ROBERT GELLMAN
Privacy and Information Policy Consultant **202-543-7923**
419 Fifth Street SE **bob@bobgellman.com**
Washington, DC 20003

The Privacy of Health Information and the Challenge for Data Protection

Prepared for

Observatory "Giordano Dell'Amore" on the
Relations Between Law and Economics

Eighth International Congress

The Information Society, the Protection of the Right to Privacy

Stresa, Italy
May 16-17, 1997

I. Introduction

The modern data protection movement applies fair information practices to personal information maintained by third party record keepers.[1] The notion of fair information practices dates from the mid-1970s, when study commissions in the United States and Britain simultaneously developed similar principles.[2] In the early 1980s, the Council of Europe[3] and the Organization for Economic Cooperation and Development[4] adopted international data protection guidelines based on fair information practices. European data protection laws and the recent European Union directive on data protection[5] all derive from fair information practices.

Fundamental principles of fair information practices apply universally to all personal record systems, but implementation of the principles can vary from system to system. Different records require different applications of the principles. For example, all personal records should be protected against theft and misuse. However, more security is appropriate for the protection of health records than for magazine subscription records. The difference is justified because health records are more sensitive and are used and disclosed more expansively than magazine records. In each case, the broad policies are similar, but the local application varies.

This brings us to the central question of this paper. Can basic principles of fair information practices be applied in an effective and realistic manner to health records? Health records are perhaps the most sensitive single collection of personal data about most individuals. At the same time, health records may also be the most widely used and circulated of all personal records.

Record keepers often have an incentive to limit disclosures of other major categories of personal records. For example, neither banks nor employers normally have a reason to share the details of their personal records with others. For competitive reasons, banks and employers seek to retain customers and employees. Maintaining a degree of confidentiality helps to accomplish that objective. Yet health records tend to flow freely between major institutions. For the most

---

[1] See generally Colin Bennett, Regulating Privacy (1992).

[2] See Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (1973) (U.S. Dept. of Health Education & Welfare); Report of the Committee on Privacy (1972) (Great Britain) ("Younger Committee").

[3] *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 20 I.L.M. 317 (1981).

[4] *Council Recommendations Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 20 I.L.M. 422 (1981), O.E.C.D. Doc. C (80) 58 (Final) (Oct. 1, 1980).

[5] Council Directive 95/46/EC on the *Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 1995 O.J. (L 281) 31.

part, each institution may exploit data for its own purposes without direct conflict with other institutions.[6]

Can basic data protection principles work to control the well-established flow of health information between institutions? The traditional American model for regulating disclosure is informed consent. Because of the number of health institutions, the volume of data sharing, and the limited ability of patients to make disclosure decisions, reliance on notice to and consent of the record subject may not be realistic.

Before proceeding, a cultural and political comment is appropriate. This article was written by an American and reflects the structure and practices of the American health care system. Because of the unique and convoluted American method of providing and paying for health care, some judgments offered here may not be relevant elsewhere. The American system has a dizzying and rapidly changing array of providers, payors, and governments. Other entities link, oversee, or otherwise provide services to major health care institutions. When a single entity provides or pays for health care -- as is often the case in other countries -- the difficulty of controlling health information use and disclosure is lessened.

Still, many basic functions that complicate the flow of information within the American health system surely have counterparts elsewhere. Every country has an interest in providing high quality, low-cost health care to all of its residents. Resources to meet these objectives are scarce everywhere. The conflict between the substantive goals of the health care system on the one hand and the privacy interests of individuals on the other has many universal elements. At the very least, the American health care system may be viewed as a worst-case challenge for principles of data protection.

One additional characteristic of the American privacy landscape is relevant. No comprehensive rules regulate the collection, maintenance, use, and disclosure of health records.[7] American legal protections for health records are often described as a *patchwork quilt* of laws, rules, and policies, with major gaps and limitations.[8] No federal law protects the privacy of all

---

[6] Competitive reasons for not sharing health records are beginning to emerge. In the past, records were more likely to be shared in the interests of science or administration. However, records may provide a competitive advantage to the increasing numbers of profit-making organizations involved in health care activities. If a provider can use records to identify a less expensive or more effective treatment, it may no longer have a reason to share the results with a competitor. For the same reason, records that could be analyzed to derive similar conclusions might not be made available to others. It remains to be seen how strongly competition will affect sharing of patient records.

