

Privacy, Information Technology, and Health Care

*One of the most controversial issues in recent years
is how technology threatens the privacy of patient information.
Today, several technologies and methods exist to better
protect that personal data.*

We are well into the digital information age. Digital communications and information resources affect almost every aspect of our lives—business, finance, education, government, and entertainment. Clinical medicine is highly information intensive, but it is one of the few areas of our society where computer access to information has had only limited success in selected areas such as billing and scheduling, laboratory result reporting, and diagnostic instrument systems (such as radiology and cardiology). The move to widely accepted electronic patient records (EPRs) is accelerating, however, and is inevitable because of many pressures. Among those pressures are the desire to improve health care through timely access to information and decision-support aids; the need for simultaneous

access to records by doctors, nurses, and administrators in modern, integrated provider and referral systems; meeting the needs of highly mobile patients; the push toward improved cost effectiveness based on analyses of outcomes and utilization information; the need for better support of clinical research; and the growing use of telemedicine and telecare [5].

We are, of course, motivated by the great benefits to patient care and medicine that can derive from this effort. But almost daily we hear about network computer break-ins—often close to home—arousing vivid fears [4]. By putting our personal medical records online, might we be increasing the risk of exposing highly private and sensitive information to outsiders?

In this article we take a systems view of privacy and information security in health care. We will put the nature of the most urgent threats to patient information privacy in perspective, the new threats that almost certainly will arise because of the technologies of digital information,



the kinds of countermeasures that can be effective, the places where technology is and is not of use, the risk/cost trade-off decisions that must be made for real-world systems, the overarching policy issues that must be addressed, and impediments to the resolution of these issues.

Online Health Care Information

Once largely a fee-for-service cottage industry, health care has seen the steady growth of Health Maintenance Organizations (HMOs) and Integrated Delivery Systems (IDSs), and the transformation of reimbursement from an invoiced service basis to a capitation basis under which providers receive a prenegotiated fee for each patient under their care, independent of actual services rendered. Growing fierce competition in the health care industry is resulting in regional IDSs that provide one-stop shopping for ambulatory clinic care, urgent care, and inpatient hospital care. Deloitte and Touche indicates that 24% of U.S. hospitals now belong to an IDS and 56% of hospitals are pursuing EPRs. Outpatient clinics are also aggressive in pursuing EPRs, driven by their roles in regional IDSs and the pressures of streamlined, modern patient care.

These developments bode well for improved health care. Providers will have access to the most current information and decision-support aids for diagnosis and treatment no matter where the point of care. Researchers and public health officials will have access to better information for their studies of disease epidemiology and treatment efficacy. And health care enterprise managers will have better information on which to base business decisions for care standards and optimization of clinical care pathways.

Our medical records contain a great deal of mundane information about us, such as height and weight readings, blood pressures, and notes about bouts with the flu, cuts, or broken bones. These records also may contain some of the most sensitive information about who and what we are—about topics such as fertility and abortions, emotional problems and psychiatric care, sexual behaviors, sexually transmitted diseases, HIV status, substance abuse, physical abuse, genetic predispositions to diseases, and so on. Access to this information must be controlled because disclosure can harm us. It may cause social embarrassment or prejudice, or affect our insurability, or limit our ability to

get and hold a job. Of course, such damage can (and does) occur no matter whether our medical records are in paper or electronic form. We have only to glance at grocery store tabloids or election year news stories to see the allure and marketability of “interesting” health information about well known people (See [11], for example).

