HEALTH PRIVACY PROJECT

Institute for Health Care Research and Policy
Georgetown University

A Health Privacy Primer
for consumers

EXPOSED

With support from the Open Society Institute's Program on Medicine as a Profession

HEALTH PRIVACY PROJECT

The **Health Privacy Project** is a part of the Institute for Health Care Research and Policy at Georgetown University. The Health Privacy Project is dedicated to raising public awareness of the importance of ensuring health privacy in order to improve health care access and quality, both on an individual and a community level. The Project receives funding primarily from the Open Society Institute's Program on Medicine as a Profession, the Robert Wood Johnson Foundation, the Kellogg Foundation, the California HealthCare Foundation, and the Trellis Fund.

RECENT PROJECT PUBLICATIONS INCLUDE:

- "Best Principles for Health Privacy," a report of the Health Privacy Working Group, July 1999; funded by the Robert Wood Johnson Foundation.
- "The State of Health Privacy: An Uneven Terrain," a practical, comprehensive guide to state health privacy laws, July 1999; funded by the Robert Wood Johnson Foundation.
- "Promoting Health/Protecting Privacy," a guide to health privacy with an emphasis on California law and practice, January 1999; funded by the California HealthCare Foundation.

Available at www.healthprivacy.org/resources

CONSUMER COALITION FOR HEALTH PRIVACY

The mission of the **Consumer Coalition for Health Privacy** is to educate and empower healthcare consumers to have a prominent and informed voice on health privacy issues at the federal, state, and local levels. Members of the coalition are committed to the development and enactment of public policies and private standards that guarantee the confidentiality of personal health information and promote both access to high quality care and the continued viability of medical research. The coalition is an initiative of the Health Privacy Project and is funded solely by the Open Society Institute's Program on Medicine as a Profession.

EXPOSED: A Health Privacy Primer for Comsumers was made possible with support from the Open Society Institute's Program on Medicine as a Profession.

Authors: Janlori Goldman, *Director*
Zoe Hudson, *Senior Policy Analyst*
Health Privacy Project

Project Management: High Noon Communications

Design: Denson Design

❝ Whatever, in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, **as reckoning that all such should be kept secret.**❞

➢ **Hippocratic Oath,** circa 4th Century B.C.

❝ 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... When all is said and done, **will our health care records be used to heal us or reveal us?**❞

➢ **Donna Shalala,** U.S. Secretary of Health and Human Services

❝ **No one should have access to your medical information or mine without our knowledge and consent.** This is what consumers want and need.❞

➢ **Abbey Meyers,** National Organization for Rare Disorders

❝ Discrimination laws only help you after something bad has happened. **We want privacy laws to limit the flow of information** so that it prevents bad things from happening in the first place.❞

➢ **Jeffrey Crowley,** National Association of People with AIDS and Consortium for Citizens with Disabilities

A Health Privacy Primer
for consumers

EXPOSED

EXPOSED

PATIENTS' health care information is EXPOSED

Individuals share a great deal of sensitive, personal information with their doctors:

- physical conditions
- personal habits
- sexual practices
- mental state
- medications
- family history.

Full disclosure is, after all, **necessary for accurate diagnosis and treatment.** But what happens to the information people share with their doctors *after* they leave the examining room?

Patient information is shared for many reasons and with many people:

- doctors and hospitals
- pharmacies
- employers
- relatives
- schools
- researchers
- insurance companies
- pharmaceutical companies
- data clearinghouses
- public health officials
- the government
- and even the press and marketers.

Many of these disclosures are necessary to treat patients, process claims, measure outcomes, and fight disease. But all of this activity is now **taking place without clear privacy rules.** In fact, there are **no real limits on the use of patients' medical records.**

Americans are becoming aware that the broad waivers they sign as a condition of receiving health care and insurance leave them **vulnerable to unwanted exposure, judgments, stigma, discrimination,** and — in some cases — **loss of jobs, credit, housing, and family.**

Now, when people sign up for a health plan, complete a medical history, see a doctor, fill a prescription, or file a claim form, they wonder,

"Who else will see my medical record?"

Here's why:

There is no comprehensive federal law that protects the privacy of medical records. Unlike other personal information, there is very little legal protection for medical records. In effect, medical records are less protected than financial information, and even video rental lists. Fortunately, federal health privacy regulations may soon be finalized.