[7] Robert Gellman, *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules*, 41 Villanova Law Review 129-172, 136-140 (1996).

[8] Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information* 12-13 (1993) ("The present system of protection for health care information offers a patchwork of codes; State laws of varying scope; and Federal laws applicable to only limited kinds of information, or information maintained specifically by the Federal Government."); Institute of Medicine, *Health Data in the Information Age: Use, Disclosure, and Privacy* 15 (Donaldson & Lohr eds., 1994) ("Existing ethical, legal, and other approaches to protecting confidentiality and privacy of personal health data offer some confidentiality safeguards, but major gaps and limitations remain."); House Committee on Government Operations, *Health Security Act*, H.R. Rep. No. 103-601 Part 5 at 83 (1994) (report to

health records, and state laws are spotty, incomplete, and limited in scope.[9] Unlike many European countries, the United States does not have an omnibus privacy law establishing general rules and policies for personal data. The lack of nationwide rules has greatly facilitated the expanded transfer of health information in recent years.

II. Background

A. The Routine Sharing of Health Information

In the United States, a third party usually pays for health care services.[10] Thus, the insurer who receives and pays bills is an integral participant in the physician-patient relationship. Because health insurance is a common benefit offered by employers, the insurer hired by the employer is most likely to pay the bills. This basic structure begins to expose the complexity of health data flows in the United States. Information created by providers is routinely disclosed to insurers and may also flow from employers to insurers and visa versa. Because federal and state governments provide or pay for much health care, governments obtain large amounts of health data as well.

Multiple intermediaries transfer data from providers to private and governmental insurers. A bill may move from a physician's office to a billing service, to one or more clearinghouses, and through one or more value added networks before reaching the insurer. Bills for prescription drugs may have a parallel but separate path, moving from pharmacist to pharmacy benefit manager to insurer. Basic payment functions involve many separate entities.[11]

Another reason for the routine sharing of information is the pressure to contain costs. Every institution that pays health bills faces constantly rising costs. The growing for-profit health care sector also seeks increasing profitability.[12] In response to these pressures, providers,

---

accompany H.R. 3600) ("Current legal protections for health information vary from State to State and are inadequate to meet the need for fair information practices standards.").

[9] See Paul Schwartz, *The Protection of Privacy in Health Care Reform*, 49 Vanderbilt Law Review 310 (1995).

[10] In 1950, individuals paid almost two-thirds of personal health care expenditures with their own personal funds. Private health insurance or government paid the rest. By 1993, only 20.1% was paid out-of-pocket. U.S. Department of Health and Human Services, Health United States 1994 229 (1995). In 1993, 17.3% of the population under the age of 65 was not covered by private health insurance or by Medicaid. Id. at 240.

[11] The traditional lines between provider, payor, and employer are blurring. Health maintenance organizations combine treatment and payment activities in a single entity. Self-insured employers combine the payor and employer in a single entity. The rapid organizational changes in the health care system that have characterized the last decade are likely to continue in the future.

[12] The use of patient information to support the marketing and sales of medical products and services (e.g., medications) has already become a factor in the restructuring of the health care industry. In one example, a pharmaceutical manufacturer (Merck) purchased a mail-order pharmacy (Medco). The purchase price was based in part on the value of the information in the databases of the pharmacy.

insurers, governments, and employers pursue cost containment and utilization review activities. These functions may be carried out directly or through third parties. The last decade sparked tremendous growth of cost containment strategies, including activities intended to assure that the quality of care meets accepted standards.[13] Examples are peer review, quality assurance, accreditation, and licensing.

Other information-intensive activities are auditing, fraud control, and law enforcement functions. The amount of fraud, waste, and abuse in the United States has been estimated to be ten percent of all health care spending.[14] The dollar losses -- measured in billions of dollars -- are huge. Federal, state, and private entities work jointly and separately to combat the losses. Criminal investigations for fraudulent health care billing are routine.[15]

The use of health data for clinical purposes creates other layers of data transfer. Treatment information routinely passes between physicians, hospitals, laboratories, and pharmacies. Each entity maintains a separate record keeping system and uses contractors for computer, communications, legal, accounting, and other information-based services.

