Privacy, Security, and Shared Access — Can Confidentiality Be Protected in a Networked Society?

by David Voran

We live in a predominantly service-oriented, market-driven economy in which detailed customer knowledge is often seen as the major differentiator between success and failure for many companies. In this environment, medical care is now a complex process involving many entities (e.g., hospitals, physician offices, insurance carriers, pharmacies, social workers, and employers). Much more patient information is now contained in medical records, and much of this information needs to be shared among a wide spectrum of service providers. As the pressure increases for access to this information, individual privacy is threatened. This paper briefly discusses the opposing forces of access and confidentiality and offers insight in dealing with these issues.

Over the past few years, society has become very fluid. People are frequently changing residences, employers, and insurance carriers. At the same time, companies are continually evaluating insurance providers and making annual changes in insurance carriers to lower health care costs. Insurance carriers also frequently modify the various insurance plans they offer to meet their customers' demands.

Changes in the health care delivery system — including increased penetration of managed care, scrutiny of documentation and billing practices, pervasiveness of litigation, and emphasis on ambulatory care — have increased the importance of the information network.

These factors and similar pressures dramatically increase the amount of information collected on each person enrolled in an insurance plan, seeing a physician, or staying in a hospital. For example, a ten-day stay at the University of Kansas Medical Center in 1938 resulted in a ten page medical record. A ten-day stay for the same condition in 1997 will routinely involve a chart that exceeds 100 pages.[1]

Decisions cannot be made without access to information in a timely fashion. The better and more personal the information, the better and more focused the decision. As a result personal information has become a commodity, captured and compiled, bought and sold in ways never before imagined.

While many businesses have been created to capitalize on this market, the significance of the information and the pressure to extend it are most important in medicine. Simultaneous access to a wide variety of personal information is a necessary link to many health care services. Time constraints and the need for many people to have information has led to duplication of the paper record and, in recent years, to computerizing the medical record.

People inadvertently leave bits of personal information in a variety of places as they shop, visit health care professionals, look up information, and receive services. Data aggregation companies such as Metromail, First Data Solutions, and Acxiom, are the conduit. Each maintains information on more than 90 million households and 140 million people. Their databases track an individual's birthplace, travel habits, purchases, (including prescription medications), and phone records.[2]

The cost of accessing and using this information used to be prohibitive. However, new technology enables most businesses to tap this information easily. As the value of this information rises, access to it becomes easier. These developments compromise individual confidentiality and threaten the security and integrity of the information.

Balancing the need for information and accessibility against the need for maintaining privacy, confidentiality, and integrity of information is a very difficult problem that must be solved to avoid future serious moral and ethical dilemmas.

Privacy

Privacy refers to an individual's right to protection from unauthorized intrusion. In the information age, privacy refers specifically to the unauthorized access, collection, and use of personal information. Privacy also means the right to control information about one's self even after divulging it to others.

Unauthorized access to personal information can be accomplished in many innocent and nefarious ways. Examples include the illicit copying of credit card numbers (e.g., by a waiter to whom a card has been entrusted); listening to cordless phone conversions on inexpensive scanners; reading a customer's purchases as they are rung up and displayed on a grocery store monitor; or, in the medical setting, reading a patient's chart when visiting a hospital.

But do people really care? A 1995 Harris Poll showed that 84 percent of American people are concerned about threats to privacy. Similarly, a 1997 Business Week/Harris poll found that 53 percent believe laws should be passed governing how information should be collected and used on the Internet. Yet there is ample evidence that most people are not taking steps to protect their privacy. Most continue to use cordless phones and credit cards, and many routinely give out personal information to sweepstakes telemarketers; call 800, 888, or 900 numbers to answer polling questions or request information; and frequently answer detailed information at various web sites.

Security

Gerard Nussbaum, senior manager with Hamilton KSA, defines security as having three interrelated facets: availability, integrity, and confidentiality.[3]

By definition, *availability* is the ability of authorized people to gain access to information for normal use. As such, availability involves not only the information but the dependable infrastructure necessary to keep systems operational at all times. If the system isn't available, then many other aspects of security may not matter. The system may also be compromised, intentionally or unintentionally, by speed.

Integrity involves measures to prevent data from being altered, and detection measures when data is altered. These efforts usually focus on the protection of the data rather than on its accuracy. Note, however, that accuracy is not possible without integrity, though integrity is possible without accuracy.