The demand for health information is on the rise. Managed care and efforts to reduce costs and improve quality also rely on access to patient information. As more information is collected and maintained in electronic format, it becomes easier to share data with others for a wide variety of purposes.

The result:

People are afraid that their personal health information can be used against them and they are taking drastic steps to protect their privacy. Health information can be used

— legally and illegally — to deny people insurance, in civil and legal disputes, in hiring and firing decisions, and in many other ways outside the health care setting. Rather than risk negative consequences, some people withhold information from their doctors, or avoid care altogether.

That's not right:

The price of health care should not be the loss of privacy.

Privacy is often portrayed as a barrier to achieving other health care goals. But the opposite is true. People have demonstrated that they need a **guarantee of privacy in order to participate fully in their own health care.**

In the absence of privacy, health care providers often receive incomplete, inaccurate information from their patients, thus compromising the quality of care. When this same data is then disclosed and used for payment, outcomes analysis, research, and public health reporting, it carries the same weaknesses, and is not reliable.

In essence, information that lacks integrity at the front end will not be reliable as it moves through the health care system. **Strong, enforceable privacy rules can benefit everyone** — privacy fosters access to care and, in turn, improves the quality of care for individuals and their communities.

"Every American has a right to know that his or her medical records are protected at all times from falling into the wrong hands."

President Bill Clinton

Consumers Support Appropriate Information Uses When Protections are in Place

It's not that collecting information, or sharing information is always a bad thing. In fact, **consumer groups advocate for mandatory reporting, health screening, disease registries, and other data collection in some cases.** Patient information can be used to:

- justify funding for certain programs or to certain populations
- understand health care needs, services, and costs
- develop new treatments and therapies.

Data collection efforts, however, must include privacy protections in order to assure the public that the information will not be used against them. To help protect patients' privacy, those who hold information should:

- collect, use and disclose only the minimum amount of information necessary
- remove name, social security number and other identifying information whenever possible
- guarantee that the information will only be used for the purpose for which it was originally collected
- inform patients up-front about how their information will be used
- give patients choices about who will see their information
- protect the information from falling into the wrong hands.

FEARS

PEOPLE ARE TAKING STEPS TO PROTECT THEIR PRIVACY often at a significant cost to their health

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. A poll conducted for the California HealthCare Foundation in January 1999 found that:

- **One in five** U.S. adults believes that a health care provider, insurance plan, government agency or employer has improperly disclosed personal medical information. Half of these people say it resulted in personal embarrassment or harm.

- **One in six** U.S. adults says they have done something out of the ordinary to keep personal medical information confidential. (See sidebar for examples.)

- **Two out of three** U.S. adults say they don't trust health plans and government programs, such as Medicare, to maintain confidentiality all or most of the time.

The 1999 poll mirrors earlier research on privacy. According to surveys by Louis Harris & Associates:

- 27% of the public believes they have been the **victims of an improper disclosure** of personal health information.
- 24% of **health care leaders polled knew of violations of patient confidentiality** and could describe the violations in detail.
- In order to protect their privacy, 11% of consumers said that they or an immediate family member **paid outof pocket for health care, rather than submit a claim.**
- 7% of consumers **chose not to seek care** because they didn't want to harm their "job prospects or other life opportunities."

Privacy-Protective Behaviors

In order to help maintain the confidentiality of sensitive medical information:

- Patients may see multiple providers to avoid a consolidated record; pay out of pocket for services to which they are entitled reimbursement; and asking a doctor not to write down the health problem or record a less serious or embarrassing condition withhold information; lie; or avoid care altogether.
- Doctors may skew diagnosis or treatment codes on claim forms, keep separate records, or share incomplete information with insurance companies and others.

Ultimately, these privacy-protective behaviors can hurt individual patients, and compromise the public health initiatives meant to serve them. **Patients have demonstrated that privacy is central to how, and whether, they seek health care.**

FEDERAL PROTECTIONS don't exist

Currently, there is **no comprehensive federal law protecting the privacy of medical records.** Congress has been trying to pass such a law for decades, but has been unable to come to consensus. As a compromise, the 1996 Health Insurance Portability and Accountability Act (HIPAA) imposed a deadline on Congress to pass a comprehensive health privacy law. Since Congress missed the August 1999 deadline, the Secretary of Health and Human Services is required to promulgate final regulations by February 2000.