Finally, state and federal public health agencies routinely collect patient data. The tracking of communicable diseases is a principal purpose, but these agencies carry out other activities including treatment. Somewhat related are health research activities, which may be conducted by physicians, hospitals, public health authorities, academics, or private companies. Other data transfers are the result of the reporting of hospital discharge data to state agencies and of other health data to state, federal, private, and international disease registries.[16]

---

[13] A newly released report on electronic health information from the U.S. National Research Council included this finding: "Information technology is becoming increasingly important in improving the quality and lowering the costs of health care; attempts to protect patient privacy must therefore center on finding ways to protect sensitive electronic health information in a computerized environment rather than on opposing the use of information technology in health care organizations." For the Record: Protecting Electronic Health Information 6-1 (Prepublication Copy, 1997) <http://www.nap.edu/readingroom/books/ftr/>.

[14] The General Accounting Office, the federal government's audit agency, regularly reports on aspects of health care fraud, waste, and abuse. The titles of recent reports are instructive: *Health Insurance: Vulnerable Payers Lose Billions to Fraud and Abuse*, GAO/HRD-92-69 (1992); *Medicare: Adapting Private Sector Techniques Could Curb Losses to Fraud and Abuse*, GAO-T-HEHS-95-211 (1995); *Medicare: Antifraud Technology Offers Significant Opportunity to Reduce Health Care Fraud*, GAO/AIMD-95-77 (1995); *Medicare Spending: Modern Management Strategies Needed to Curb Billions in Unnecessary Payments*, GAO/HEHS-95-210 (1995); *Fraud and Abuse: Medicare Continues to Be Vulnerable to Exploitation by Unscrupulous Providers*, GAO-T-HEHS-96-7 (1995); *Medicare: Millions Can Be Saved by Screening Claims for Overused Services*, GAO/HEHS-96-49 (1996); *Health Care Fraud: Information-Sharing Proposals to Improve Enforcement Efforts*, GAO/GGD-96-101 (1996).

[15] Recent federal legislation illustrates congressional willingness to allow access to health records for criminal law enforcement purposes related to health care fraud. The Attorney General was given the authority to subpoena any health record. See the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, §247 (adding new §3486 to title 18, United States Code). The legislation also place some limitations on the use of subpoenaed records in actions directed against the subject of the records.

[16] Traditional distinctions between research, management, oversight, and even some law enforcement activities are eroding. Institutions with different functions and methods may share the same interest in using patient records to find cost-effective treatments and cures for disease.

While American health care institutions do not exist in other countries in the same form, the functions they perform are commonplace: treatment, payment, management, cost containment, oversight, law enforcement, public health, and research.[17] Whether these diverse activities are conducted by separate institutions or entirely within a single institution, the widespread reliance on patient data is a common element.[18] The need for rules regulating use and disclosure of data is another common element.

B. Policy Standards

In the United States, the traditional principle for regulating the disclosure of health records is *informed consent*.[19] Patient records are only disclosed when the subject has been informed of and has consented to the disclosure. At a health record confidentiality hearing held in 1993 by a U.S. House of Representatives subcommittee, witnesses representing major health care institutions publicly identified informed consent as a bedrock principle governing disclosure of records.[20] As we will see, however, the policy of informed consent is more of a fiction than an accurate description of current practice. Nevertheless, the tradition, rhetoric, and emotion surrounding informed consent for disclosure are strong. Many patient and privacy advocates as well as many physicians and other health professionals are unaware of the extent to which patient records are disclosed without notice to or consent of patients.

In theory, at least, informed consent imposes stricter limits on the disclosure of health records than would result from basic application of fair information practices. The two fair information practices principles from the 1981 privacy guidelines of the OECD most relevant here are the purpose specification principle and the use limitation principle.

Purpose Specification Principle

---

[17] This list is by no means complete. Other institutions, public and private, rely on health data for other activities. Examples include vital statistics reporting, life insurance underwriting, judicial use, and press reporting.

