

information is used by secondary and tertiary users. For example, a pharmacy benefit manager could receive information to determine whether an insurance plan or HMO should cover a prescription, but then use the information to market other products to the same patient. Similarly, many of us obtain health insurance coverage through our employer and, in some instances, the employer itself acts as the insurer. In these cases, the employer will obtain identifiable health information about its employees as part of the legitimate health insurance functions such as claims processing, quality improvement, and fraud detection activities. At the same time, there is no comprehensive protection prohibiting the employer from using that information to make decisions about promotions or job retention.

Public concerns reflect these developments. A 1993 Lou Harris poll found that 75 percent of those surveyed worry that medical information from a computerized national health information system will be used for many non-health reasons, and 38 percent are very concerned. This poll, taken during the health reform efforts of 1993, showed that 85 percent of respondents believed that protecting the confidentiality of medical records is "absolutely essential" or "very essential" in health care reform. An ACLU Poll in 1994 also found that 75 percent of those surveyed are concerned a "great deal" or a "fair amount" about insurance companies putting medical information about them into a computer information bank to which others have access. Harris Equifax, Health Information Privacy Study 2.33 (1993) <http://www.epic.org/privacy/medical/poll.html>. Another survey found that 35 percent of Fortune 500 companies look at people's medical records before making hiring and promotion decisions. Starr, Paul, "Health and the Right to Privacy," *American Journal of Law and Medicine*, 1999, Vol 25, pp. 193-201.

Concerns about the lack of attention to information privacy in the health care industry are not merely theoretical. In the absence of a national legal framework of health privacy protections, consumers are increasingly vulnerable to the exposure of their personal health information. Disclosure of individually identifiable information can occur deliberately or accidentally and can occur within an organization or be the result of an external breach of security. Examples of recent privacy breaches include:

- A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet

(The Ann Arbor News, February 10, 1999).

- A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store (Kiplingers, February 2000).

- An employee of the Tampa, Florida, health department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS (USA Today, October 10, 1996).

- The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut (The Hartford Courant, May 14, 1999).

- A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 of the hospital's employees (The Boston Globe, August 1, 2000).

- A Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy data base included names, addresses, social security numbers, and a list of all the medicines the customers had purchased. (The New York Times, April 4, 1997 and April 12, 1997).

- A speculator bid \$4000 for the patient records of a family practice in South Carolina. Among the businessman's uses of the purchased records was selling them back to the former patients. (New York Times, August 14, 1991).

- In 1993, the Boston Globe reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women. (ACLU Legislative Update, April 1998).

- A few weeks after an Orlando woman had her doctor perform some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol. (Orlando Sentinel, November 30, 1997).

No matter how or why a disclosure of personal information is made, the harm to the individual is the same. In the face of industry evolution, the potential benefits of our changing health care system, and the real risks and occurrences of harm, protection of privacy must be built into the routine operations of our health care system.

Privacy Is Necessary To Secure Effective, High Quality Health Care

While privacy is one of the key values on which our society is built, it is more than an end in itself. It is also necessary for the effective delivery of health care, both to individuals and to populations. The market failures caused by the lack

of effective privacy protections for health information are discussed below (see section V.C below). Here, we discuss how privacy is a necessary foundation for delivery of high quality health care. In short, the entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers.

The need for privacy of health information, in particular, has long been recognized as critical to the delivery of needed medical care. More than anything else, the relationship between a patient and a clinician is based on trust. The clinician must trust the patient to give full and truthful information about their health, symptoms, and medical history. The patient must trust the clinician to use that information to improve his or her health and to respect the need to keep such information private. In order to receive accurate and reliable diagnosis and treatment, patients must provide health care professionals with accurate, detailed information about their personal health, behavior, and other aspects of their lives. The provision of health information assists in the diagnosis of an illness or condition, in the development of a treatment plan, and in the evaluation of the effectiveness of that treatment. In the absence of full and accurate information, there is a serious risk that the treatment plan will be inappropriate to the patient's situation.

Patients also benefit from the disclosure of such information to the health plans that pay for and can help them gain access to needed care. Health plans and health care clearinghouses rely on the provision of such information to accurately and promptly process claims for payment and for other administrative functions that directly affect a patient's ability to receive needed care, the quality of that care, and the efficiency with which it is delivered.

Accurate medical records assist communities in identifying troubling public health trends and in evaluating the effectiveness of various public health efforts. Accurate information helps public and private payers make correct payments for care received and lower costs by identifying fraud. Accurate information provides scientists with data they need to conduct research. We cannot improve the quality of health care without information about which treatments work, and which do not.

Individuals cannot be expected to share the most intimate details of their lives unless they have confidence that such information will not be used or

shared inappropriately. Privacy violations reduce consumers' trust in the health care system and institutions that serve them. Such a loss of faith can impede the quality of the health care they receive, and can harm the financial health of health care institutions.