The **Secretary's regulations will be the first federal health privacy rules,** but they will not be comprehensive — by law they may **only cover the electronic records held by *certain* entities.** Further, the regulations will **not be effective until at least February 2002.** Clearly, there is still an important role for Congress to play to fill the gaps.

STATE LAWS Provide Limited Protections

The limited privacy protections people currently do enjoy have been put in place by state legislatures. However, **very few states have comprehensive laws.** What does this mean for consumers?

- **The same health information may be afforded more or less protection depending on who is holding the information.** For the most part, states have different laws for different entities that possess health information. This makes some sense: a school, hospital, and insurance company all have different information needs. But this approach may leave people vulnerable as information moves between entities. A state, for example, may protect the information held by a hospital, but not protect the same information when it is held by an insurance company.
- **Certain types of health information may be treated differently.** Nearly every state has laws that specify privacy protections for specific medical information such as HIV/AIDS, genetic information, mental health, and communicable diseases. Many of these laws were passed to encourage people to seek testing and treatment without fear of exposure.

  In some cases, however, the privacy protections were enacted hand-in-hand with mandatory reporting requirements. A doctor, for example, may be legally obligated to report a positive test for HIV, a birth defect, or a patient with tuberculosis to public health officials.
- **State laws have not kept pace with the changing health care delivery system and new demands for health information.** State laws do not anticipate the growing market for health information. As information changes hands, it is increasingly unclear as to who has responsibility for maintaining the confidentiality of the information. Many state laws do not apply to new users of health information such as data clearinghouses, HMO's, benefit managers, and drug companies.

Even within a state, protections vary widely. To understand what kinds of protections exist, first determine:

- Who's holding the data?
- Where did the data come from?
- What is the medical condition at issue?
- Who wants access and for what purpose?

To learn more about your state's laws, see *The State of Health Privacy: An Uneven Terrain* available at http://www.healthprivacy.org/resources.

CONCERNS

SPECIAL CONCERNS for health care consumers

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. **Many consumers worry that employers might use health information against them in hiring, firing, and promotion decisions.**

Here's why:

- In a 1998 national survey by the Kaiser Family Foundation, 89% of medium and large employers report that they require health plans to guarantee the confidentiality of employees' medical records. However, **30% 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,** not just the portion required for the given activity. (February 26, 1998)
- A 1996 survey found that **35% of Fortune 500 companies look at people's medical records** before making hiring and promotion decisions. (Unpublished study, University of Illinois at Urbana-Champaign)

How is this legal?

Currently, some restrictions on employer use of employee medical information exist 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 disabilities, or for the resolution of Worker's Compensation claims.

While the ADA extends critical protections to the disabled, those protections are not absolute. Employers may be legally prohibited from *using* information in certain ways, but there are very few laws that restrict their *access* to the information. Ultimately, **privacy must be the first line of defense against discrimination** by employers using confidential medical information.

Genetic Information

Many people may shy away from genetic testing because they fear that too many have access to the information, and that it can be used against them.

- In a 1997 national survey, **63% of people** reported that they **would not take genetic tests for diseases if insurers or employers could access the tests**.
- **One in three 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.("Genetic Information and the Workplace," U.S. Department of Labor, January 20, 1998)

In order to encourage people to seek genetic testing and counseling, and participate in genetic research, a number of states have passed laws to provide greater confidentiality protections for, and to prohibit discrimination based on, genetic tests.

Research

Currently, **federal regulations regarding research 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). The IRB generally requires that researchers ask people to consent to the use of their information. The IRB, however, may also grant a waiver of this informed consent requirement.

Increasingly, research is privately funded and may not involve direct contact with patients. As a result, **more research is falling outside the scope of these federal regulations**. In a recent GAO report, investigators noted that "during a research presentation at a national meeting, notes on a patient suffering from extreme depression and suicidal impulses stemming from a history of childhood sexual abuse were distributed. The notes included the patient's identity, medical history, mental status and diagnosis, as well as extensive intimate details about the patient's experience." Because the study did not receive federal funding, there was no legal recourse for the research subjects. (GAO Report, "Medical Records Privacy," 1999)