[18] Not all activities always require identifiable patient data. In many cases, functions can be performed effectively with anonymized data. When a need exists to link records over time or location, identifiers can sometimes be replaced with codes that will support linking without directly revealing identifiers. These techniques minimize data protection concerns. However, for each function, some circumstances will require identifiers. It appears unlikely that all threshold data protection issues can be evaded with anonymizing techniques. This is an area that requires greater study and research.

[19] Informed consent is a standard feature of model health privacy codes prepared by health institutions. Several examples are reprinted in Office of Technology Assessment, Protecting Privacy in Computerized Medical Information at Appendix B (1993).

[20] *Health Reform, Health Records, Computers and Confidentiality*, Hearing before the Information, Justice, Transportation, and Agriculture Subcommittee of the House Committee on Government Operations, 103d Cong. (1993). Informed consent is also the model for regulating the provision of care to patients. The discussion in this paper about informed consent is applicable *only* to disclosure of records and not to treatment of patients.

> The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent uses limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
>
> **Use Limitation Principle**
>
> Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with [the purpose specification principle] except: a) with the consent of the data subject; or b) by the authority of law.

These fair information practices principles allow disclosures for purposes that are not incompatible with the purpose specified at the time of data collection. Changes in the specification of purpose are permitted. Other uses require subject consent or legal authority. Consent is not required if a disclosure is consistent with the specified purpose.

III. Analysis

A. Shortcomings of Informed Consent

The informed consent model for disclosure of health records is not an accurate description of current American practices. Of the major types of disclosures identified above (treatment, payment, management, cost containment, oversight, law enforcement, public health, and research), informed consent is routine only for treatment and payment disclosures. For other disclosures, control mechanisms or legal authority for disclosure are spotty. For example, state laws mandate many disclosures to public health authorities. Also, most disclosures for health research require advance approval of research protocols by institutional review boards.[21] State or federal laws may mandate or regulate disclosures for fraud control or for other specific purposes.

For most disclosures, however, no laws or regulations apply. No general statutory prohibition against or regulation of health record disclosures exists. As a result, each record keeping institution may have its own policies and practices for disclosures for management, cost containment, oversight, and even law enforcement activities. Ethical rules may provide some guidance for health professionals, but medical ethics do not address many modern disclosure circumstances. In any event, medical ethics do not apply to insurance companies, claims processors, and other non-professional record keepers.[22]

---

[21] This requirement derives from federal rules on the protection of human subjects, 45 C.F.R. Part 46 (1994). It applies to research conducted, supported, or regulated by federal agencies. Some private research activities are beyond the scope of the federal rules.

[22] See generally Robert Gellman, *Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy*, 62 North Carolina Law Review 255-294, 266-80 (1984).

The result is that despite glowing public endorsements of the policy of informed consent for disclosure, health record keepers do not and cannot comply with the rigors of the process. This is, of course, no surprise to the record keepers themselves. In private conversations, all acknowledge that informed consent is more of a theoretical ideal than a reality.

From the patient's perspective, informed consent is not informed. Patients are not normally told about broader uses of health records. The long chain of users of health records as they move from provider to insurer and back again is not identified. Nor are patients told about the even longer list of institutions permitted or required to access records without patient consent. Neither health care providers nor insurers must disclose information practices or policies to patients at the time of treatment or at any other time. It is fair to conclude, therefore, that little or nothing in the informed consent process meets any reasonable standard for informing patients about disclosure policies and practices.

For most patients, informed consent is not consensual either. A choice between signing a claim form and paying a large medical bill is not a real choice for most people. People have been trained over the years to sign insurance forms when they have encounters with the medical system. Signing an insurance form is typically a pre-condition for seeing a health professional. Without question or complaint, patients sign consent forms permitting disclosure of "any and all" information to their insurance companies.[23] Most do not read or attempt to understand the forms. Those in pain or mentally or physically impaired probably do not care what they sign.

A patient who has the interest and capacity to evaluate the consequence of a consent form still has no real opportunity to make changes or add conditions. The receptionist in a physician's office is hardly the right person to conduct negotiations about disclosure policies. Even educated patients, health professionals, and lawyers may not have the knowledge or capacity to understand and draft disclosure restrictions. Sometimes, the authority in a consent form is superfluous because the patient has already agreed to disclosure as a condition of obtaining an insurance policy.[24] If so, changes made to a consent form might have no legal effect.

