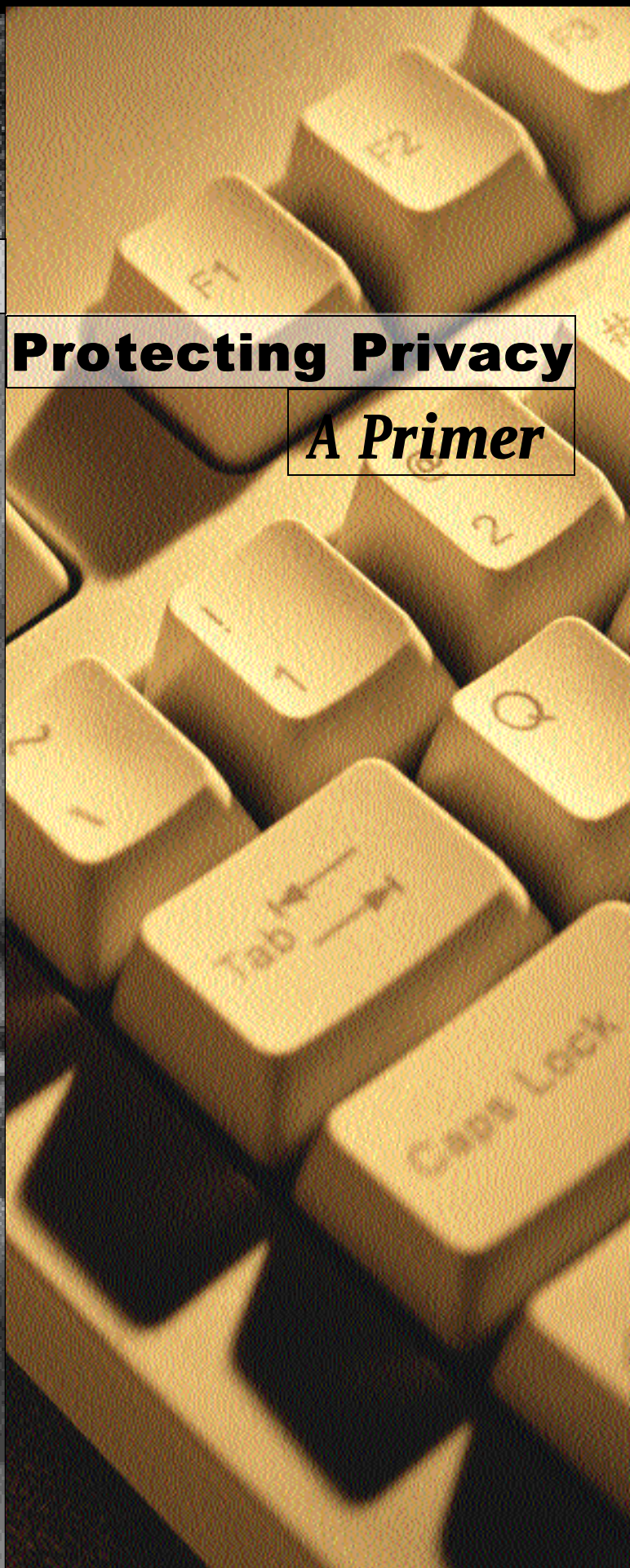
California HealthCare Foundation and Consumers Union

Promoting Health

Protecting Privacy

A Primer



January 1999

Promoting Health/Protecting Privacy: A Primer was prepared for the California HealthCare Foundation and Consumers Union. It was written by Janlori Goldman and Zoe Hudson of the Health Privacy Project at Georgetown University. Robert Mittman at the Institute for the Future also contributed to the writing of this Primer and it was edited by Lise Rybowski at the Severyn Group.

The Health Privacy Project
The Health Privacy Project's mission is to raise public awareness of the importance of health privacy to improving health care, both on an individual and a community level. Founded in 1997, the Project is part of Georgetown University Medical Center's Institute for Health Care Research and Policy. The Project receives support from the Robert Wood Johnson Foundation, and the Open Society Institute, as well as the Glen Eagles Foundation, the Kellogg Foundation and the California HealthCare Foundation.

Contact: Health Privacy Project, IHCRP, Georgetown University, 2233 Wisconsin Avenue NW, Suite 525, Washington, DC, 20007; Tel: (202) 687-0880; Fax: (202) 687-3110; http://www.healthprivacy.org.

California HealthCare Foundation
The California HealthCare Foundation is a nonprofit philanthropic organization based in Oakland California. The Foundation was established in May 1996, as a result of the conversion of Blue Cross of California from a nonprofit health plan to WellPoint Health Networks, a for-profit corporation.

The Foundation focuses on critical issues confronting a changing health care marketplace: managed care, the uninsured, California health policy and regulation, health care quality, and public health. Grants focus on areas where the Foundation's resources can initiate meaningful policy recommendations, innovative research, and the development of model programs.

Contact: California HealthCare Foundation, 476 Ninth Street, Oakland, California 94607; Tel: (510) 238-1040; Fax: (510) 238-1388; http://www.chcf.org.

Consumers Union West Coast Regional Office
Consumers Union, publisher of Consumer Reports, is a nonprofit membership organization chartered in 1936 to provide consumers with information, education, and counsel about goods, services, health and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers.

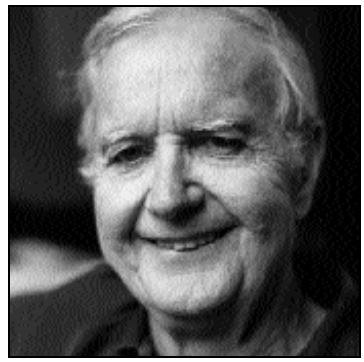
The West Coast Regional Office (WCRO) is one of three regional advocacy offices established to represent consumer interests on a variety of public policy issues, including: health care, credit and finance matters, food availability and marketing, corporate accountability, and auto and homeowners insurance. In the area of health policy, the WCRO has worked on Medicaid reform; implementation of the new children's health insurance program, the Healthy Families Program; legislation protecting consumers enrolled in managed health care plans; and the conversion of nonprofit health care institutions into for-profit companies.

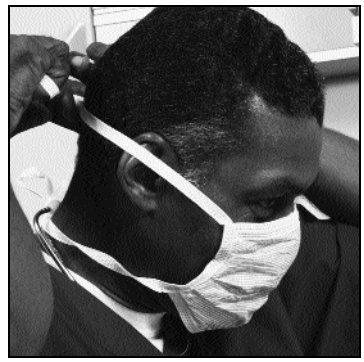
Contact: Consumers Union, 1535 Mission Street, San Francisco, California 94103; Tel: (415) 431-6747; Fax: (415) 431-0906; http://www.consunion.org.

Contents

The Terrain

THROUGHOUT OUR HISTORY, PRIVACY HAS BEEN A CHERISHED RIGHT, ALTHOUGH AN OFTEN ELUSIVE CONCEPT. PRIVACY INCLUDES NOT ONLY THE "RIGHT TO BE LET ALONE" BUT ALSO THE RIGHT TO DECIDE WHEN AND WHERE TO ENGAGE WITH INDIVIDUALS AND SOCIETY. THESE TWO FACES OF PRIVACY ALLOW PEOPLE TO DECIDE WHEN TO STEP FORWARD TO PARTICIPATE IN SOCIETY AND WHEN TO RETREAT.





In the health care arena, the desire for confidentiality of medical information and communication has been an essential element of the relationship between patients and health care professionals. At the same time, initiatives to improve individual and community health depend on accumulation of, and access to, complete and reliable information.

The long-standing tension between these two goals has been heightened by concerns about rising health care costs and by the rapid transition to a managed-care dominated health care delivery system. In traditional fee-for-service settings, patients interacted with fewer providers, records were maintained on paper in individual physicians' offices, and insurers generally asked only for the information needed to pay claims.

Contrary to popular belief, the information people share with their doctors has never remained completely private. Paper records are routinely shared with other parties, but they place natural limits on the large-scale use and disclosure of health information. While information can be protected more effectively in electronic form, it also raises new questions about the use and dissemination of health information.

As the public's fear and anxiety over loss of privacy grows, people face a conflict over whether to share information with their health care providers or avoid seeking care in order to shield themselves. At stake is the quality of care people receive, as well as the integrity of information needed to improve the health of the larger community.

Thus, promoting health and protecting privacy are values that must go hand-in-hand.

Existing Law is Inadequate

There is no federal law that protects the confidentiality of medical records, unlike credit reports or video rental records. Instead, a patchwork of state laws governs what information is available and to whom. Even California's health privacy laws, though stronger than the laws in most states, do not address all of the circumstances in which patient information changes hands. Nevertheless, many consumers may be unaware of existing protections and rights with regard to their medical records.

The Clock Is Ticking: Deadline Approaches for Federal Health Privacy Law

While concerns about privacy are not new, there is a new urgency to identify enforceable, workable rules about the use and disclosure of personal health information. The Health Insurance Portability and Accountability Act (HIPAA), passed by Congress in 1996, includes a deadline for enacting federal privacy rules.

HIPAA requires that if Congress fails to pass comprehensive health privacy legislation by August 1999, the Secretary of Health and Human Services must issue regulations by February 2000.

Urgency to Establish Protection

There is some urgency to identify common ground on the use and disclosure of personal health information:

- **Congress is under a self-imposed deadline to pass a comprehensive health privacy law (see sidebar). Through regulations or legislation, providers, health insurers, consumers, researchers, and others will soon feel the impact of new rules regarding the confidentiality and security of personal health information. Under some federal proposals, state legislatures would be prohibited from enacting stronger health privacy protec-**

We are at a decision point. Depending on what we do, revolutions in health care, biotechnology, and communications can hold great promise or great peril. We must ask ourselves: Will we harness these revolutions to improve, not impede, health care? Will we strengthen, not strain, the very lifeblood of our health care system—the bond of trust between a patient and a doctor? When all is said and done, will our health care records be used to heal us or reveal us?