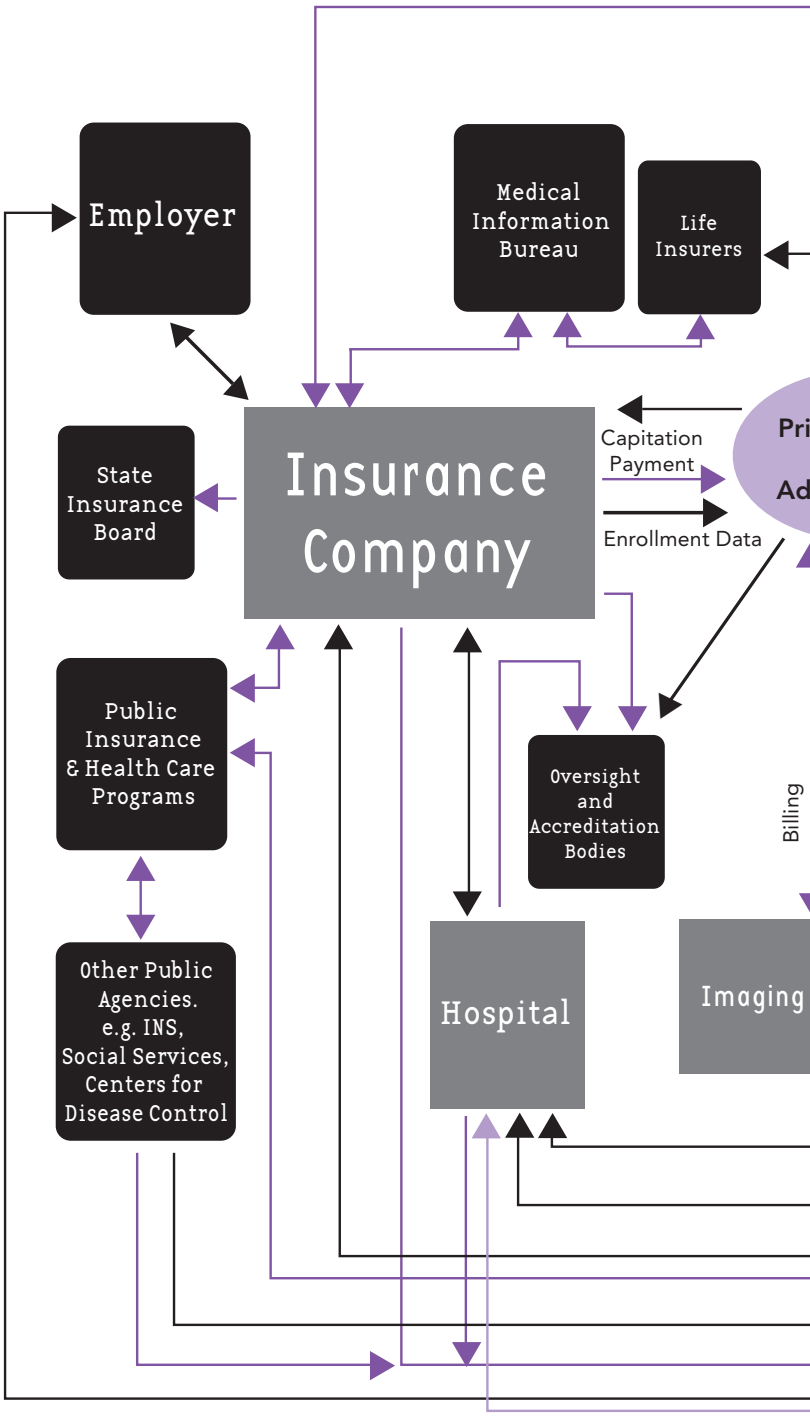
"Knowledge about how to prevent and cure breast cancer will only come if women participate in research. But without appropriate safeguards against misuse, public distrust will increase and few women will be willing to participate in research efforts… Only if women believe that their individual health information will be kept private so that it can't be used against them by insurers or employers or be made public will they have the confidence to participate in clinical research. I can't emphasize enough that we must focus our attention on building trust. It has to be something real, something believable, if women are to place their trust in the medical and research process."