Even if a patient makes changes on the consent form, it is not clear that the changes will have practical effect. This issue arose at recent hearings on health privacy held by the National Committee on Vital and Health Statistics, an advisory committee to the U.S. Department of Health and Human Services.[25] Insurance claims are now routinely submitted electronically through a claims processing network. The actual form signed by the patient does not physically

---

[23] During my last medical encounter, I was required to sign three different, very general disclosure release forms. The last authorized "the release of pertinent medical information to insurance carriers." No explanation was provided. The form did not have an expiration date, restrict use or redisclosure by the insurer, or even limit disclosure to a known insurer. If the insurance carrier I had identified declined the claim, the physician could disclose information to an unlimited number of other carriers in the search for someone to pay the bill.

[24] Even automobile insurance policies that provide coverage for injuries may contain clauses permitting complete disclosure of health records to the insurer.

[25] Transcripts from the hearings are available at <http://aspe.os.dhhs.gov/ncvhs/index.htm>.

move through the network. As a result, downstream recipients are unaware of any restrictions imposed by the patient. Processors and insurers assume that the originator of the claim obtained the standard disclosure consent.

The paradox of informed consent is that giving the patient more of a say in the disclosure of health records for payment results in the patient having less actual control. Because third party payment is the rule today rather than the exception, the signing of a consent form is not an event that triggers concern or suspicion. Written by insurance companies and health care providers, consent forms allow broad disclosure without any conditions or restrictions. Health care providers -- who may share their patients' concern about confidentiality -- nevertheless want to be sure that they can make disclosures necessary for payment. The effect of the informed consent model is to protect the interests of all parties except the patient.

Informed consent can be affirmatively destructive to patient rights as well. Even if legislative protections for patient records existed, a patient might waive the protections and authorize other uses by signing a routine consent form. For example, assume that legislation restricts non-consensual secondary uses by insurance companies. If an insurance company's consent form waives this restriction, then the intended statutory protections will be overridden. Of course, legislation can limit the ability of patients waive rights granted under a health privacy bill. But it may not be possible to foresee and close all loopholes.

B. Shortcomings of Fair Information Practices

Fair information practices rely on purpose specification and notice as a tool for regulating use and disclosure of identifiable information. For simple records where contact with the record subject is recurring (e.g., magazine subscriptions), this principle may work well. However, specifying purposes is a challenging task for multifarious health records stored in many locations, maintained by multiple record keepers, and kept for long periods. Some health record keepers have no routine contact with the record subject.

In the United States, a specification-of-purpose requirement would result in a lengthy list of uses and users.[26] An artfully worded notice drafted by the record keeper's lawyer would allow maximum flexibility to make profitable use of information virtually without any substantive

[26] The purpose specification principle permits uses for purposes that are "not incompatible" with the specified purposes. The Privacy Act of 1974 has similar language. 5 U.S.C. §552a (1994). Federal agencies are permitted to establish by regulation "routine uses" (disclosures) of information from a personal system of records. A "routine use" is defined as a use that is compatible with the purpose for which a record was collected. The standard is stated as a positive requirement ("compatible with") as opposed to the negatively defined standard ("not incompatible with") used in fair information practices. Although the Privacy Act is slightly more restrictive, it has nevertheless failed as a substantive limitation on disclosure. Agencies interpret the routine use provision to justify virtually any disclosure that they care to make. See Paul Schwartz & Joel Reidenberg, Data Protection Law §5-2(a) (1996). Based on this experience, it is not clear that any general compatibility standard will be effective, at least not in the absence of an aggressive oversight authority.

restrictions.[27] The presence of a data protection authority may prevent a record keeper from drafting an unrestricted purpose statement, but no such authority exists in United States.[28]

The challenge becomes more complex because of the large number of institutions that can make a justifiable claim for access. The many uses of identifiable health information for regulating the health care system developed in response to identified problems and constraints. Most users are well-intentioned and perform a socially useful purpose.