We have a strong (but often implicit) expectation that such information will be used only in the context of providing effective care, and otherwise, will be kept secret. This expectation is based on a number of principles, beginning with the Hippocratic Oath of more than 2,000 years ago,¹ and reinforced by the Code of Ethics of the American Medical Association² and by the federal Privacy Act of 1974.³

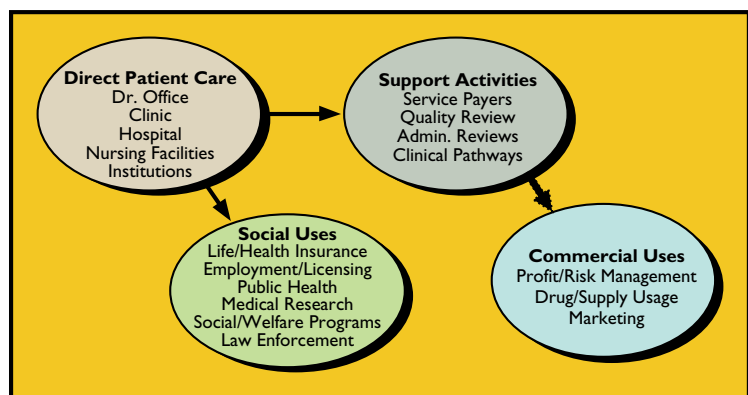


Figure 1. Flow of health care information in the U.S. system (after [12]).

Without broad confidence in medical privacy, we know there are consequences. Patients may avoid needed health care and physicians may not enter all information into patient records (or may even keep double sets of records).

Paradoxically, our medical records contain information about us that is of the utmost sensitivity, yet this information is only useful to us when it is shared with the medical providers and system under which we get our care. Indeed, our physicians need and expect access to our complete medical records in order to help diagnose diseases correctly, to avoid duplicative risky or expensive tests, and to design effective treatment plans that take into account many complicating factors. The desirable sharing goes beyond our per-

¹“What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself...”

²“A physician shall respect the rights of patients, colleagues, and of other health professionals, and shall safeguard patient confidences within the constraints of the law. . . .”

³ The 1974 Privacy Act specifies restrictions on federal agencies maintaining records on individuals including a right to know that identifiable information is being kept and why, and a right to review and amend/correct data.

sonal care and includes our relationships to society as a whole through support of medical research, public health management, and law enforcement. Thus, we must distinguish among three concepts involved in protecting health care information:

- *Privacy*: The right and desire of a person to control the disclosure of personal health information.
- *Confidentiality*: The controlled release of personal health information to a care provider or information custodian under an agreement that limits the extent and conditions under which that information may be used or released further.
- *Security*: A collection of policies, procedures, and safeguards that help maintain the integrity and availability of information systems and control access to their contents.

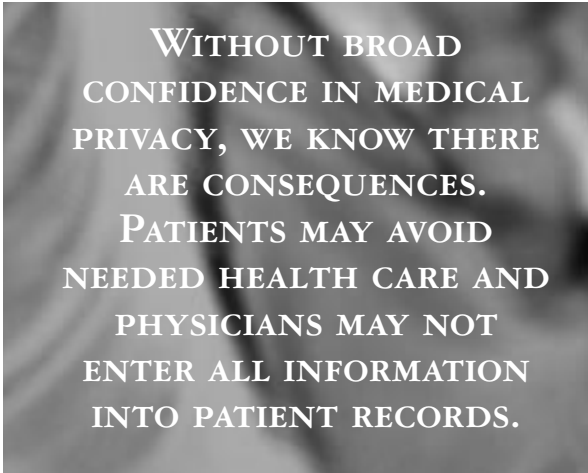
Threats to Confidentiality of Health Care Information

To understand the risks of disclosure of health care information and where information system technologies might be of help, we need to know how health care information is used. In 1976, Alan Westin developed a diagram [12] that shows the overall flow of information in the U.S. Health Care system (Figure 1). More recent studies have documented the extent of this flow as well (see [6, 9, 10]). We normally think of the medical record as a tool at the point of care—the doctor's office, clinic, or hospital. It supports primary care physicians, specialists, nurses, and administrators and has contributions from the many testing and treatment services. It is a memory aid to help a team of providers manage a patient during an encounter, to provide continuity of care from encounter to encounter, and to serve as an institutional record of care rendered.