Fran Visco, National Breast Cancer Coalition

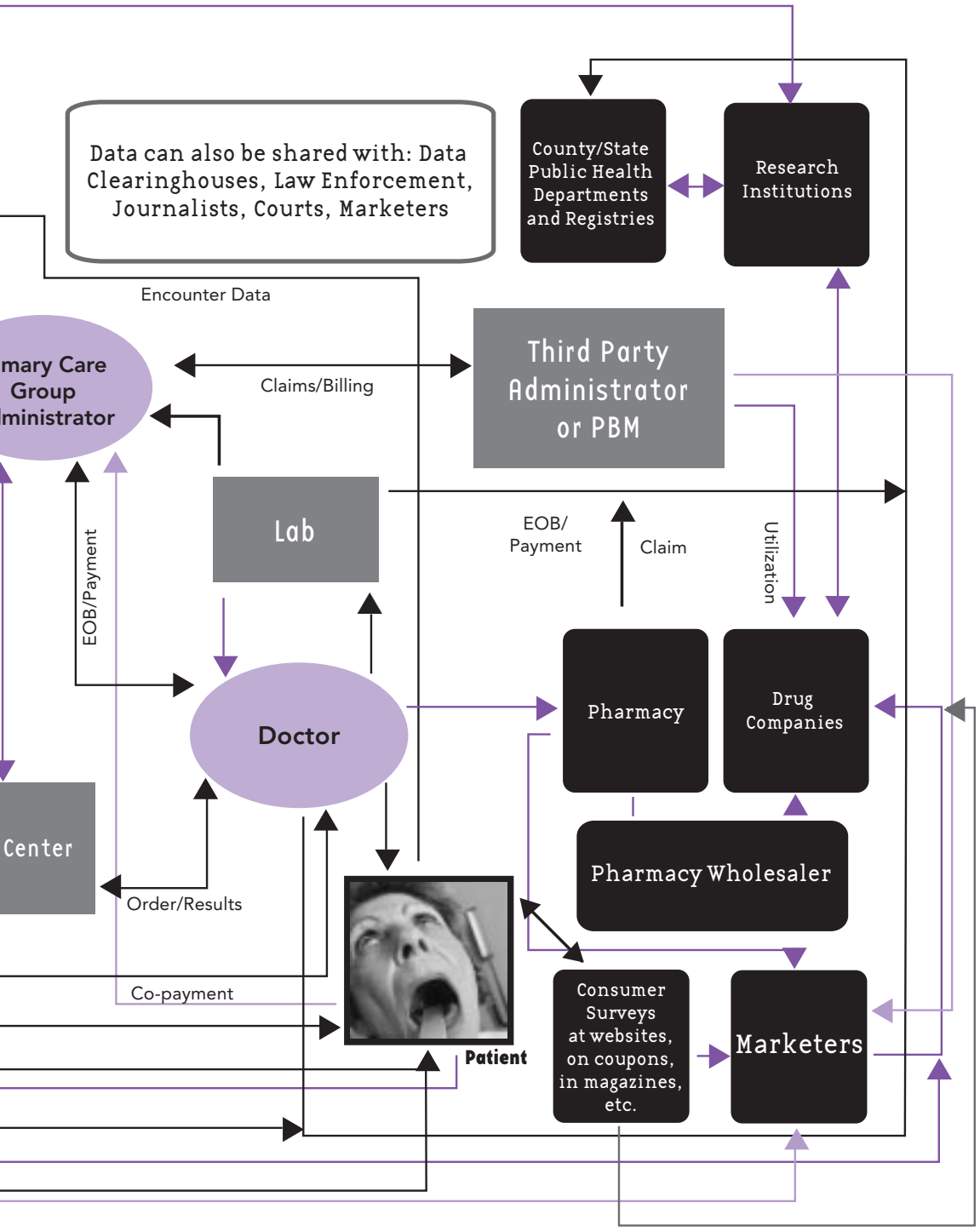
FLOW

Sample Data Flow

Based on a presentation developed by the California HealthCare Foundation



Please note that the explanations are meant to be illustrative. They are not comprehensive.


Data can also be shared with: Data Clearinghouses, Law Enforcement, Journalists, Courts, Marketers
County/State Public Health Departments and Registries
Research Institutions
Encounter Data
mary Care Group dministrator
Claims/Billing
Third Party Administrator or PBM
Lab
EOB/Payment
EOB/ Payment
Claim
Utilization
Pharmacy
Drug Companies
Doctor
Center
Order/Results
Pharmacy Wholesaler
Co-payment
Patient
Consumer Surveys at websites, on coupons, in magazines, etc.
Marketers

DOWNSTREAM

Information flows to DOWNSTREAM USERS

As with all personal information, **health information can be used for many purposes other than those for which it was gathered.** As more information is put in electronic format, it is becoming easier to harness patient data for activities unrelated to health care. Often these uses **take advantage of information patients offered in confidence.** While many activities are currently legal, many consumers consider them inappropriate. Here are some examples:

Drug Marketers

Two major chain pharmacies, CVS and Giant Food, made **patient prescription records available to a direct mail and pharmaceutical company as part of a marketing campaign.** The stated goal was to send letters to customers encouraging them to refill prescriptions and to consider alternative treatments—but their customers had not agreed to this use of their information. After a series of news reports and substantial public outrage, the companies abandoned the practice. (*Washington Post*, February 15, 1998)

Public Assistance Programs

In New York City, the Giuliani Administration announced plans to **use medical billing records to identify welfare recipients and applicants who sought drug or alcohol treatment.** Those individuals could in turn be forced into mandatory treatment programs as a condition of receiving public assistance. (*The New York Times*, September 25, 1999)

Immigration and Naturalization Services

An anti-fraud program came under fire when the California Department of Health and 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.)

Law Enforcement Agencies

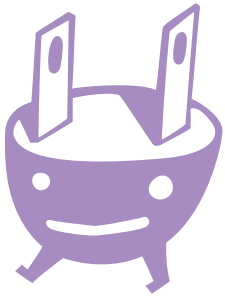
In Virginia, **police seized 200 medical records from a drug treatment center** after a car was stolen from a nearby parking garage. While the police believed that the records could help them identify the culprit, they later returned the records, conceding that the search was an unnecessary intrusion of patient privacy. ("Fairfax Police Concede Seizure Was Wrong," *The Washington Post*, September 1, 1998)

Judicial Proceedings

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,** she 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 would result in news coverage — and therefore further disclosure — of his illness. ("Longs Drugs Settles HIV Suit," *San Diego Union Tribune*, September 10, 1998.)

Private Databases

Medical information is shared between companies. One company, All Claims, **collects medical information from numerous insurance companies and makes it available** "in the investigation of potentially fraudulent activities." They advertise that their database includes "millions of records" and can be used to identify pre-existing conditions, duplicate coverage and over-utilization. (See www.allclaims.com) Another company, the Medical Information Bureau provides a similar service to more than 600 member insurance companies. (See www.mib.com)



Grabbing Information On-line

Consumers, in increasing numbers, are turning to the internet to get medical information, communicate with people with similar conditions, and even to manage chronic conditions. But the web has a darker side for consumers looking to communicate and receive information anonymously.

Many websites ask for detailed information about consumers, sometimes as a condition of visiting the site. But they may not tell you:

- what they do with the information,
- who they share the information with,
- and for what purposes.

Consumers may *unintentionally* reveal information about themselves – such as a medical condition, medications, and high-risk behaviors — simply by *visiting* a website. New technology can enable website hosts to gather, analyze, cross-reference and share information on consumers. For this reason, **the internet is increasingly being used by drug manufacturers, health care organizations and others as a way of studying patient populations and promoting products.**

"Web site promotion makes especially good sense for pharmaceutical companies... the Net is better than other means for collecting information about patients — so much better, in fact, that it raises privacy issues. The document trail that visitors follow at a Web site can indicate their preferences or provide clues about their underlying medical conditions... Many patients divulge personal information without asking who will use it or how."

"Why Drug Companies are Banking on Web Sites to Reach Customers," Medicine & Health Marketplace, December 28, 1998

Health Information Bought and Sold

- Employees in emergency rooms in large city hospitals have been reported selling accident victims' names to personal injury lawyers.
- Physicians and pharmacists can receive software and equipment from pharmaceutical companies in exchange for allowing the companies to regularly download patient data.
- Pharmacies can receive payments from marketers and others for lists of patients and prescriptions.
- Financial institutions may use health information as a factor in making financial service decisions such as mortgage qualifications.
- Pharmaceutical companies may use patient information for direct marketing of their products.
- Information brokers and marketers sell health information to interested parties. Some sell lists of patients and their illnesses to pharmaceutical companies. One company advertises in pharmaceutical industry journals that it has nearly a million names of people with bladder control problems. Other brokers provide health claims information to members, including self-insured employers with the stated purpose of controlling fraudulent claims.

VOICE

Consumer Coalition for Health Privacy: A VOICE FOR HEALTH CARE CONSUMERS

Heightened public concerns about the privacy of personal health information and the growing debate surrounding appropriate public and private policies **galvanized health care consumers and advocates** to organize the **Consumer Coalition for Health Privacy** in the fall of 1998.