The conflict between an individual's interest in confidentiality and the societal interest in maintaining an efficient and effective health care system may be sharp at times. A good example comes from demands by health researchers for access to patient records. In at least some instances, access to identifiable records may be necessary to allow the linking of records from disparate locations and times.[29] A society may select from a variety of rules and procedures for regulating researcher access. Options include a complete ban on access, requiring individual patient consent, requiring approval by a neutral referee, unrestricted access by qualified researchers, and sanctions for misuse of records obtained for research purposes.

If a purpose specification statement regulates access to health records by researchers, then each of the many health record keepers may craft terms to satisfy its own view of the utility of health research. The result might be a diverse array of inconsistent, overlapping, or even conflicting policies. This is not an effective way for a nation to establish a privacy policy for health records. This approach will only add to the uncertainty of patients, who may not be aware if their physician, hospital, pharmacy, or insurer makes records available to researchers or on what terms.

Another set of issues surrounds the lack of patient consent for disclosures covered by a purpose specification statement. As described above, seeking and obtaining patient consent may not always be easy or effective. Nevertheless, some patients will have reasonable objections to some disclosures normally seen as routine or non-controversial. For example, psychiatrists report that some patients who have health insurance pay for care with personal funds. Their goal is to avoid disclosure of the treatment to an insurer or employer. Another example comes from drug abuse clinics, where patients may be undergoing treatment for activities that are criminal. The routine disclosure of treatment information may be directly harmful to the patients and to their ability to seek treatment.[30]

---

[27] This happens already in the United States. Supermarkets operate so-called *frequent shopper* programs that collect detailed information on the weekly purchases of each registered customer. The explanation on the program's registration form typically says that the information will only be used "for marketing purposes". This vague phrase permits virtually any use of the collected information.

[28] Robert Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 Software Law Journal 199-238 (1993).

[29] This can be especially important in the United States, where no centralized health records are maintained and where the movement of individuals throughout the country is commonplace.

[30] Federal laws provide special confidentiality rules for records of federally funded alcohol and drug abuse clinics. 38 U.S.C. §7332; (1994) 42 U.S.C. §290dd-2 (1994).

Standards that allow for disclosures of health information without either patient consent or the opportunity for patient objection may create unfairness and even harm. Fair information practice policies governing disclosure do not offer the flexibility that may be appropriate for health records.

VI. A Different Approach

This brief analysis suggests weaknesses with health records disclosure rules based on consent and with disclosure rules based on notice. Four factors make the challenge of controlling disclosures especially difficult. First, the United States has an enormously complex and diverse system for the maintenance and transfer of health records characterized by a multitude of record keepers performing a variety of functions. Second, health records contain perhaps the most sensitive collection of personal information about most individuals. Third, because of the growing need to regulate the delivery of and payment for health care, the use of health records for socially beneficial purposes continues to increase. Fourth, during the last decade, new health care institutions have emerged that require health records to perform their functions. More major structural, organizational, and technological changes are likely in the future.

The challenge for data protection is to devise a set of rules and procedures that will provide a reasonable degree of protection for privacy, accommodate essential users of information, and allow for practical and efficient operation. One novel way to balance these different interests has been proposed by U.S. Representative Gary Condit (D-CA).[31] His legislation combines the familiar elements of notice and consent with a twist.

The legislation proposes that disclosures for treatment and payment be *nonconsensual* and permitted under specified terms and conditions. The statutory rules limit how information obtained for treatment and payment may be used by recipients. The restrictions imposed in the legislation would not be subject to waiver by patients.

Patients with specific concerns about payment or treatment disclosures would still be allowed to arrange for more limited disclosure practices. For example, if a patient did not want an insurance company to pay for a particular treatment, then the patient could agree with the physician on an alternate form of payment. This agreement would be binding on the physician, and disclosure of the record to an insurer would be improper and sanctionable.

The goal of the Condit bill is to make the signing of consent forms an unusual event. Rather than ask everyone to sign a consent form when only a small percentage would object, the

---

[31] The Condit legislation is titled *Fair Health Information Practices Act*. It originated as H.R. 4077 (103d Congress). See House Committee on Government Operations, Health Security Act, H.R. Rep. No 103-601 Part 5 at 71-72 (1994). In subsequent Congresses, the legislation was reintroduced as H.R. 435 (104th Congress) and H.R. 52 (105th Congress).

legislation would eliminate routine consent forms and require those with special concerns to come forward on their own. In exchange, the statute would grant stronger protections for patients than are routinely available today.