Patients who are worried about the possible misuse of their information often take steps to protect their privacy. Recent studies show that a person who does not believe his privacy will be protected is much less likely to participate fully in the diagnosis and treatment of his medical condition. A national survey conducted in January 1999 found that one in five Americans believe their health information is being used inappropriately. See California HealthCare Foundation, "National Survey: Confidentiality of Medical Records" (January, 1999) (<http://www.chcf.org>). More troubling is the fact that one in six Americans reported that they have taken some sort of evasive action to avoid the inappropriate use of their information by providing inaccurate information to a health care provider, changing physicians, or avoiding care altogether. Similarly, in its comments on our proposed rule, the Association of American Physicians and Surgeons reported 78 percent of its members reported withholding information from a patient's record due to privacy concerns and another 87 percent reported having had a patient request to withhold information from their records. For an example of this phenomenon in a particular demographic group, see Drs. Bearman, Ford, and Moody, "Foregone Health Care among Adolescents," *JAMA*, vol. 282, no. 23 (1999); Cheng, T.L., et al., "Confidentiality in Health Care: A Survey of Knowledge, Perceptions, and Attitudes among High School Students," *JAMA*, vol. 269, no. 11 (1993), at 1404-1407.

The absence of strong national standards for medical privacy has widespread consequences. Health care professionals who lose the trust of their patients cannot deliver high-quality care. In 1999, a coalition of organizations representing various stakeholders including health plans, physicians, nurses, employers, disability and mental health advocates, accreditation organizations as well as experts in public health, medical ethics, information systems, and health policy adopted a set of "best principles" for health care privacy that are consistent with the standards we lay out here. (See the Health Privacy Working Group, "Best Principles for Health Privacy"

(July, 1999) (Best Principles Study). The Best Principles Study states that—

To protect their privacy and avoid embarrassment, stigma, and discrimination, some people withhold information from their health care providers, provide inaccurate information, doctor-hop to avoid a consolidated medical record, pay out-of-pocket for care that is covered by insurance, and—in some cases—avoid care altogether.

Best Principles Study, at 9. In their comments on our proposed rule, numerous organizations representing health plans, health providers, employers, and others acknowledged the value of a set of national privacy standards to the efficient operation of their practices and businesses.

Breaches of Health Privacy Harm More Than Our Health Status

A breach of a person's health privacy can have significant implications well beyond the physical health of that person, including the loss of a job, alienation of family and friends, the loss of health insurance, and public humiliation. For example:

- A banker who also sat on a county health board gained access to patients' records and identified several people with cancer and called in their mortgages. See the *National Law Journal*, May 30, 1994.
- A physician was diagnosed with AIDS at the hospital in which he practiced medicine. His surgical privileges were suspended. See *Estate of Behringer v. Medical Center at Princeton*, 249 N.J. Super. 597.
- A candidate for Congress nearly saw her campaign derailed when newspapers published the fact that she had sought psychiatric treatment after a suicide attempt. See *New York Times*, October 10, 1992, Section 1, page 25.
- A 30-year FBI veteran was put on

administrative leave when, without his permission, his pharmacy released information about his treatment for depression. (*Los Angeles Times*, September 1, 1998) *Consumer Reports* found that 40 percent of insurers disclose personal health information to lenders, employers, or marketers without customer permission. "Who's reading your Medical Records," *Consumer Reports*, October 1994, at 628, paraphrasing Sweeny, Latanya, "Weaving Technology and Policy Together to Maintain Confidentiality," *The Journal Of Law Medicine and Ethics* (Summer & Fall 1997) Vol. 25, Numbers 2,3.

The answer to these concerns is not for consumers to withdraw from society and the health care system, but for society to establish a clear national legal framework for privacy. By spelling out

what is and what is not an allowable use of a person's identifiable health information, such standards can help to restore and preserve trust in the health care system and the individuals and institutions that comprise that system. As medical historian Paul Starr wrote: "Patients have a strong interest in preserving the privacy of their personal health information but they also have an interest in medical research and other efforts by health care organizations to improve the medical care they receive. As members of the wider community, they have an interest in public health measures that require the collection of personal data." (P. Starr, "Health and the Right to Privacy," *American Journal of Law & Medicine*, 25, nos. 2&3 (1999) 193-201). The task of society and its government is to create a balance in which the individual's needs and rights are balanced against the needs and rights of society as a whole.

National standards for medical privacy must recognize the sometimes competing goals of improving individual and public health, advancing scientific knowledge, enforcing the laws of the land, and processing and paying claims for health care services. This need for balance has been recognized by many of the experts in this field. Cavoukian and Tapscott described it this way: "An individual's right to privacy may conflict with the collective rights of the public * * *. We do not suggest that privacy is an absolute right that reigns supreme over all other rights. It does not. However, the case for privacy will depend on a number of factors that can influence the balance—the level of harm to the individual involved versus the needs of the public."

The Federal Response

There have been numerous federal initiatives aimed at protecting the privacy of especially sensitive personal information over the past several years—and several decades. While the rules below are likely the largest single federal initiative to protect privacy, they are by no means alone in the field. Rather, the rules arrive in the context of recent legislative activity to grapple with advances in technology, in addition to an already established body of law granting federal protections for personal privacy.

In 1965, the House of Representatives created a Special Subcommittee on Invasion of Privacy. In 1973, this Department's predecessor agency, the Department of Health, Education and Welfare issued *The Code of Fair Information Practice Principles* establishing an important baseline for