Medical records also serve a variety of functions for organizations not involved directly in care. Records are sent to insurers (government and private) to justify payment for medical services rendered, and to detect fraud. They are used for quality reviews, administrative reviews, and utilization studies to manage the business aspects of health care. And they are used for societal purposes, such as medical research, public health management, social service

and welfare system management, law enforcement, screening and licensing for professions such as airline pilots, and determining life insurance eligibility.

Despite signing general consent forms as a requirement for obtaining health care in the U.S., the great majority of people (patients and physicians alike), have only a vague understanding of where health care data flows, often with little control of its use. In this complex system, risk of disclosure arises often. As in most information systems, few quantitative data exists on the nature and extent of security problems in health care institutions. There are few incentives or mechanisms to report incidents, and specific cases are most often handled quietly, unless a legal proceeding is filed. The consensus among health care CIOs is that the most important threats to patient information confidentiality are the following [9]⁴:



WITHOUT BROAD
CONFIDENCE IN MEDICAL
PRIVACY, WE KNOW THERE
ARE CONSEQUENCES.
PATIENTS MAY AVOID
NEEDED HEALTH CARE AND
PHYSICIANS MAY NOT
ENTER ALL INFORMATION
INTO PATIENT RECORDS.

From inside the patient care institution:

Accidental disclosures. Medical personnel make innocent mistakes and cause unintentional disclosures. A conversation may be overheard between care providers in the corridor or elevator. A lab technician may notice test results for an acquaintance. Information may be left on a computer screen where it can be seen by a passerby, or email or FAX messages may

be misaddressed.

Insider curiosity. Medical personnel abuse their record access privileges out of curiosity or for their own purposes. Some do so out of concern for the well being of fellow employees or family members. Some want to know about celebrities being treated. Some may be concerned about the possibility of sexually transmitted diseases in a colleague they are dating.

Insider subornation. Medical personnel knowingly access information and release it to outsiders for spite, revenge, or profit. Embarrassing health information about prominent people finds its way into grocery store tabloids or the public press with relative ease. It is said that Nicole Brown Simpson's (paper) medical records were available to the press

⁴We ignore threats from environmental and system failures in this list as outside the scope of this article. Good practice to cover these kinds of failures have been in place for decades and lower cost systems and peripheral equipment, such as RAID arrays, have made redundancy and backup more convenient and cost-effective than ever.

Table 1. Summary of technologies applicable to information system security management.

Intervention	Function	Example Technologies
Deterrents		
Alerts and reminders	Reinforce user ethics	Vendor-specific
Audit trails	Document access/give alerts	Custom research systems and some vendors
Obstacles		
Authentication	Determine who is connecting	Accounts/passwords, kerberos, tokens (e.g., SecurID), public-key systems, biometric systems
Authorization	Define who can access what information	OS file and database vendor access controls, DCE access control lists
Integrity management	Ensure information content is as intended	Cryptographic checksums
Digital signatures	Validate notes and orders	Evolving standards
Encryption	Prevent eavesdropping	PGP, kerberos, DES, public-key systems, secure sockets
Firewalls and network service management	Define system perimeter and control means of access	Many vendors
Rights management tools	Control information distribution and access	IBM Cryptolopes
System Management Precautions		
Software management	Guard against viruses, Trojan horses, etc.	Tripwire and controls over loading of uncertified software
System vulnerability analysis tools	Detect unintended system vulnerabilities	SATAN, crack, National Computer Security Association

within a week of her murder in 1994. The *London Sunday Times* reported in November 1995 that the contents of anyone's (electronic) medical record in Great Britain could be purchased on the street for £200.

From within secondary user settings:

Uncontrolled secondary usage. Those who have access rights to patient information for a purpose in support of primary care may exploit that access for other purposes not envisioned in patient consent forms—data mining in modern parlance.