Confidentiality refers to the overall use of the data and requires a management framework of policies and procedures that address legal issues associated with appropriate uses and disclosure. Absolute confidentiality of one set of data may impair the function of another dependent data set.

Measures to protect security include encryption, authentication, access control, physical barriers, and administrative controls. An ever-increasing level of sophisticated technologies and management structures surrounds each one of these measures. Nearly all institutions that computerize medical records are implementing all or most of these measures to protect unauthorized access and the integrity of the data as they struggle to increase the availability of the information.

The medical record, by definition, is composed of all information pertaining to an individual's medical condition. Keeping a patient's secrets private is a basic element of the Hippocratic oath.

In practice, however, it is virtually impossible to practice medicine without sharing this information with others. While laws do seem to protect private information and prohibit its disclosure, many exemptions exist. Most patients, for example, must waive their right to confidentiality in return for insurance coverage.

Medical records are created when treatment from a health professional is received. These records may include a medical history, lifestyle details (e.g., smoking or drinking habits, or involvement in high-risk sports), and the patient's family medical history. They may also contain laboratory test results and other reports indicating the results of operations and other medical procedures. A wide range of people both inside and outside the health care industry shares this medical information, including insurance companies, government agencies, employers and self-insured businesses, courts, quality control and licensing personnel, researchers, public health agencies, and direct marketers.

- Insurance companies require clients to release their records before they will issue a policy or make payment under an existing policy. Medical information gathered by one insurance company may be shared with others through the Medical Information Bureau.

- Government agencies request medical records to verify claims made through Medicare, Social Security Disability and Workers' Compensation.

- The Medical Information Bureau (MIB) is a central database of medical information. Approximately 15 million Americans and Canadians are on file in the MIB's computers. Over 750 insurance firms use the services of the MIB primarily to obtain information about life insurance policy applicants. A decision on whether to insure an individual is not supposed to be based solely on the MIB report.

  The MIB does not have a file on everyone. But if a person's medical information is on file, it can be obtained by writing to Medical Information Bureau, P.O. Box 105, Essex Station, Boston, MA 02112, or call (617) 426-3660.

- Employers usually obtain medical information about their employees by asking employees to authorize disclosure of medical records. This can occur in several ways.

  When employers pay medical insurance, they may require insurance companies to provide them with copies of employees' medical records.

  Self-insured businesses establish a fund to cover the insurance claims of employees. Since no third party is involved, the medical records that would normally be open for inspection by an insurance company are accessible to the employer.

  While employers may gain access to their employees' medical records, state and federal law offers some privacy. Employers must establish procedures to keep employee medical records confidential. According to the federal Americans with Disabilities Act (42 USC §12101 et seq.), in workplaces with more than 25 employees, employers may not ask job applicants about medical information or require a physical examination prior to offering employment. After employment is offered, an employer can only ask for a medical examination if it is required of all employees holding similar jobs.

- Medical records may be subpoenaed for court cases.

- Other disclosures of medical information occur when medical institutions such as hospitals or individual physicians are evaluated for quality of service. This evaluation is a licensing requirement for most hospitals.

- Occasionally, medical information is used for health research and is sometimes disclosed to public health agencies like the Centers for Disease Control. Specific names are usually not included with the information.