—Confidentiality of Individually Identifiable Health Information, Recommendations of the Secretary of Health and Human Services, September 11, 1997.

tions in the future.

- The California Legislature continues to consider legislation to protect the confidentiality of personal health information. Since the 1980s, in response to the HIV epidemic, the State Legislature has passed some of the strongest confidentiality laws in the country to encourage people to seek testing and treatment. More recently, the Legislature passed a law that prohibits insurers from using genetic information in underwriting and rating decisions and provides heightened confidentiality protections for genetic tests.
- The European Union (EU) passed a Data Protection Directive that took effect in October 1998. The scope of the Directive reaches beyond the EU's borders—it prohibits the transfer of personal information to any country, including the U.S., that lacks "adequate" levels of protection. The centerpiece of the Directive is a provision that voluntary, express consent of the data-subject is necessary before personal information can be used or disclosed. The U.S. is unlikely to pass the adequacy test given the absence of a federal health privacy law or a sector-wide set of enforceable privacy policies and regulations.

The Challenge

This primer provides a broad overview of the major issues related to health privacy. To ensure that our health care system serves to both promote health and protect privacy, a renewed and cooperative dialogue must take place among consumers, providers, health plans, employers, researchers, and other stakeholders to determine how, when, and with whom patient information should be shared.

The Health Care Landscape in California

California is on the leading edge of many of the health care trends identified in this primer. Its population's diversity, highly organized health care delivery system, sophisticated purchasers of health care, and high use of managed care, both for publicly and privately insured people, make it a unique laboratory for health care information privacy. Several characteristics are worth highlighting:

The Safety Net is moving to managed care.

In California, managed care involves not just the privately insured, but those covered by publicly funded health plans, as well. Medicare managed care, which covers about 15 percent of the Medicare population nationally, reaches almost 40 percent of Californians. In some counties, that share exceeds 50 percent. In 12 California counties (largely those with the highest populations) Medi-Cal, which provides coverage for various low-income populations, has gone to a managed care model for some populations (specifically those linked to the program through welfare).

Large purchasers drive managed care.

In part, the growth of managed care in California has been driven by the priorities of large purchasers of health care. Notably, the Pacific Business Group on Health, which represents 34 of the largest employers in California; and the California Public Employees Retirement System, which provides insurance coverage for more than one million publicly employed Californians, have been prime movers in the growth of managed care in the state. Their interest in comparing the quality and clinical outcomes of the managed care services they purchase has pushed MCOs to make more systematic use of information.

Managed care is the mainstream.

California is the cradle of managed care and continues to be a source of innovation and development. Nationally, about 25 percent of the population are in HMOs (many others are in PPOs and other forms of managed care). In California, that share is closer to 40 percent. In certain metropolitan areas in California, such as Sacramento, managed care penetration exceeds 65 percent. Managed care is no longer the exception; it is the mainstream way of delivering care.

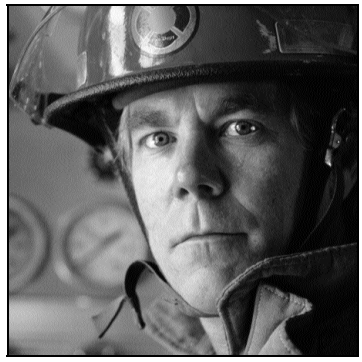
California's population is diverse.

California has more ethnic, income, educational, and technological diversity than anywhere else in the country. Statewide, non-Hispanic whites, who represented 75 percent of the population in 1970, will represent less than 50 percent of the population by 2000. Health care providers must offer services for immigrants from around the world—with a range of languages and cultural attitudes toward medical care and sharing of information.

Health care companies are consolidating.

Health care organizations in California always have been large. Kaiser Permanente, the largest health plan in California, covers 5.5 million Californians. Other large health plans have merged—HealthNet with Foundation, PacifiCare with FHP, and so on. At the same time, large physician groups have been forming and merging, as well. These larger health care organizations have the capital and management resources to put in place sophisticated health care information systems.

What's Driving Concern About Health Care Privacy?



FEW ARE UNAFFECTED BY THE IMPACT OF NEW TECHNOLOGY AND CHANGES IN THE FINANCING AND DELIVERY OF HEALTH CARE. MORE THAN 20 MILLION CALIFORNIANS ARE ENROLLED IN MANAGED CARE, REPRESENTING 80 PERCENT OF THOSE WITH INSURANCE IN THE STATE. MANAGED CARE HAS STIMULATED A DEMAND FOR PATIENT DATA THAT COULD BARELY BE IMAGINED A DECADE AGO.

Changes in Health Care Delivery

Managed care organizations (MCOs) operate on the principle that by monitoring and controlling patient care, they can deliver care more efficiently, and reduce costs. To achieve these objectives, many different people employed by or under contract with MCOs must analyze patient data for a wide variety of purposes, including:

- Utilization review (How are participating providers using services?);
- Risk management (Is the MCO being put at legal or financial risk?); and,
- Quality assessment (How can the MCO deliver better patient care and outcomes?).

Thus, in a managed care setting, not only do more people have access to personal health information, but it is also increasingly difficult to determine who has responsibility for protecting the confidentiality of this data.

Growing Uses of Health Care Information

Over the years, the number of health care organizations handling patient data has grown significantly *(See list in Appendix A)*. The growth of integrated delivery systems has led to the development of large, integrated databases of personal health information. With access to this data, people are discovering new and often improved ways to deliver effective care, identify and treat those at risk for disease, conduct population-based research, assess and improve quality, detect fraud and abuse, and market their services.

Not surprisingly, these uses may conflict with the desire of patients to keep their information private. Some common uses include the following:

- **Managing Disease**
  Disease management programs aim to improve care by targeting people with certain conditions for education, help with drug compliance, and preventive measures. A health plan, employer or pharmaceutical company may initiate the programs, generally requiring that patient data be shared well beyond the treating doctor.

- **Conducting Research**
  Hospital records have long been a rich source of data for research—from clinical trials to epidemiological, public health, cost, and efficiency studies. MCOs—whose data files also represent thousands of patients—offer opportunities for both public and private sector researchers to collect and analyze data on a cross-section of the population.

- **Ensuring Quality and Accountability**
  Over the past several years, an increasing number of employers, government agencies, and patients have been asking health care practitioners (including doctors, pharmacists, and health plans) for evidence that they are delivering high-quality care and taking steps to improve quality on an ongoing basis. This demand for accountability has:

  - Contributed to the adoption of information systems and technologies in the health care industry;

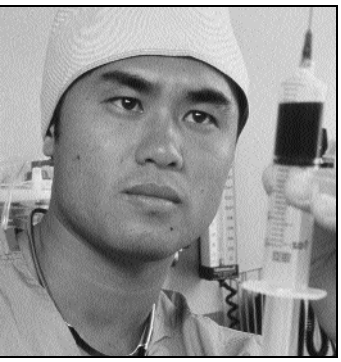
What Are Managed Care Organizations?

Managed Care Organizations (MCOs) is a catch-all term that encompasses many different types of health care financing and delivery systems: health maintenance organizations, preferred provider organizations, independent practice associations, and others.

> [The] importance of medical record information to those outside of the medical care relationship, and their demands for access to it, will continue to grow. Moreover, owing to the rising demand for access by third parties, coupled with the expense of limiting disclosure... there appears to be no natural limit to the potential uses of medical record information for purposes quite different from those for which it was originally collected.
>
> —Personal Privacy in an Information Society, U.S. Privacy Protection Study Commission, 1977.

- Raised concerns among health plans and providers about how to track the outcomes of care and to take steps to better manage the care they provide; and
- Spurred the development of independent organizations that can evaluate and verify the quality of health plans and providers.

Measuring outcomes, providing performance measures and managing patient care are data-intensive activities that depend on access to patient data.



■ Investigating Fraud and Abuse

Fraud and abuse are well-documented problems in the health care industry. Investigations often require access to patient records.

■ Monitoring Public Health

In order to track and promote public health, government agencies require that providers report certain health information, such as cases of infectious disease, immunization, or violent incidents on an ongoing basis.

■ Increasing Government Oversight

At both the state and federal level, government regulators have sought to exercise greater oversight of the health care industry in general—and MCOs in particular. While statistical summaries are sufficient for much of this oversight activity, information that identifies individual patients is sometimes sought.

■ Expanding Commercial Activities

Patient information has commercial value for those able to identify and harness the marketing opportunities. This is one of the most controversial uses of health information, particularly by entities not directly involved in patient care.

New Technologies: Benefits and Risks

Historically, the physical limits of the medical record itself provided a modicum of protection against broad disclosure, but at times also prevented providers from getting information quickly and efficiently. Paper records are burdensome: An individual's medical information can be kept in several different places, notes are written by hand, and sensitive information can be buried in a chart. Consequently, it has often been expensive and difficult to consolidate and share information.

Harnessing the Power of the Internet

The Internet offers an unprecedented opportunity to transmit and share information quickly, relatively easily, and with few start-up or infrastructure costs. However, it has not been established that the Internet can provide an adequate level of personal privacy and technological security. As such, many health care organizations have not taken advantage of these capabilities.

Compared to other industries, health care organizations have yet to take full advantage of new information technologies. Nevertheless, technological developments have already had a profound impact on health care:

■ Clinical Care

In some integrated networks, physicians are electronically linked to insurance companies, laboratories, and hospitals. In these situations, patient information has

the potential to move seamlessly, making it easy to process claims, prescribe medications, check test results, and monitor care. These kinds of systems often become available to practitioners through their participation in a health plan or integrated delivery system. In some cases, researchers or marketers offer software to provider groups at a discount in exchange for access to patient data.