Outsider intrusion into medical information systems:

Unauthorized access. Vindictive former employees, angry patients, network intruders, or others may steal information, damage systems, or disrupt operations. A recent NRC study of security practices in

health care institutions found no examples of (detected) outside intruder break-ins [9]. Nevertheless, reports abound of intrusions in business, academic, and government sites on the Internet (see [2, 4]). It must be considered an accident that such intrusions have not yet occurred at health care sites. This is a result of the fact the U.S. health care industry is still almost totally reliant on paper records.

The threats from insider disclosures and break-ins from outside intruders are easy to understand. But the risks to patient information confidentiality from secondary users need further explanation. We must emphasize that such secondary users as medical research, public health, governmental administration (like Health Care Finance Administration and Medicare), and law enforcement are very carefully controlled. Institutional review boards closely review and control medical research activities, courts

supervise law enforcement access, and the federal Privacy Act controls government use.

Secondary users of concern include insurers, pharmaceutical payers, some employers, and other players in the emerging health information services industry. While each of these users has a justified need to access patient information to carry out their function in the system, few controls are currently in place to ensure the information is used only for authorized purposes [9]. Some secondary users are highly conflicted. For example, self-insuring employers, under the Employment Retirement Income Security Act (ERISA), are entitled to receive fully identified patient information for employees being covered. Such information is nominally used to help the employer/insurer make sound benefits management decisions, but it can also affect whether employees get promoted, or even whether their employment is continued.

There is a temptation to use medical record information for business purposes other than those initially authorized—for example, to manage risk in insurance underwriting, to guide marketing of medical products, or to target special market segments for nonmedical services based on health status (for example, the presence of Alzheimer's disease). In a March 1996 consent decree filed in Minnesota and joined by 17 other states, a drug company agreed to stop using questionable marketing practices in interfering with the prescription of medications made by other companies as a by-product of seeing information to assess the allowability of drug insurance coverage.⁵

The potential for (ab)use of personal genetic information is very sobering. A recent study [3] reported 206 cases of direct discrimination—employment and insurability problems—from unauthorized use of genetic-test information. These cases reflect discrimination on the basis of future potential for (treatable) diseases. The patients exhibited no current phenotypic evidence of disease.

We must expect the privacy threat from data mining to grow. In a June 1996 cover story, *Information Week* predicted that overall industry revenues for data warehousing and mining technologies ran at \$2 billion in 1995 and were estimated to jump to \$8.8 billion by 1998. At least three companies in the health information services industry are members of the “terabyte club”—that is, organizations with very large-scale data warehouses used to collect and analyze data for business applications. It may be argued there is nothing wrong with using health care infor-

mation to make prudent and profitable business decisions. It's merely capitalism at work. But these uses conflict deeply with the confidentiality understandings most patients have when they sign consent forms. They certainly result in patients avoiding needed treatment in sensitive areas. And they make part of our population uninsurable or place the burden of costs on a group that can least afford them. We should at the very least openly discuss and decide these policy issues at a national level.

Technologies to Help Protect Health Care Information

Unlike paper-based patient records, where access control is almost entirely manual and procedural, technological security tools are an integral part of EPR systems and offer a number of advantages. The applicable technologies come largely from cryptographic and distributed systems research in computer science and, at the highest level, serve five key functions: [9]

- *Availability and integrity*: Ensuring that accurate and up-to-date information is available when needed at appropriate places.
- *Accountability*: Helping to ensure that health care providers are responsible for their access to and use of information, based on a documented need and right to know.
- *Perimeter definition*: Knowing and controlling the boundaries of trusted access to the information system, both physically and logically.
- *Role/need-limited access*: Enabling access for personnel only to information essential to the performance of their jobs, and limiting the real or perceived temptation to access information beyond a bona fide need.
- *Comprehensibility and control*: Ensuring that record owners, data stewards, and patients can understand and have effective control over appropriate aspects of information security and access.

We do not have space to detail the relevant technologies in this article, but only to provide a summary listing of various interventions, their functions, and how they relate to protecting privacy.⁶ As summarized in Table 1, there are three general classes of technological interventions to improve system security: *deterrents, obstacles, and system management precautions*. Deterrents depend upon the ethical behavior of people and provide reminders and oversight to reinforce those standards. Obstacles directly control the

⁵ Some pharmaceutical companies, like Merck and Lilly, have subsidiaries (Medco and PCS respectively) that administer insurance coverage for drugs.