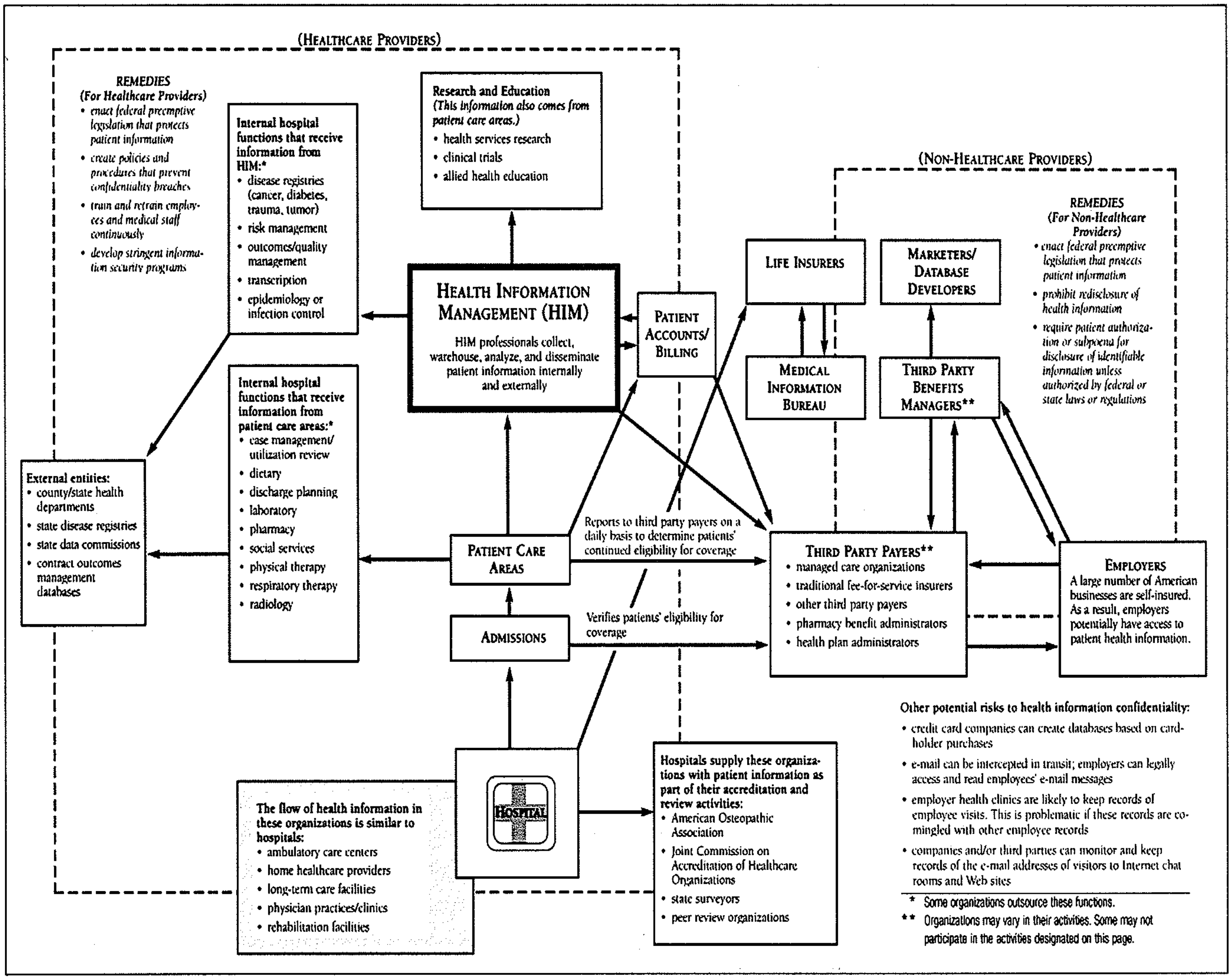
(Healthcare Providers)
REMEDIES
(For Healthcare Providers)
• enact federal preemptive legislation that protects patient information
• create policies and procedures that prevent confidentiality breaches
• train and retrain employees and medical staff continuously
• develop stringent information security programs
Internal hospital functions that receive information from HIM:*
• disease registries (cancer, diabetes, trauma, tumor)
• risk management
• outcomes/quality management
• transcription
• epidemiology or infection control
Research and Education
(This information also comes from patient care areas.)
• health services research
• clinical trials
• allied health education
Health Information Management (HIM)
HIM professionals collect, warehouse, analyze, and disseminate patient information internally and externally
Patient Accounts/ Billing
Internal hospital functions that receive information from patient care areas:*
• case management/ utilization review
• dietary
• discharge planning
• laboratory
• pharmacy
• social services
• physical therapy
• respiratory therapy
• radiology
External entities:
• county/state health departments
• state disease registries
• state data commissions
• contract outcomes management databases
Patient Care Areas
Reports to third party payers on a daily basis to determine patients' continued eligibility for coverage
Admissions
Verifies patients' eligibility for coverage
(Non-Healthcare Providers)
Life Insurers
Marketers/ Database Developers
Medical Information Bureau
Third Party Benefits Managers**
REMEDIES
(For Non-Healthcare Providers)
• enact federal preemptive legislation that protects patient information
• prohibit redisclosure of health information
• require patient authorization or subpoena for disclosure of identifiable information unless authorized by federal or state laws or regulations
Third Party Payers**
• managed care organizations
• traditional fee-for-service insurers
• other third party payers
• pharmacy benefit administrators
• health plan administrators
Employers
A large number of American businesses are self-insured. As a result, employers potentially have access to patient health information.
Hospital
The flow of health information in these organizations is similar to hospitals:
• ambulatory care centers
• home healthcare providers
• long-term care facilities
• physician practices/clinics
• rehabilitation facilities
Hospitals supply these organizations with patient information as part of their accreditation and review activities:
• American Osteopathic Association
• Joint Commission on Accreditation of Healthcare Organizations
• state surveyors
• peer review organizations
Other potential risks to health information confidentiality:
• credit card companies can create databases based on cardholder purchases
• e-mail can be intercepted in transit; employers can legally access and read employees' e-mail messages
• employer health clinics are likely to keep records of employee visits. This is problematic if these records are comingled with other employee records
• companies and/or third parties can monitor and keep records of the e-mail addresses of visitors to Internet chat rooms and Web sites
* Some organizations outsource these functions.
** Organizations may vary in their activities. Some may not participate in the activities designated on this page.