- **Patient Education**

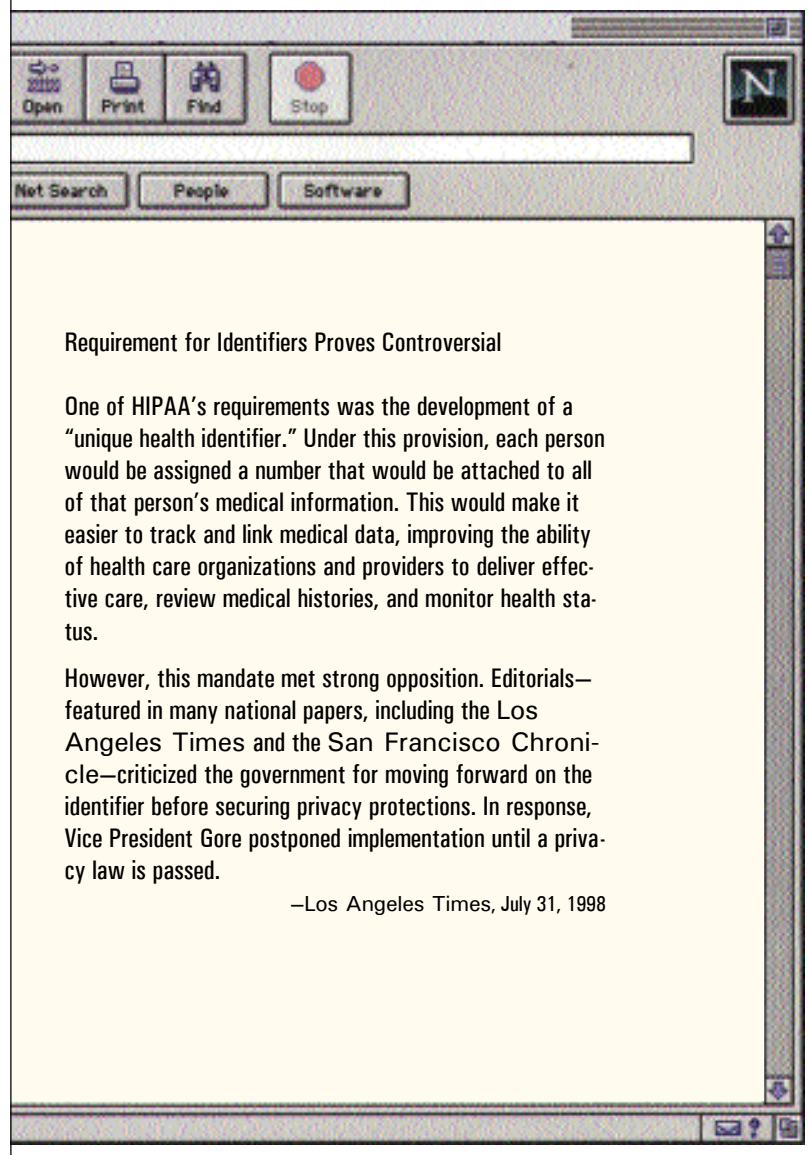
  Health plans, disease-specific groups, professional associations, and commercial health interests are beginning to use technology to inform, and interact with consumers. For example, through interactive Web sites and e-mail, members of some health plans can make appointments, get advice from nurses, check on lab tests, or even participate in discussion groups focused on a particular medical condition.

- **Consumer Safety**

  Pharmaceutical companies and providers may be required to monitor the consumption and effects of drugs even after FDA approval. Diagnostic, prescription, and medical records data help to detect adverse reactions and measure effectiveness in real-life settings. While the information may not identify individual patients, it is sometimes encoded in a way that enables doctors, pharmacists, and others to contact patients in the event of a recall or other safety warning.

- **Outcomes Research**

  Access to clinical data allows researchers to track health status, measure outcomes, monitor patient care, and develop treatment programs over time and across populations in a way that was never before possible.



Technology offers many public health benefits. But it poses new privacy risks as well. Without strong privacy policies to define when and how personal health information may be shared, consumers may be vulnerable to unwanted disclosure of their information, exposure, and judgments. In the worst scenarios, the disclosure of personal health information may cause people to be discriminated against, fired from their jobs, or to be afraid to seek additional care and treatment.

The health care community has recognized that unrestricted access to patient records puts patient privacy at risk and can even compromise care. But without some access to patient records, the full public health benefits of new information technologies will not be realized.

In many ways electronic health information may be more securely protected than paper records by limiting access, monitoring users, and stripping data of personal identifiers before it is shared with third parties. At the request of the National Library of Medicine, the National Research Council conducted a study on privacy and security of health care information. Their report, published in 1997, found that the technology to protect data is readily available and not particularly costly. But the existence of such technological security measures does not ensure that every data user will properly and consistently use them. Nor does it answer the larger policy questions about how data should be used, shared, and exchanged.

In fact, the NRC concluded that there are few incentives to use privacy-enhancing technologies. Most health care organizations believe that, notwithstanding the Internet, the risk of a security breach is low. In the event of such a breach, they would survive with little consequence. Given competing demands for resources, few organizations are investing in privacy safeguards.

CALINX: Developing a Health Care Information Infrastructure in California

California is one of a handful of states leading the way towards the development of an industry-wide infrastructure for collecting and reporting health care information. With funding from the California HealthCare Foundation, a consortium of physician and hospital organizations, purchasers, and health plans (collectively known as CALINX) has joined forces to develop common data standards and rules to implement electronic data interchange (EDI). Through the convening of workgroups, task forces, and panels, CALINX is working to standardize the sharing and use of encounter data, laboratory and pharmacy records, enrollment and eligibility data, provider and provider group identifiers, plan member ID cards, and the provider credentialing process.

What's at Stake for Health Care Consumers?

Accessible health care information, used appropriately, can greatly enhance the quality and efficiency of the care we all receive. For instance, with improved access to medical records and other data;

- Consumers stand to benefit from improved outcomes through efforts to improve quality and increase accountability in health care;
- Physicians will be able to deliver emergency care more quickly and effectively;
- Insurers will be able to expedite claims and manage costs; and
- Provider organizations will be able to monitor, improve, and report on the outcomes of care.

Polls over the past two decades, however, indicate that the public is becoming increasingly concerned about privacy in general, and the confidentiality of medical records in particular. A 1995 Louis Harris & Associates poll found that 82 percent of people were concerned about their privacy, up from 64 percent in 1978. Nearly 60 percent of the public have at some point "refused to give information to a business or company" out of concern for privacy, up from 40 percent in 1990.

Evidence of "Privacy-Protective" Behaviors

Many people fear their personal health information will be used against them: to deny insurance, employment, and housing, or to expose them to unwanted judgments and scrutiny. After all, the information people share with their doctors is among the most sensitive. Medical records include family history, personal behaviors and habits, and even subjective information on mental state.

Uses of health information often extend beyond patients' current knowledge and expectations, giving rise to a profound sense of anxiety—especially when the uses are inconsistent with the original purpose for which the information was gathered.

In response, patients are developing a variety of "privacy-protective" behaviors to shield themselves from what they consider to be harmful and intrusive uses of their health information. To protect their privacy—and avoid embarrassment, stigma, and discrimination—some pay out-of-pocket for medical care for which they have insurance coverage. Others "doctor-hop" to avoid entrusting their medical record to a single provider or health plan. Still others withhold information, lie, or avoid health care altogether.

According to a 1992 survey by Louis Harris & Associates:

- 27 percent of the public believe they have been the victims of an improper disclosure of personal health information.
- In order to protect their privacy, 11 percent said that they or an immediate family member paid out-of-pocket for health care, rather than submit a claim.
- Seven percent chose not to seek care because they didn't want to harm their "job prospects or other life opportunities."

Example of Unauthorized Disclosure

The *San Diego Union Tribune* recently reported that Longs Drugs settled a lawsuit filed by an HIV-positive man. After a pharmacist inappropriately disclosed the man's condition to his ex-wife, the woman was able to use that information in a custody dispute. However, rather than pursue the suit against the pharmacy, the man chose to settle in order to avoid a court trial that could result in news coverage and therefore further disclosure of his illness.

—"Longs Drugs Settles HIV Suit," *San Diego Union Tribune* September 10, 1998.

Concern about Sensitive Topics

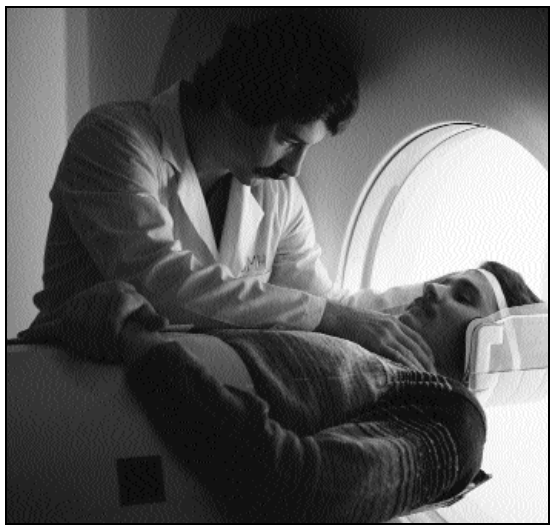
California law, as in many states, provides greater protection for HIV/AIDS, mental health, and genetic tests. The rationale is that some groups of people are especially vulnerable to the misuse of their health information, and the promise of confidentiality encourages people to get testing and seek treatment. Unfortunately, this condition-specific approach has some drawbacks:

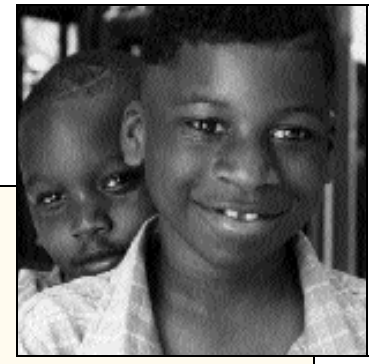
- **Addressing unique conditions is a quick fix.**
  Public policy has been enacted in reaction to serious threats to public health. As

each new threat is identified, we re-engage in the discussion about confidentiality. But these efforts have not served to create a cohesive framework for assuring a basic level of confidentiality for all health information.