⁶Detailed technological descriptions are readily available from other sources (for example, see [1, 7, 8]).

ability of a user to get at information, with the goal of constraining access only to information for which they have a need or right to know. System management precautions involve proactively surveying an information system to ensure that known sources of vulnerability are eliminated.

Table 2. Relation of disclosure threats to security technologies.

Threat	Principal Countermeasures
Insider abuse	
Accidental disclosures	Education, alerts, reminders
Insider curiosity	Education, authentication, authorization, audit trail, rights management tools (future possibility)
Insider subornation	Same as above
Secondary users	Rights management tools (future possibility)
Outsider intrusion	All available obstacles and system management precautions

It has been shown that deterrents—alerts, reminders, and education of users—are very effective in reinforcing already highly ethical behavior of the great majority of health care providers [9]. Also, audit trails are effective. If it is known that the system will record the identities, times, and circumstances of all users accessing information, and that these records are reviewed regularly, ethical users will think twice about abusing their privileges.

Technological obstacles can be equally effective. They support strong user and computer authentication, and ensure that users can access only information for which they have a bona fide need and right to know based on their identity and job function. They can also protect information against eavesdropping, ensure the integrity of information and software content, and validate the origin and content of orders and other critical transactions (digital signatures). Firewalls enforce manageable perimeters around distributed information systems, and limit modes/protocols for access. Finally, rights management software, such as the IBM Cryptolope system, offers interesting future possibilities for securely delivering information. Content is segmented and encrypted, the software used to access the record is standardized and distributed from the information custodian, and users are granted access keys based on their identity and need/right to know. Obtaining the key serves as a basis for an audit trail, even perhaps across institutional boundaries.

System management precautions are crucial and include taking advantage of accumulated community experience about security vulnerabilities. Software management prevents introduction of programs like viruses, Trojan horses, or other aberrant codes. The Computer Emergency Response Team (CERT) emphasizes that many ongoing network break-ins come from failures to configure systems properly and maintain them at current releases of system/service software.

The Role of Technology

The application of any administrative or technical intervention to protect information requires an explicit policy defining what is appropriate use of information and what is not. Such a policy should include as a minimum a statement of institutional philosophy and goals regarding privacy and security;

a classification of information assets by type; standards for administering, controlling, and monitoring information use by type; standards for information system design, implementation, and operation; and a definition of procedures for detecting and handling abuses.

In principle, many of the technologies needed to do a prudent job of protecting medical information system security are available, if not deployed in commercial systems or in routine practice [9]. We can relate the classes of disclosure threats to available tools as shown in Table 2.

Simple, mostly nontechnical measures are appropriate to avoid accidental disclosure of confidential information or curiosity-driven disclosure. Technology, such as audit trail systems, can play an important role to curtail insider curiosity or subornation. In the future EPR technology might help by maintaining patient anonymity through use of coded patient identifiers (pseudonyms) in at least some parts of the care process.

To date, technological deterrents and obstacles play almost no role in controlling exploitation of patient information by secondary users. Once information leaves the hands of the health care provider, it is stored off-site by the secondary user and access and use controls are subject to the ethics and procedures in place by that user site. With such an unsupervised system, ethical controls fall short. In the future, in addition to tighter legal restraints, rights management software may provide a more effective

way to control inappropriate secondary use.

Blocking outsider intrusions will be a major problem judging from the successes intruders now enjoy in attacking academic, business, and government systems. Special diligence is needed for health care systems to ensure state-of-the-art protections. This might include special dedicated network segments for health care enterprises and establishment of "medical CERT" and industry oversight groups to ensure high security standards.