The **Coalition is dedicated to empowering healthcare consumers** to have a prominent and informed voice on health privacy issues at the federal, state, and local levels and to informing consumers and their advocates about the steps individuals can take to protect the privacy of their health information.

Members of the Coalition are committed to the development and enactment of **public policies and private standards that guarantee the confidentiality of personal health information, and promote both access to high quality care and the continued viability of medical research**. In order to accomplish these goals, the Coalition established and endorsed the following health privacy principles.

CONSUMER HEALTH PRIVACY PRINCIPLES

Right to Privacy
An individual's right to privacy with respect to individually identifiable health information, including genetic information, should be established statutorily. Individuals should retain the ultimate right to decide to whom, and under what circumstances, their individually identifiable health information will be disclosed. Confidentiality protections should extend not only to medical records, but also to all other individually identifiable health information, including genetic information, clinical research records, and mental health therapy notes. Additional protections may be necessary for highly sensitive information.

Identifiable Information
Use and disclosure of individually identifiable health information should be limited. Protections should be in place to ensure that anonymized data is used whenever possible.

Access
An individual should have the right to access his or her own health information and the right to supplement such information. Individuals should have the right to access and supplement their own medical records so that they can make informed health care decisions and can correct erroneous information in their records.

Notice
Individuals should be notified about how their medical records are used and when their individually identifiable health information is disclosed to third parties. Individuals should be given written, easy-to-understand notice of how their individually identifiable health information will be used and by whom. With such notice, people can make informed, meaningful choices about uses and disclosures of their health information.

Informed Consent

The use or disclosure of individually identifiable health information absent an individual's informed consent should be prohibited. Health care providers, health plans, insurance companies, employers and others in possession of individually identifiable health information should be prohibited from using or disclosing such information unless the use or disclosure is authorized by the individual. Use or disclosures without informed consent should be permitted only under exceptional circumstances — for example, if a person's life is endangered, if there is a threat to the public health, or if there is a compelling law enforcement need. Disclosure of individually identifiable health information for marketing or commercial purposes should never be permitted without informed consent.

Any time information is used or disclosed it should be limited to the minimum amount necessary for the use or disclosure.

Public Health and Research

While protecting individual privacy rights, legislation should not impede important public health efforts or clinical, medical and quality of care research.

Safeguards

The development of security safeguards for the use, disclosure and storage of personal health information should be required. Appropriate safeguards should be in place to protect individually identifiable health information from unauthorized use or disclosure.

Penalties

Strong and enforceable remedies for violations of privacy protections should be established. Remedies should include a private right of action, as well as civil penalties and criminal sanctions where appropriate. Individuals that come forward to report violations of this law should be protected from retaliation.

Preemption

Federal legislation should provide a floor for the protection of individual privacy rights, not a ceiling. Like all other federal civil rights and privacy laws, federal privacy legislation for health information should set the minimum acceptable standard. Federal legislation should not preempt any other federal or state law or regulation that is more protective of an individual's right to privacy of or access to individually identifiable health information.

See the attached information or visit www.healthprivacy/coalition for a current list of endorsing organizations, or to join the Coalition.

"The voices of consumers are finally being heard. Protecting privacy is a core patient right that affects all aspects of health care, from diagnosis and treatment, to research and public health. When privacy is protected, everyone stands to benefit."

Janlori Goldman, Health Privacy Project

CHECKLISTS

HEALTH PRIVACY CHECKLIST for Consumers

- **Learn about the privacy protections in your state**
  Visit http://www.healthprivacy.org/resources —The State of Health Privacy: An Uneven Terrain. Look up your state and see what rights and protections you have. Federal regulations are due to be finalized in February 2000, but health care organizations are not required to comply until the year 2002. Under the proposed regulation, stronger state laws will continue to stand.

- **Request a copy of your medical record**
  Currently, 28 states give individuals a legal right to inspect and copy their medical records. Even if your state does not provide such a legal right, you may be able to inspect and copy your record upon request.

- **Request a copy of your file from the Medical Information Bureau**
  The Medical Information Bureau (MIB) is a membership association 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. MIB, Inc., P.O. Box 105, Essex Station, Boston, MA 02112, Tel. 617-426-3660, Fax 781-461-2453, www.mib.com.