- **Attempts to segregate health information may fail.**
  California law prevents providers from disclosing HIV status in a number of circumstances. But HIV status may be disclosed inadvertently. A pharmacy, for example, may share information about a prescription for AZT with a third party, effectively disclosing the diagnosis. Others have noted anecdotally that "blacked out" information on a medical chart can inadvertently indicate HIV status.

- **Sensitivity is subjective.**
  People are sensitive to disclosure for different conditions at different times and in specific circumstances. An asthma sufferer might welcome marketing information or greater coordination of care but someone recently diagnosed with diabetes, epilepsy, or depression may want greater control over access to her or his health records.





People Especially Vulnerable to Breaches of Privacy

Adolescents

Adolescents make a strong connection between their willingness to seek care and the ability of providers to keep their information private. Several research studies have found that adolescents are more inclined to communicate sensitive information, such as sexual activities, and seek health care when their physician assures them of confidentiality. Adolescents are particularly concerned about their parents' ability to see their medical records.

Immigrants

Immigration reporting laws, welfare reform legislation precluding recent immigrants from receiving public services, and efforts to identify undocumented immigrants through public benefit files, have led many immigrants to shy away from enrolling in programs for which they are eligible, and to choose between seeking care or possibly jeopardizing their immigration status.

Mental Health Patients

Fearing discrimination or stigma, many people pay out-of-pocket for mental health services and prescriptions, withhold information from primary care providers about medications they are taking, or ask physicians to miscode the diagnosis of mental health conditions. Consequently, claims databases have limited usefulness to researchers studying mental health.

HIV/AIDS

Numerous studies have found that people are less likely to get tested for HIV, or to avoid testing altogether, if their name will be reported to public health officials. For this reason, HIV advocates are encouraging the state to collect HIV information through a non-names based alphanumeric code number. In addition, in order to encourage people to seek testing and treatment for HIV/AIDS, every state has passed some legislation concerning the confidentiality of a person's HIV status.

Key Issues

SOME HEALTH PLANS, RESEARCHERS, DRUG COMPANIES, AND OTHERS FEAR THAT "TOO MUCH PRIVACY" WILL CHOKE THE FREE FLOW OF HEALTH INFORMATION, REDUCING THE AMOUNT OF DATA AVAILABLE FOR THEIR WORK. THROUGH THIS LENS, PRIVACY IS OFTEN VIEWED AS A STUMBLING BLOCK TO ACHIEVING OTHER HEALTH CARE-RELATED GOALS.

But without trust that the information they share with their doctors will be treated with some degree of confidentiality, patients may not reveal all pertinent information about their conditions. If health care providers receive incomplete, inaccurate information from their patients, the quality of care is compromised, and the data disclosed and used for payment, outcomes analysis, research, and public health reporting will reflect the same weaknesses.

In essence, information that lacks integrity at the front end will not be valid or reliable as it moves through the health care system. Thus, protecting privacy is critical to promoting health, fostering access to care, and improving the quality of care for individuals and their communities.

The following is a broad outline of the key issues in this debate.

Genetic Testing

- In a 1997 national survey, 63 percent of people reported that they would not take genetic tests for diseases if insurers or employers could access the tests.
- One-third of women invited to participate in a breast-cancer study using genetic information refused because they feared discrimination or loss of privacy.
- A pilot study documented 206 instances of discrimination as a result of access to genetic information, culminating in loss of employment and insurance coverage, or ineligibility for benefits.
- A number of states have passed laws to provide greater confidentiality protections for, and to prohibit discrimination based on, genetic tests.

—See *"Genetic Information and the Workplace,"* U.S. Department of Labor, January 20, 1998

Patient Access

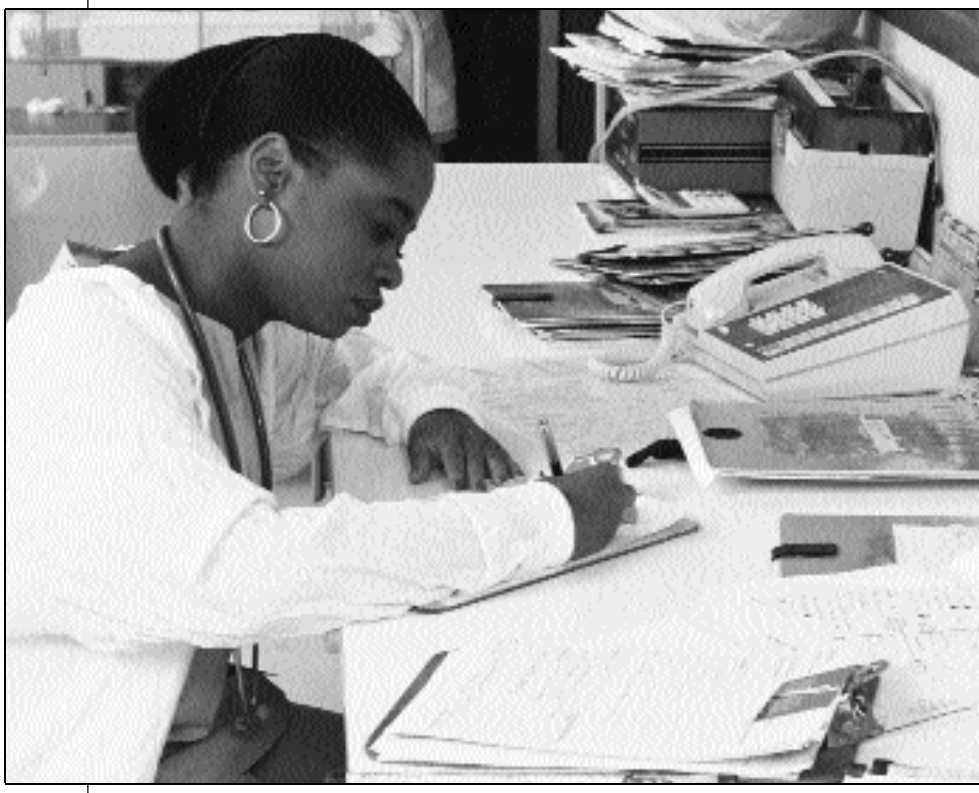
As more medical information is shared, it becomes increasingly important for consumers to understand the contents of their own medical record. California and 27 other states give individuals a right to see and copy their medical records. *(See Appendix B.)* Allowing patients to see their own medical records serves many purposes: It allows patients to better understand their care, flag incorrect information, supplement the record, and engage in a discussion with their provider or insurer about what information can be disclosed.

Consent

Today, most sign broad waivers that allow their medical records to be used in an almost limitless number of circumstances. Authorization for the disclosure of medical information may also be tied to authorization for treatment. In fact, in some circumstances, insurers and providers can condition treatment or enrollment in a health plan on receiving patient consent. The end result is that consumers do not know who will see their data and have little control over how their information is used.

At the same time, in today's managed care environment, it would be cumbersome to obtain a patient's consent each and every time medical information is disclosed. There are other activities—such as some reporting for public health purposes—which currently do not require patient consent.

Developing a meaningful consent process remains a challenge. Are there some activities that need not require authorization?



Under what circumstances should consumers be allowed to "opt-out" of or "opt-in" to disclosures? When and where should patient authorization be obtained: at the time of application, enrollment, treatment, or periodically? Should authorization be limited to the "minimum amount of information necessary" to accomplish the purpose?

Employer Access

Because many employers provide health care coverage—and sometimes health care—to employees and their families, employers are often privy to personal health information. Large employers who provide actual health care may use unidentified data to monitor costs, run employee wellness programs, and provide on-site medical care. In light of the strong connection between employers and health care, many consumers worry that employers might use health information against them in hiring, firing, and promotion decisions.

- In a 1998 national survey by the Kaiser Family Foundation, 89 percent of medium and large employers report that they require health plans to guarantee the confidentiality of employees' medical records. However, 30 percent of employers also report that they have access to medical records for case management or other similar situations.

  —KPMG Peat Marwick, November 1998

- The American Association of Occupational Health Nurses testified before the U.S. Senate that employers often pressure nurses to release a worker's entire medical record.

  —February 26, 1998

Currently, restrictions on employer access to employee medical information exist on the federal level under the Americans with Disabilities Act (ADA). The ADA prohibits employers from making employment-related decisions based on a real or perceived disability. It also provides that employers may have access to personal health information only for purposes of determining the employee's ability to perform the job or for a reasonable business necessity. This can include determining reasonable accommodation for non-obvious disabilities, or for the resolution of Worker's Compensation claims. On the state level, a court ruled recently that the California Constitutional Right to Privacy restricts employer access to certain medical information.

While the ADA extends critical protections to the disabled, its protections are not absolute. Employee claims of disability-based discrimination or unlawful medical inquiries continue to arise and both disabled and non-disabled employees must still pursue their claims at great cost and effort. Ultimately, privacy is the first line of defense against discriminatory misuse by employers of confidential medical information. Recognizing that current protections may not be sufficient, consumer and disability rights activists have advocated broader restrictions on employer access to and use of personal health information.