Ultimately, security and privacy of health care information is a "people problem." Technology can help to ensure that only health care personnel access information they have a right and need to know, and that information gets from one place to another accurately and securely. But technology can do very little to ensure the person receiving the information will handle it according to confidentiality standards. That depends on ethics and an effective supervisory and legal structure that provides sanctions against detected misuse.

Security measures in medicine must be chosen and integrated rationally. The measures must be balanced so they protect against a realistic assessment of risks and costs. Real-world information systems will always be vulnerable. Also, threats, particularly those arising from outside the enterprise, will continue to evolve with overall technological developments in computing and networking. Finally, each security intervention must be evaluated jointly in terms of its functional benefits for protecting patient, provider, and institutional privacy and in terms of its costs. These costs include the cost of purchase and integration into the information system environment; the cost of on-going management, operations, and maintenance; the cost of user time lost to satisfy security protections; and the cost of user frustration with clumsy interfaces and procedures.

It is unthinkable that we would impose system security constraints so tight that they would prevent an emergency room doctor from accessing the record of a seriously ill, comatose patient. Such exigent access may only be needed from special locations, but their existence means an enterprising intruder may fool system access controls and break-in more easily. How should we make this trade-off?

Also, we must recognize that physicians are under growing pressure to increase productivity. They are asked to see more patients in less time while making better (or at least better justified) decisions about diagnosis and treatment. Providers can not tolerate

time delays and frustrations in passing frequent record access security hurdles.

Individual technologies vary widely in terms of these cost/benefit characteristics and, as new technologies are developed and reduced to commercial practice, their characteristics change with time. System managers must choose a set of technological interventions that provide effective protection against perceived threats to system security but which overall impose acceptable costs. This choice is difficult at best and no acceptable standards of performance exist. These remain to be defined and will certainly require ongoing updates of threat models; evaluations of technologies; reconsideration of integration and operation strategies; and education of management, systems staff, and users.

Opportunities, Actions, and Impediments

The development and integration of EPR systems into modern U.S. health care institutions is absolutely essential and inevitable for optimal health care, medical research, public health, and the operation of modern health care enterprises. Such systems do not exist in most health care institutions today, but they have been demonstrated in a variety of academic, public, and commercial medical settings. Even paper-based medical record systems entail substantial risks of disclosure of sensitive personal health care information. The primary threats arise from various kinds of disclosures by members of the health care provider community themselves, and from uncontrolled use of information among secondary users. Longer-term threats to health information confidentiality will come from network intruders. The rapidly developing uses of data mining technologies in business and health care signal still more threats that raise significant policy and legal issues.

As we move toward the era of computerized medical record systems, we must design the systems from the start to accommodate evolving policies and security management technologies, and develop standards to integrate and administer computerized health information systems prudently. The broad and effective use of existing, but largely undeployed, technological tools in the computerization of patient-identified health care information can help prevent exploitations of sensitive information, and/or make it clear to data owners that exploitations have happened.

Substantial U.S. public policy and legislative issues must soon be addressed that will define the standards and safeguards that are to be applied to all health care information, not just that in digital

form.⁷ These must focus on the current hodgepodge of state-based privacy laws and the loopholes in current laws that allow uncontrolled access to and exploitation of patient-identified health care information in parts of a developing health information services industry.

There are extremely difficult trade-offs to be made in this debate. The significant advantages of facile information access for improved medical care, enhanced research, and more cost-effective management of medical institutions have to be traded off with the privacy consequences. In cold business terms, this comes down to assessing the value of health care information, the magnitude of the risks of improper disclosure, the costs of an improper disclosure incident, and the costs of preventative measures. However, whereas financial enterprises such as banks and credit card systems can absorb the costs of abuse over the user community, without undue hardship on individuals, medical enterprises can not. Once sensitive information about an individual is exposed and the resulting damage is done to that person, the information can not be withdrawn and made secret again. Thus, we must move very aggressively on issues such as strong legal restraints for abuse and incorporating effective cryptographic tools for security management. At the same time, we must move very carefully on features such as universal patient identifier (UPI) systems.⁸ A UPI may be desirable from some medical practice viewpoints to link dispersed records in the interest of care, but would pose unacceptable privacy risks. In the current setting, the UPI could be exploited as easily by data miners as by bona fide physicians. Such features should not be adopted broadly until we have demonstrated and are confident about the strength of properly designed medical information system security and accountability procedures, and have in place effective legal safeguards and sanctions for abuse.