- **Talk about confidentiality concerns with your doctor**
  Your health care provider 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 providers keep treatment notes separate from the general medical chart to help ensure that the most sensitive information remains confidential. Your provider 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 or public health purposes.

- **Read authorization forms before signing and 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 purposes. 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 objections to disclosures that you consider inappropriate**
  Registering objections may not result in immediate change, but sharing your concerns will help to educate your providers, plans, and others seeking health information. These entities should be aware that the lack of privacy affects how you seek and receive your health care. If you feel that your rights have been violated, contact your state insurance commissioner's office to see what remedies are available.

- **Be cautious when providing personal medical information for "surveys," health screenings, and health-related Web sites**
  Ask how the information will be used and who will have access to it. Read any posted privacy policies, and know your choices.

- **Educate yourself about medical privacy issues**
  The resources page provides a list of informative publications and Web sites.

HEALTH PRIVACY CHECKLIST for Organizations

- **Join the Consumer Coalition for Health Privacy**
  Become an active member of the only Coalition dedicated solely to improving health privacy protections for health care consumers. More information is available at www.healthprivacy.org/coalition.

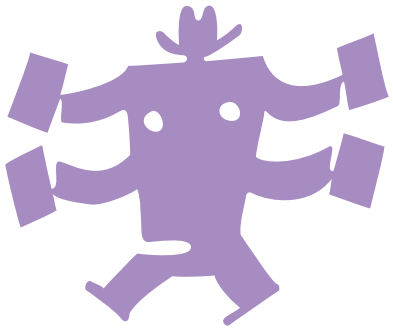
- **Protect the information you hold**
  Information about your members, including a simple list of members, could by its very nature reveal personal health information. Develop strong policies to protect that information and provide all members with information about those protections.

- **Secure your website**
  Develop and post strong privacy policies on your website. This is especially important if you have patient chat rooms or offer health information at your website. Also require any health care companies, including pharmaceutical companies, with whom you work to develop and post strong privacy policies as a condition of collaborating with you. (For guidance, see the Consumer Coalition principles.)

- **Poll your membership**
  Find out what their health privacy concerns are and how they impact their health care decisions. Ask members if their health privacy has ever been breached and, if so, how they were impacted. Ask what protections they would like.

- **Learn state laws**
  Review the state health privacy fact sheet for the state or states where you operate. Fact sheets for all 50 states are available at www.healthprivacy.org/resources

- **Advocate for stronger laws and policies**
  Determine how the laws of your state or states can be improved and advocate for change. Join with other advocates at the national level to urge Congress to pass a comprehensive federal health
  privacy law.



RESOURCES

Health Privacy Project Resources

Best Principles for Health Privacy, A Report of the Health Privacy Working Group, July 1999.

The State of Health Privacy: An Uneven Terrain/A Comprehensive Survey of State Health Privacy Statutes, by Joy Pritts, Janlori Goldman, Zoe Hudson, Aimee Berenson, and Elizabeth Hadley, July 1999.

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

Promoting Health/Protecting Privacy: A Primer, by Janlori Goldman and Zoe Hudson, 1999. Prepared for the California HealthCare Foundation and Consumers Union.

Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality, by Janlori Goldman and Deirdre Mulligan, 1996. Prepared for the Foundation for Health Care Quality.

All available at www.healthprivacy.org. To receive e-mail notices about recent health privacy news and developments, subscribe to the Health Privacy Project's news service at www.healthprivacy.org.

Reports

Draft health privacy regulations are available at http://aspe.hhs.gov/admnsimp/index.htm. The final regulations will be available at the same site.

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)

For the Record: Protecting Electronic Health Information, National Research Council, National Academy Press, 1997. (http://www.nap.edu/readingroom/)

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 Data in the Information Age, Institute of Medicine, Committee on Regional Health Data Networks, National Academy Press, 1994. (http://www.nap.edu/readingroom/)

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

Medicare: HCFA Needs to Better Protect Beneficiaries' Confidential Health Information, United States General Accounting Office, July 20, 1999. (GAO/T-HEHS-99-172)

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)

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

HEALTH PRIVACY PROJECT

Institute for Health Care Research and Policy
Georgetown University

2233 Wisconsin Ave., NW
Suite 525
Washington, DC 20007
202.687.0880 phone
202.687.3110 fax
www.healthprivacy.org