Government Use of Personal Health Information

Government at all levels plays many roles in the collection, use, and distribution of health care information:

- California's Medi-Cal program is one of the country's largest purchasers of health care.
- Federal and state public health officials gather, analyze, and distribute a wide range of information on infectious disease, cancer, violence-related injury, and other medical conditions.
- Law enforcement officials obtain medical information in criminal investigations.
- Agencies involved in health oversight use

patient records to combat fraud and abuse.

- One of the newest uses of medical information involves the reporting of quality measures to state and federal agencies to allow them to more closely monitor managed care organizations.

Most recent federal bills allow the release of patient medical records for fraud and abuse investigations. However, they differ in terms of whether they require patients to be notified of the disclosure and whether they specifically prohibit subsequent use of information obtained during an oversight investigation.

At present, federal law does not require law enforcement to present a warrant or subpoena before obtaining personal health information. Each proposal takes a different approach to the level of safeguards to put in place. Law enforcement officials have argued against any new restrictions on their access to patient records. But no federal privacy statute currently provides law enforcement with such a broad exception. In fact, most U.S. privacy laws were enacted specifically to bring law enforcement under the search warrant requirement of the Fourth Amendment.

Privacy Act of 1974

The Federal Privacy Act limits government agencies from sharing information with each other. But once information is collected for one purpose, the temptation to use it for other purposes is often irresistible. Recently, an anti-fraud program came under fire when the California Department of Human Services was accused of providing the Immigration and Naturalization Services with information about immigrants' lawful use of Medi-Cal services.

–California Healthline, August 8, 1998

Research

Currently, federal regulations regarding privacy apply only to researchers who receive federal funds or are conducting research in anticipation of FDA approval. The regulations require that prior to using identifiable health information, the research study must be approved by an

Institutional Review Board (IRB) and that participants give their informed consent; however, the law allows the IRB to grant a waiver of informed consent under a number of circumstances.

Increasingly, research is privately funded and may not involve direct contact with patients. As a result, more research that relies primarily on the patient record or "encounter data" is falling outside the scope of federal regulations. Also, expanding uses of medical information outside of the clinical setting are broadening the definition of "research." Research activities that involve review of medical information (such as for cost studies or outcomes analysis) often do not require direct contact with patients, and may not require patient-identifiable information. As such, they are often not subject to the federal regulations—including the informed consent requirement—that apply to other kinds of research, including clinical trials.

Almost every recent federal medical privacy bill requests a formal study of the issue to determine whether existing patient protections for research studies are adequate, and to identify what research falls outside current regulations.

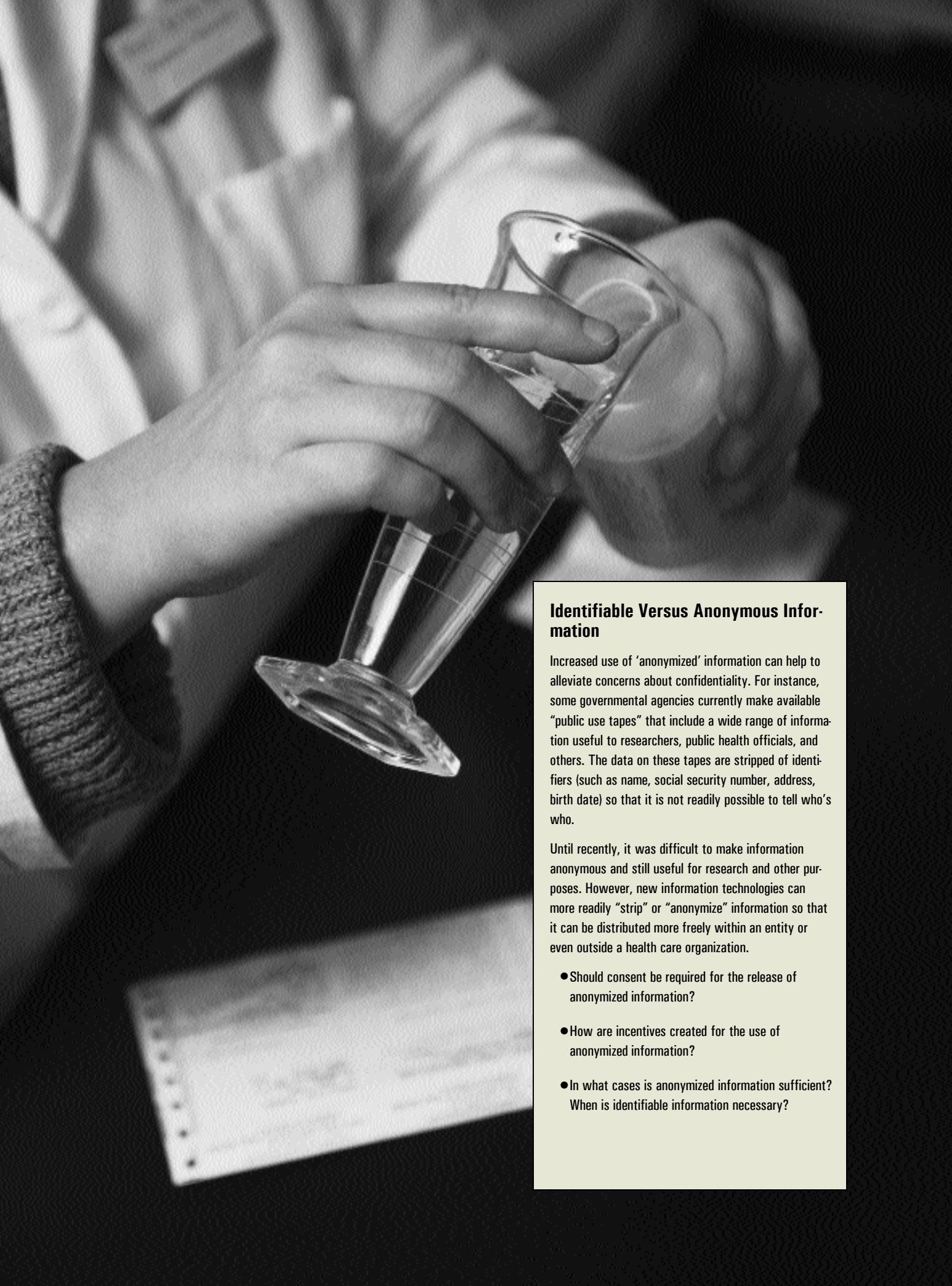
Data for Sale

Medical Marketing Service advertises a database available to pharmaceutical marketers that includes the names of 4.3 million people with allergies; 923,000 with bladder control problems; and 380,000 who suffer from clinical depression. (See http://www.mmslists.com)

Commercial Use

As with all personal information, there is a commercial value to personal health information. As more information is put in electronic format, it is becoming easier to harness patient data for commercial purposes.

Many consumers, however, do not welcome the use of their information, particularly outside the context of treatment or payment for care. Recently, public outrage led the chain drug stores CVS and Giant Food to abandon a marketing campaign in which they shared patient prescription records with a direct mail and pharmaceutical company. The stated goal was to send letters to customers encouraging them to refill prescriptions and to consider alternative treatments—but those customers had not agreed to this use of their information. (*Washington Post*, February 15, 1998.)



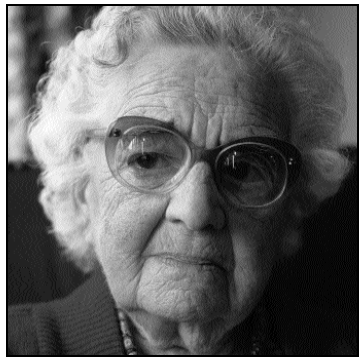
Identifiable Versus Anonymous Information

Increased use of 'anonymized' information can help to alleviate concerns about confidentiality. For instance, some governmental agencies currently make available "public use tapes" that include a wide range of information useful to researchers, public health officials, and others. The data on these tapes are stripped of identifiers (such as name, social security number, address, birth date) so that it is not readily possible to tell who's who.

Until recently, it was difficult to make information anonymous and still useful for research and other purposes. However, new information technologies can more readily "strip" or "anonymize" information so that it can be distributed more freely within an entity or even outside a health care organization.

- Should consent be required for the release of anonymized information?
- How are incentives created for the use of anonymized information?
- In what cases is anonymized information sufficient? When is identifiable information necessary?

The Public Policy Response



HEALTH PRIVACY IS NOT YET WIDELY REGARDED AS A CORE PART OF THE HEALTH CARE REFORM AGENDA, WHICH CENTERS ON EFFORTS TO IMPROVE QUALITY OF CARE AND ACCESS TO CARE. AT THE SAME TIME, MEDICAL PRIVACY IS A LEADING CONCERN OF CONSUMERS, AND THE STRONG EMPHASIS ON QUALITY—COMING FROM PURCHASERS, GOVERNMENT, AND CONSUMERS—CONTINUES TO DRIVE THE DEMAND FOR PATIENT DATA. GIVEN THESE COMPETING PRIORITIES, PROTECTING THE PRIVACY OF PERSONAL HEALTH INFORMATION IS EMERGING BOTH AS A CORE INFORMATION PRIVACY ISSUE AS WELL AS A CRITICAL HEALTH POLICY ISSUE.

Health Care Reform and Privacy

Two major accreditation organizations—the National Committee for Quality Assurance (NCQA) and the Joint Commission on Accreditation of Healthcare Organizations (JCAHO)—recently released a series of recommendations to address the increasing demands for health information. Both the NCQA and JCAHO have confidentiality requirements for the health care organizations that they evaluate and may revise these standards in the near future.

In the legislative arena, privacy is sometimes incorporated into larger health care reform initiatives.