If patients learn that the granting of consent is an unusual event, they will be more wary when asked for consent. The current consent system offers patients no cues that agreeing to a disclosure is something that requires careful review. Whether most patients could effectively protect their own interests in their health information is an open question. Informed consent for payment as currently practiced offer patients little hope of fair treatment for their health data. Legislation can provide patients better protection than they can negotiate on their own through one-sided informed consent agreements.

The Condit bill also contains provisions regulating non-consensual disclosures for research, public health, oversight, and law enforcement. Each of these authorized disclosures has an associated set of procedures and limitation on use and redisclosure. The goal is to balance patient confidentiality interests with other important societal goals. The bill accomplishes this in part by allowing other defined uses under strictly controlled conditions. Another protection comes from a prohibition on the use of a health record against the record subject in unrelated civil or criminal actions. The legislation also implements other basic fair information practices such as a right of access and a right to seek correction. Record keepers of all types must offer notices of information practices to inform patient of their rights and of data handling policies.

V. Conclusion

What is unusual about the Condit proposal is that it proposes to abandon the opt-in[32] model of informed consent in favor of an opt-out approach for basic treatment and payment disclosures. When offered a choice about further disclosure of information, most record subjects are likely to accept default disclosure policies.[33] This means normally that opt-in is associated with greater control by record subjects and fewer disclosures. Opt-out rules usually result in less control and more disclosures.

In the peculiar context of health information, however, the exercise of affirmative choice by the record subject does not work as expected. Patients will sign any disclosure form offered by a physician. Unlike other opt-in situations, patients universally agree to any disclosure

---

[32] Opt-in requires the affirmative consent of the record subject as a precondition to secondary use of personal information. Opt-out means that information can be reused unless the record subject has objected. A third alternative that may work best in an online environment is direct consumer choice. Consumers can be required to select between two or more alternatives as a condition of accessing a computer service so that default options are no longer needed. See Robert Gellman, *In Cyberspace, Having a Choice Favors Marketers*, DM News 12 (Jan. 22, 1996); Center for Democracy and Technology, Testimony before the Federal Trade Commission Workshop on Consumer Privacy on the Global Information Infrastructure (June 4-5, 1996) <http://www.cdt.org/publications/FTC_June96_test.html>.

[33] This is why marketers argue strenuously for opt-out and against opt-in. If affirmative consent for disclosure is required, the availability of information for marketing will be severely undermined.

presented to them. The effect of the informed consent/opt-in approach is to undermine patient privacy interests. Because of the need to provide for third-party payment, this seems unlikely to change.

The basic rules and procedures of fair information practices contain many approaches designed to accomplish the broad goals of protecting the privacy interest of individuals. As stated earlier, a strength of data protection is that the implementation of general principles can vary from system to system. In any given context, different combinations of the basic elements may be needed to achieve the desired results. Principles cannot be automatically applied to situations without an analysis of the circumstances and the effects.

A more general conclusion -- offered here tentatively -- is that record subject consent should not automatically be assumed to provide a high degree of privacy protection. Whether consent works in any specific circumstance may be a matter of fact and not just a matter of policy. It may be appropriate to examine how the procedure actually works in the marketplace to learn if consumers in a particular context are alert to the choice and are able to make judgments effectively. One obvious challenge will be distinguishing between instances where consumers do not object to wider use of their information and instances where they are unable to make a real choice. For health information, patient concern about disclosure has been clearly shown,[34] but the current informed consent control mechanism does not operate to give patients the information or the protection that they seek.

By combining familiar data protection techniques in new ways, it should be possible to fulfill the spirit of fair information practices and provide consumers with more effective and more meaningful protection for vital interests.

[34] See generally Louis Harris & Associates, Health Information Privacy Survey 1993 (1993) (85% of the American public believes that maintaining the confidentiality of health records is absolutely essential or very important in national health care reform).