Existing medical information systems are mostly home built, or involve collections of legacy systems that do not interoperate. For wide deployment, we will need a uniformly interoperable, vendor-supplied set of system components that incorporate highest performance security features, based on public and secret key encryption technologies. Only then will the standards develop and the costs come down to allow these tools to be integrated in effective ways.

The needed technologies exist or are under development in the Internet distributed computing and commerce arenas, but they are not yet deployed in a way that allows integration into enterprise computing environments.

Contentious policy issues and potential roadblocks surround ongoing federal government controls on the export of strong cryptographic technologies. These restraints, based on understandable concerns for national security and law enforcement, in turn delay the willingness of U.S. computer companies to invest in commercializing strong security tools since they could not be marketed in the worldwide market for modern Internet systems. A further consequence may be a delay in the emergence of essential electronic medical information systems that are acceptably secure. **C**

REFERENCES

1. Garfinkel, S. and Spafford, E. *Practical UNIX & Internet Security*. O'Reilly, Sebastopol, Calif., 1996.
2. General Accounting Office/Defense Information Systems Agency. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. GAO/AIMD-96-84, May 1996.
3. Geller, L.N., Alper, J.S., Billings, P.R., Barash, C.I., Beckwith, J., and Natowicz, M. Individual, Family, and Societal Dimensions of Genetic Discrimination: A Case Study Analysis. *Sci. and Eng. Ethics* 2, 1 (1996).
4. Gembicki, M. Information Systems Security Survey. WarRoom Research, LLC, <http://www.infowar.com/sample/survey.html-ssi> Nov. 23, 1996.
5. Institute of Medicine. The computer-based patient record: An essential technology for health care. National Academy Press, Washington, DC, 1991.
6. Institute of Medicine. Health Data in the Information Age: Use, Disclosure, and Privacy. National Academy Press, Washington, DC, 1994.
7. Khanna, R. *Distributed Computing—Implementation and Management Strategies*. Prentice-Hall, Englewood Cliffs, N.J., 1994.
8. National Research Council. Computers at Risk: Safe Computing in the Information Age. National Academy Press, Washington, DC, 1990.
9. National Research Council. For the Record: Protecting Electronic Health Information. National Academy Press, Washington, DC, 1997.
10. Office of Technology Assessment. Protecting Privacy in Computerized Medical Information. OTA-TCT-576, US Government Printing Office, Washington, DC, 1993.
11. Rothfeder, J. *Privacy for Sale*. Simon and Schuster, New York, NY, 1992.
12. Westin, A.F. Computers, Health Records, and Citizen Rights. National Bureau of Standards, Monograph 157, US Government Printing Office, Washington, DC, 1976.

This work was supported by the CAMIS (# LM05305) and InterMed (# LM4-3514) grants from the National Library of Medicine.

THOMAS C. RINDFLEISCH (tcr@smi.stanford.edu) is director of the Lane Medical Library, and director for the Center for Advanced Medical Informatics, Stanford University.

Permission to make digital/hard copy of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage, the copyright notice, the title of the publication and its date appear, and notice is given that copying is by permission of ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a fee.

© ACM 0002-0782/97/0800 \$3.50

⁷The Health Insurance Portability and Accountability Act, passed in Sept. 1996, requires the secretary of Health and Human Services to establish regulations about health information exchange standards and security practices should Congress fail to pass explicit legislation in this area.

⁸The social security number has been proposed for this purpose, but clearly lacks necessary features such as authenticated uniqueness, resistance to forgery, revocability, trust, and controlled use.