- **Health Insurance Portability and Accountability Act (HIPAA)**
  HIPAA includes a major initiative to standardize health care transactions. A provision known as "administrative simplification" will facilitate the exchange, storage, and analysis of health information across entities. But this move towards standardization has raised serious privacy concerns. To reconcile these competing priorities, Congress voted to accept "administrative simplification" only if coupled with a self-imposed deadline to enact a federal health privacy law. *(See Appendix C for more on this.)*

- **Managed Care Reform**
  In November 1997, a Presidential Advisory Commission released a "Patients' Bill of Rights," which includes a provision on confidentiality. Several bills were introduced on the tail of this report, some of which also address the confidentiality of medical records.

Federal Health Privacy Proposals

Proposals to establish a federal health privacy law have been circulating for more than 20 years, but a consensus has yet to emerge on the details of such a law. Driven by the congressional deadline, legislators will soon have to address a number of complex issues and competing priorities in order to meet the deadline. Most of the federal bills include provisions on the following areas. *(For a more detailed discussion, please see Key Issues section):*

- **Patient Access to Medical Records:** When and how can individuals access, supplement, or amend their medical records?

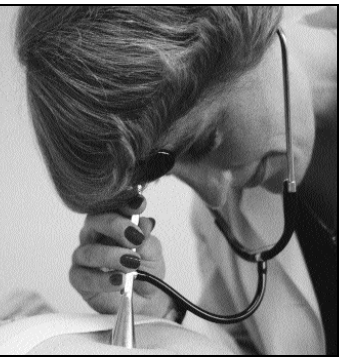
Timeline

1974
In the wake of Watergate, Congress enacts the Privacy Act of 1974, limiting the government's collection and use of personal information.

1970-1996
Congress passes laws to protect the privacy of education, credit, financial, communications, and video rental records.

August 1996
President Bill Clinton signs the Health Insurance Portability and Accountability Act, which includes a requirement that Congress pass legislation protecting the privacy of medical records by August 1999.

1997-1998
To meet the August 1999 deadline for health privacy legislation mandated by HIPAA, legislator introduced a number of comprehensive bills.



- Consent/Authorization: Under what circumstances, how, and how often should patient consent be obtained prior to the release of health information that identifies them individually?
- Use of Medical Records without Consent: When can information that identifies individual patients be released without patient consent?
- Notice: When and how should individuals be notified about how their medical records are used, and when their health information is disclosed to third parties?
- Research: Under what circumstances can personal health information be used for research?
- Law Enforcement Access, Oversight: Under what circumstances can law enforcement officials access personal health information? What safeguards or protections do individuals have when their personal health information is used in criminal investigations of providers, or for the purposes of health care oversight?
- Penalties: What penalties will apply to entities that violate the law? What remedies are available to individuals whose medical information was improperly disclosed?

Federal Preemption of State Laws

Each of the most recent federal bills takes a different approach to the issue of federal premption of state law. Some bills preempt state law. Other bills preserve state laws related to communicable disease, mental health, and public health. Since there is not yet a comprehensive compendium of state health privacy laws, the potential impact of federal preemption of state laws cannot be fully assessed.

Federal Proposals

The following health privacy bills were introduced in the 105th Congress:

H.R. 1815, Rep. McDermott (D-WA)

H.R. 52, Rep. Condit (D-CA)

H.R. 3900, Rep. Shays (R-CT)

S. 1368, Sens. Leahy (D-VT) and Kennedy (D-MA)

S. 1921, Sens. Jeffords (R-VT) and Dodd (D-CT)

S. 2609, Sens. Bennett (R-UT) and Mack (R-FL)

Copies of all bills can be found at http://thomas.loc.gov.

May 7,1998

Publication of Federal Register Notice of proposed federal standard for a National Provider Identifier.

May 7, 1998

Publication of Federal Register Notice of proposed federal standard for Administrative and Financial Transactions and Code Sets.

June 1998

Vice President Al Gore launches a privacy initiative, with medical privacy at the top of the list.

June 16, 1998

Publication of Federal Register Notice of proposed federal standard for a National Employer Identifier.

August 12, 1998

Publication of Federal Register Notice of proposed federal standard for Security Standards to protect health care information.

Health insurers, employers, researchers and others, have made a compelling case for national, uniform standards for the use and disclosure of health information. They argue that since the delivery and financing of health care frequently is coordinated across state lines, a single federal standard is easier and more cost-effective to administer in compliance with federal requirements.

However, the preemption of state privacy and civil rights laws by federal law is unprecedented. Customarily, the federal government establishes a minimum standard and allows states to enact laws that provide a greater level of protection for individuals.

Preemption of state law has proven to be an extremely contentious issue. The debate over preemption turns in part on how high the federal standard is set. Consumers worry that if the federal law sets a weak privacy standard and preempts state law, they will actually lose significant protections they have won at the state level.

August 1998

The Vice President halts federal action on the health identifier until Congress passes a health privacy law.

Also, shortly before the August 1998 recess, the House passes the Gingrich-Hastert "Patient Protection Act," which would broadly preempt certain state health privacy laws and allow health plans to share and disclose patient data for a wide variety of activities without patient consent. The bill does not receive attention in the Senate and dies when Congress adjourns.

November 1998

The Joint Commission on Accreditation of Healthcare Organizations and the National Committee for Quality Assurance release new recommendations: "Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment."

February 2000

Deadline for Secretary of Health and Human Services to issue regulations protecting health care privacy should Congress fail to meet its August 1999 deadline.

Consumers: What You Can Do Right Now

ABSENT STRONG STATE OR FEDERAL LAWS THAT PROTECT THE PRIVACY OF PERSONAL HEALTH INFORMATION, CONSUMERS TODAY MAY NOT KNOW HOW THEIR HEALTH INFORMATION IS USED AND SHARED. CONSUMERS WHO ARE CONCERNED ABOUT THE CONFIDENTIALITY OF THEIR HEALTH INFORMATION CAN TAKE STEPS TO LEARN ABOUT THE CONTENTS OF THEIR MEDICAL RECORD, THE USE OF THEIR HEALTH INFORMATION, AND OPTIONS FOR RESTRICTING DISCLOSURE.

- **Request a copy of your medical record.**
  California law gives individuals a right to inspect and copy records maintained by physicians; podiatrists; dentists; psychologists; optometrists; chiropractors; marriage, family, and child counselors; clinical social workers; hospitals and other licensed health facilities; clinics; and home health agencies. In the case of minors, the minor, and not the parent or guardian, may get access to records for treatment for which the minor is legally authorized to give consent. There are limited exceptions to this right, but providers may not deny access because they are owed money.

- **Request a copy of your file from the Medical Information Bureau.**
  The Medical Information Bureau (MIB) is a membership organization of more than 600 insurance companies. When applying for insurance, you may be authorizing the insurance company to check your records with MIB to verify that the information you have provided is accurate. MIB does not have a file on everyone. MIB reports are compiled on those with serious medical conditions or other factors that might affect longevity, such as affinity for a dangerous sport. If MIB has a file on an individual, that person has a right to see and correct the file.

- **Talk about confidentiality concerns with your doctor.**
  Your health care practitioner should be able to help you understand the uses of your health information, and may be able to offer certain assurances of confidentiality. For example, some practitioners keep treatment notes separate from the general medical chart to help ensure that the most sensitive information remains confidential. Your physician or caregiver may also be able to help you understand the current limits of confidentiality, such as what kinds of information he or she is required to provide for insurance purposes.

- **Read the authorization forms before you sign; edit them to limit the sharing of information.**
  Before you sign any forms, find out to whom you are authorizing the release of your medical records and for what purpose. You may be able to limit distribution and restrict secondary disclosures of the information by revising the authorization form. Be sure to initial and date your revisions.

- **Register your objection to disclosures that you consider inappropriate.**
  Registering objections may not result in immediate change, but sharing your concerns will help to educate your practitioners, plans, and others seeking health information. These entities should be aware that lack of privacy impacts how you seek and receive your health care.

- **Be cautious when providing personal medical information for "surveys," health screenings and on medical information Web sites.**
  Ask how the information will be used and who will have access to it.

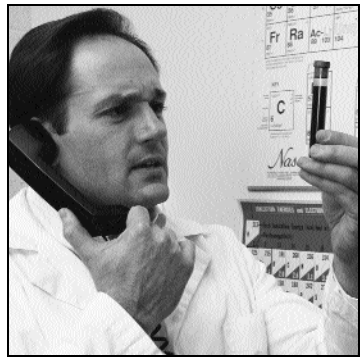
- **Educate yourself about medical privacy issues.**
  The bibliography at the end of this pamphlet provides a list of informative publications and Web sites.

For More Information

- To obtain a copy of your file from the MIB, Contact: MIB Inc., P.O. Box 105, Essex Station, Boston, MA 02112
  (617) 426-3660
  (http://www.mib.com)
- The American Civil Liberties Union (212) 549-2500
  (http://www.aclu.org)
- Electronic Privacy Information Center (202) 544 9240
  (http://www.epic.org)
- The Health Privacy Project
  (202) 687-0880
  (http://www.healthprivacy.org)
- The Privacy Rights Clearinghouse
  (619) 298-3396
  (http://www.privacyrights.org)

Providers and Plans: What You Can Do Right Now

WHILE MOST PROVIDERS PLEDGE TO KEEP PATIENT INFORMATION CONFIDENTIAL, THE DEMANDS FOR ACCESS TO THIS DATA ARE GROWING EVERYDAY—BOTH WITHIN THEIR ORGANIZATIONS AND OUTSIDE OF THEM.



One way that providers and health plans can protect patient privacy is by putting in place technological safeguards, such as systems that automatically limit access to specific users. Another way is to log and monitor who sees which data.

But such security measures cannot be developed in a vacuum. State and federal law, internal policies, and contractual agreements must establish how and when information may be shared. They must also be integrated into employee training.

Providers and plans can take several steps to prepare for new federal rules governing the confidentiality of health information.

- **Review existing policies.**
  Develop a detailed organizational confidentiality and security policy that is strong, clear, and enforceable. Do your contracts include prohibitions on secondary disclosure? Do you give

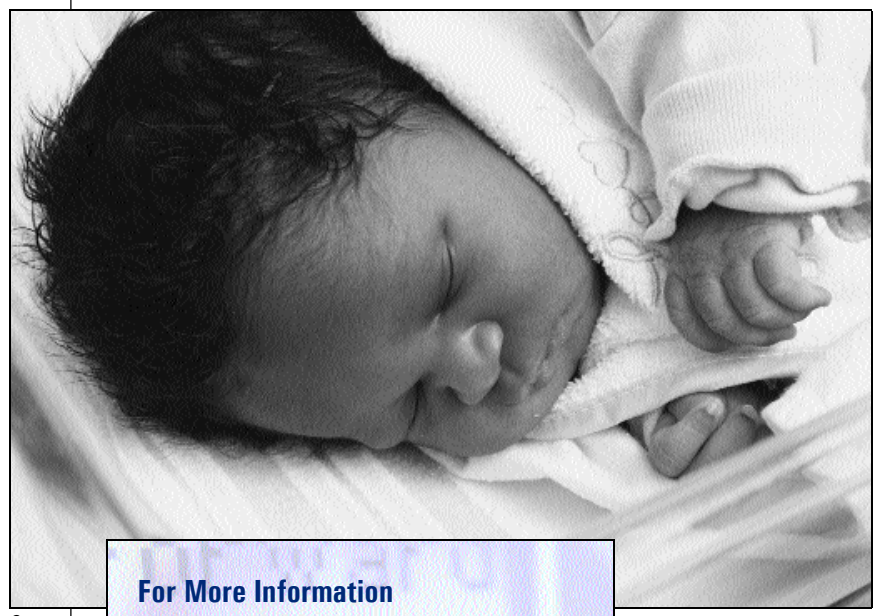
patients notice about the use of their health information? When do you require patient consent prior to disclosure?

- **Review and update existing safeguards.** Often the greatest threat to patient confidentiality comes from people who have authorized access to medical records. Who has access to what information, and under what circumstances? Does your organization have passwords and audit trails to help identify who is accessing patient information?

- **Determine when identifiable information is necessary.** As a general rule, removing personal identifiers, encrypting health information, or restricting access helps to minimize unauthorized use of personal health information. Before disclosing information to third parties, determine whether identifying information (such as name, address, Social Security Number, race/ethnicity) is necessary.

- **Emphasize confidentiality policies and procedures in employee trainings.** All employees working with identifiable health information should receive education on the confidentiality concerns of patients, and the company's policies and procedures for safeguarding information. Personnel policies should clearly outline consequences for failure to comply with company rules.

- **Give notice to patients and enrollees.** Give clear, up-front notice about your organization's privacy and confidentiality policies, the safeguards in place to keep information confidential, and the contact information for employees who can answer questions.



For More Information

California Health Information Association (209) 251-5038 **(http://www.californiahia.org)**

California Information Exchange (CALINX) (415) 281-8660 **(http://www.calinx.org)**

California Medical Association (415) 882-5131 **(http://www.cmanet.org)**

Association for Electronic Health Care Transactions (202) 244-6450 **(http://www.afehct.org)**

Computer-based Patient Record Institute (301) 657-5918 **(http://cpri.org)**

Work Group for Electronic Data Interchange (703) 391-2716 **(http://www.wedi.org)**

Joint Commission on Accreditation of Healthcare Organizations (630) 792-5000 **(http://www.jcaho.org)**

National Committee for Quality Assurance (202) 955-3500 **(http://www.ncqa.org)**

Appendix A

Appendix

Glossary of Users of Personal Health Information

Accreditation and Standard-Setting Organizations. Organizations that provide information on, and set standards for, health plan procedures, systems, and performance include the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) and the National Committee for Quality Assurance (NCQA).

Clearinghouses. The health care industry is characterized by a seemingly limitless array of one-on-one relationships between individual entities, each of which has its own information system. Clearinghouses are used to facilitate the flow of claims data across different operating systems by processing data, reformatting or verifying transactions, producing reports, and routing information. They may also forward claims to other clearinghouses. Some clearinghouses serve a specific purpose: the Medical Information Bureau, for instance, enables a membership of more than 600 insurance companies to share patient information for underwriting purposes.

Employers. Employers who choose to provide health care coverage for their employees may contract with a health insurer or "self insure," which means that they are at risk for the costs of care. In either case, there are no legal limits to employers' access to their employees' medical claims. Employers also typically use medical information for employee health programs, to determine physical fitness for certain jobs, and to monitor costs and utilization.

Government Agencies. County, state, and federal agencies use medical information for a variety of purposes, including oversight of the industry, delivery of care, and financing of care. They also collect information in order to track and safeguard public health.

Hospitals. Hospitals maintain and develop their own patient records, and may request patient records from providers (especially in the case of emergency care). Because hospitals serve a broad population, their records may be valuable for research projects. In the case of university-affiliated medical centers, the hospital is explicitly a research institution.

Insurers/Health Plans. Insurers include a wide variety of arrangements, from traditional indemnity plans (i.e., fee-for-service) to managed care organizations (which combine the role of insurer and provider). Insurers use patient information to determine individual's eligibility for insurance, set rates, study and justify expenses, pay for care, review the performance of physicians, and help develop new treatment guidelines. MCOs perform all these functions and provide direct patient care as well.

Some insurers carve out certain areas of coverage, such as mental health benefits, or functions, such as the transmittal of patient information to third parties (e.g., researchers).

Laboratories. While many providers and hospitals have in-house labs, specialized tests are often sent to outside laboratories. Labs may retain identifiable samples; they are also frequently required to notify public health authorities of results related to certain infectious diseases.

Pharmaceutical Companies. Pharmaceutical companies develop and market new drugs. This requires extensive population research, clinical trials, and monitoring after a drug is introduced in the market. A pharmaceutical company, for instance, may have an interest in measuring the effectiveness of its drug in comparison to a competitor's product. Increasingly, pharmaceutical companies are expanding their commercial reach by purchasing pharmaceutical benefit managers (see sidebar), laboratories, and pharmacies, and establishing independent relationships with providers.

Pharmaceutical Benefits Managers (PBMs). PBMs are private companies that contract with employers, MCOs, and other payers, to handle prescription benefits, create drug formularies, monitor drug compliance, and measure costs. They may be independent, or owned by a larger entity such as a managed care organization or a pharmaceutical company.

PBMs use patient information in a wide variety of ways: to process prescription claims, help to design benefits programs, develop drug formularies, flag adverse drug reactions, recommend alternative medications, evaluate prescribing patterns of providers, monitor patient drug compliance, and conduct outcomes research. They may also provide channels for providers to sell patient information (in the aggregate) to drug manufacturers, researchers, and others.

A researcher at PCS, a large benefits management company, notes that "Data can come from a variety of sources, such as pharmacy and/or medical claims, patient or provider reports, and patients' charts... At PCS, the outcomes research group has online access to 700 million pharmacy claims, which represent the past 25 months of prescriptions filled. The information on a prescription becomes available online within 48 hours after the pharmacist dispenses it."

—Hughes, Tom, "Translating Data into Useful Information: the Evolving Role of the PBM," *Drug Benefit Trends*, 1998

Pharmacies. Pharmacies not only fill prescriptions, but also provide a wide array of services including tracking compliance, flagging adverse drug reactions, monitoring outcomes, and recommending different medications. Pharmacies may be independent (single store or chain), based in a larger institution (such as a hospital), or serve in an integrated network (such as an HMO).

Appendix A

Practitioners. Practitioners encompass a varied group of medical professionals: physicians, dentists, psychiatrists, nurses, mental health care professionals, social workers, chiropractors, and others. Licensing requirements (and legal classification as a "practitioner") may be different in different states. Practitioners may be organized in a network, participate in a health plan, based in a larger institution, or engage in private practice. Their use of patient information beyond payment and treatment largely depends on the structures in which they operate.

Researchers. Researchers are an extremely diverse group: They may be privately or publicly funded, they may or may not be covered by state or federal regulations, and they may have extensive or little contact with individual people (clinical trials and epidemiology, respectively). The growing field of health services research often does not require any direct contact with patients; it merely involves the use of medical records, claims data, and other information.

Statewide Organizations. Some statewide organizations, such as hospital associations, gather patient information for a specific purpose. Often it is analyzed and returned to the source.

Others. Many other institutions use and collect medical information for a variety of reasons. These include credit bureaus, life insurers, and educational institutions.

Current Protections in California Law

The following summarizes the major statutes regarding the confidentiality of medical information in California. This is not intended to be an exhaustive list—there are additional laws that speak to specific circumstances and information including adoption records, use of medical information in court proceedings, and research.

State Constitution

Article 1, Section 1 of the State Constitution establishes that "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty; acquiring, possessing, and protecting property; and pursuing and obtaining safety, happiness, and privacy."

The Confidentiality of Medical Information Act (CMIA)

(Civil Code, Section 56 et seq.)

As a general rule, CMIA requires health care providers and employers to obtain written authorization from patients prior to disclosure of identifiable information. There are many exceptions to the authorization requirement. Authorization is not required for disclosures related to diagnosis, treatment, billing, emergency situations, licensing and accreditation, utilization review, and quality assurance activities. Finally, "upon specific inquiry, unless specific written request by the patient to the contrary, [health care providers] may release patient name, address, age, sex, general description of the reason for treatment, general nature of condition, or other information not defined as 'medical information.'" Minimal remedies are available for violation of the Act.

Insurance Information and Privacy Protection Act (IIPPA)

(Insurance Code, Section 791 et seq.)

The IIPPA applies to insurers—broadly defined—and requires that written authorization be obtained prior to disclosure of personal information. There is a long list of exceptions to the authorization requirement. Authorization is not required to verify coverage/benefits, to inform an individual of a medical problem, to detect/prevent criminal activity and fraud, or for marketing purposes as long as no medical record or personal information "re: an individual's character, personal habits, mode of living or general reputation is disclosed... An individual must have been given the opportunity to indicate s/he does not want personal information disclosed for marketing purposes and must not have given any indication that s/he does not want it disclosed." The law gives individuals the right to see and copy their own records, for a "reasonable fee." Civil penalties may apply for violation of the Act, but individual remedies are extremely limited.

Appendix B

Patient Access to Health Records Act
(Health and Safety Code, Section 123100 et seq.)

California's Patient Access to Health Records Act requires that health care providers allow individuals to see and copy their medical records within five days of a written request and for a "reasonable fee." However, mental health records may be withheld if the provider determines there is "substantial risk of significant adverse or detrimental consequences" to the patient.

Information Practices Act
(Civil Code, Section 1798 et seq.)

The Information Practices Act (IPA) limits the use and disclosure of personal information—including medical information—held by the state and local government. The law also provides people with notice of the purposes for which their information is collected and maintained, and states, as a general rule, that information may not be disclosed outside the original agency without the individual's "prior written voluntary consent." A lengthy list of exceptions to the consent requirement includes disclosures for law enforcement access, adoption proceedings, and scientific research. The law requires that information be maintained with "accuracy, relevance, timeliness, and completeness." The IPA is the companion state law to the federal Privacy Act of 1974.

Law Enforcement
(Penal Code, Section 1543 et seq.)

Medical records may be released without consent for fraud investigations, and to law enforcement after showing of "good cause," or after presenting a search warrant.

Penalties
(S.B. 1374, Chaptered September 14, 1998)

A recent law amends the California Penal Code to establish fines for the willfull misuse of personal health information. The law covers medical information, credit, goods, and services.

Special Protections

- **Drug-and Alcohol Abuse**
  Institutions that receive federal funding are subject to the federal Alcohol and Drug Abuse Act (42 U.S.C. Sec 290dd-2 (1988)). The law's regulations apply strict confidentiality rules to oral and written communications of patient records, including "the identity, diagnosis, prognosis, or treatment of any patient."

- **HIV/AIDS Information**
  (See Health and Safety Code, Section 120975 et seq; 121015 et seq.; Insurance Code, Section 799 et seq)

  California has enacted a number of HIV/AIDS specific confidentiality laws, covering testing, reporting, partner notification, and discovery. The results of an HIV/AIDS test may not be disclosed in a form which identifies an individual, without patient consent for each disclosure, except in very limited circumstances. For instance, a physician or local health officer may disclose HIV test results to the sex or needle-sharing partner of the patient without consent, but only after the patient refused or was unable to make the notification.

  Specifically, an individual's health care provider may not disclose to another provider or health plan without written authorization, unless to a provider for the direct purposes of diagnosis, care, or treatment of the individual.

- **Genetic Discrimination**
  (Insurance Code, Section 10140 et seq.)

  California law prohibits insurers from discriminating on the basis of a person's "genetic characteristics that may, under some circumstances be associated with disability in that person or that person's offspring." In most instances, the law bars insurers from seeking, and disclosing, a person's genetic information without that person's written authorization.

- **Mental Health**
  (California Welfare and Institutions Code, Section 5000 et seq.)

  There are specific restrictions on the release of mental health information. The Lanterman-Petris-Short Act generally applies to institutions, not private physicians. The Act provides greater protection to mental health records than provided for under the CMIA.

Appendix D

Requirements for Administration Simplification

The 1996 Health Insurance Portability and Accountability Act (HIPAA) includes a provision called "administrative simplification," which requires all health care providers, plans, and clearinghouses that use electronic health information to adopt uniform data standards for the electronic transmission and security of personal health data. The U.S. Department of Health and Human Services (HHS) is moving to finalize regulations.

Regulations are set to take effect 24 months after the final regulations are announced (small health plans will have 36 months to comply). Failure to comply with the administrative simplification regulations could result in a civil penalty.

Up-to-date information on administrative simplification regulations can be found at: **http://aspe.os.dhhs.gov/admnsimp.**

In enacting administrative simplification, Congress intended to streamline the processing of health care claims, reduce paperwork, lower costs, improve accuracy, safeguard the security of information, and facilitate the networking and coordination of health information and health care activities.

Currently pending as draft proposals issued during summer 1998, these standards will soon become mandatory for most health care entities, including providers and plans. All covered entities that store, maintain, or transmit health data electronically—such as to verify eligibility or process claims—must comply with these federal standards. Entities that lack the resources in-house to comply with the law must contract with clearinghouses to convert the data.

Thus far, HHS has released three sets of proposed regulations, all of which will apply to all providers, plans, and clearinghouses that transmit and store electronic health information.

- **Health care provider identification number:** Under the proposal, providers would apply for an eight-digit number that they would be required to use whenever they submitted claims electronically. They would keep the number regardless of where—or what—they practice.
- **Standard billing:** All health plans are required to use a single standard electronic format for billing. All health plans would be required to accept these standard electronic claims.
- **Standards for certain encounter data:** All health plans and providers are required to use standard encounter data for reporting diagnoses, referrals, authorizations and procedures.
- **Employer identification number:** All employers are required to use an identifying number based on the numbers already assigned by the IRS.
- **Security standards:** All health care organizations are required to develop a security plan and provide employee training for the security of electronic health information. The proposed regulations include an electronic digital signature standard, to verify the authenticity of the signer and of the transaction. Organizations must assess their risks, develop practices, policies and procedures to address the risk, establish sanctions for breaches, institute audit trails, access controls, physical security, software discipline, and system assessment.

Appendix D

Select Bibliography

Government Reports

Confidentiality of Individually-Identifiable Health Information, U.S. Department of Health and Human Services, Recommendations submitted to Congress, September 1997. (**http://aspe.os.dhhs.gov.admnsimp**)

Genetic Information and the Workplace, US Department of Labor report, January 20, 1998. (**http://www.dol.gov/dol/_sec/public/media/reports/genetics.htm**)

Health Privacy and Confidentiality Recommendations, National Committee on Vital and Health Statistics, June 25, 1997. (**http://aspe.os.dhhs.gov/ncvhs/privrecs.html**)

Privacy and Health Research: A Report to the U.S. Secretary for Planning and Evaluation, U.S. Department of Health and Human Services, Office of the Assistant Secretary for Planning and Evaluation, May 1997.
(**http://aspe.os.dhhs.gov/datacncl/PHR.htm**)

Protecting Privacy in Computerized Medical Information, U.S. Congress, Office of Technology Assessment, September 1993.
(**http://www.wws.princeton.edu/~ota/ns20/alpha_f.html**)

Quality First: Better Health Care for All Americans, The President's Advisory Commission on Consumer Protection and Quality in the Health Care Industry, 1998. *(See Appendix A: Consumer Bill of Rights and Responsibilities, pp. A57-A60 for "Confidentiality of Health Information.")* To order, call (800) 732-8200,
ISBN 0-16-049533-4.

Commissioned Reports

The Computer-Based Patient Record: An Essential Technology for Health Care, Institute of Medicine, National Academy Press, 1997.

For the Record: Protecting Electronic Health Information, National Research Council, National Academy Press, 1997.

Health Data in the Information Age, Institute of Medicine, Committee on Regional Health Data Networks, National Academy Press, 1994.

Full text of all these books can be found at **http://www.nap.edu/readingroom.**

Appendix D

Additional Resources

"Fact Sheet: How Private is My Medical Information?" Privacy Rights Clearinghouse, 1997. (**http://www.privacyrights.org**)

"Getting Your Medical Records," California Medical Association, 1996. (**http://www.cmanet.org**)

"Health Information Privacy" by Lawrence Gostin, *Cornell Law Review*, Vol. 80:451.

"HIV Surveillance and Name Reporting," American Civil Liberties Union, 1997. To order: (212) 549-2500. (**http://www.aclu.org/issues/aids**)

"Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization," Final Report Presented to: The U.S. Centers for Disease Control and Prevention; The Council of State and Territorial Epidemiologists; The Task Force for Child Survival and Development Carter Presidential Center, by Lawrence O. Gostin, et al, 1997. (**http://www.epic.org/privacy/medical/cdc_survey.html**)

Medical Records and the Law, by William Roach and the Aspen Health Law and Compliance Center, 1998.

"Nothing Sacred: The Politics of Privacy," Center for Public Integrity, 1998. (**http://www.publicintegrity.org**)

"Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality," by Janlori Goldman and Deirdre Mulligan, 1996. To order, contact the Foundation for Health Care Quality at (206) 682-2911.

"Protecting Privacy to Improve Public Health" by Janlori Goldman, *Health Affairs*, November/December 1998.

"Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment," Developed by the Joint Commission on Accreditation of Healthcare Organizations and the National Committee for Quality Assurance, November 1998. (**http://www.ncqa.org/confide/tablcont.htm**)

Dennis Johnson Design

To order additional copies of the
Confidentiality Primer
contact the California HealthCare Foundation
at (510) 587-3199 or visit our Web site at
http://www.chcf.org/orderpub.cfm

California HealthCare Foundation
476 Ninth Street
Oakland, California 94607
tel: (510) 238-1040
fax: (510) 238-1388
www.chcf.org

Consumers Union
West Coast Regional Office
1535 Mission Street
San Francisco, California 94103
tel: (415) 431-6747
fax: (415) 431-0906
www.consunion.org