Figure 1. — Flow of Patient Health Information Inside and Outside the Health Care Industry (AHIMA 1999).

- Medical information may be passed on to direct marketers when people participate in informal health screenings. Tests for cholesterol levels, blood pressure, weight and physical fitness are examples of free or low-cost screenings offered to the public. Screenings are often conducted at pharmacies, health fairs, shopping malls or other nonmedical settings. The information collected may end up in the databanks of businesses that sell products related to the test.

In the paper world, this need for sharing led to duplications of the medical record. In fact, any given interaction of a person with formal medicine generates several medical records, and a person's complete medical record is stored in many locations, as illustrated in Figure 1.

Managing the distribution of multiple entities of the medical record is challenging. Furthermore, monitoring authorized access to these charts is daunting. Many would argue that there is no feasible way of effectively monitoring paper-based records. The only effective barriers to access are literacy and geographic proximity.

Computerizing the chart would allow many individuals simultaneous access and, through audit trails, provide documentation of each use. Furthermore, computerization of the medical record does increase the difficulty of printing out a single medical paper record in chart-like fashion — since the computerized record is composed of disparate data elements from different systems brought together "on the fly" by the user interface.

It is, on the other hand, very easy to locate and print sensitive components of the record.

On the surface, computerization does appear to address the issues of availability and access. However, this method also increases the potential for invasions of privacy by eliminating many of the physical barriers to the chart. This "invasion" of privacy can be used to good and bad effect.

For example, Harvard Pilgrim New England, a Boston-based health plan, identifies patients with diabetes and includes them in a disease management plan. The plan increased annual retinal exams by 26 percent and eliminated diabetes-related major malformations of newborns. On the other hand, horror stories of medical records abuse include the Colorado medical student who sold patient records to lawyers looking for easy malpractice cases, and the Maryland banker who tracked his customers suffering with cancer to call in their mortgages.[4]

Protection

Currently, no comprehensive laws exist to protect medical record privacy. There are, however, steps that individuals can take to improve their privacy. These steps include

- Limiting the amount of information released through a treatment waiver. Instead of signing a "blanket waiver," individuals may cross general terms out and write in more specific terms (Fig. 2).

- Revoking a previous consent. In this case, individuals can bring a written request to the appointment that revokes their consent to release specific medical information to the insurance company and/or to their employer for that visit. They must also pay for the visit themselves rather than obtain reimbursement from the insurance company.

Blanket waiver: I authorize any physician, hospital or other medical provider to release to [insurer] any information regarding my medical history, symptoms, treatment, exam results or diagnosis.

Edited waiver: I authorize my records to be released from [X hospital, clinic or doctor] for the [date of treatment] as relates to [the condition treated].

Figure 2. — Limiting the extent of treatment waivers.

- Using caution when filling out medical questionnaires or participating in informal health screenings. Individuals can find out whether disclosure is mandated by an episode of care, the purpose of the disclosure, and who will have access to the information before they give consent.

- Asking that health care providers and the courts use caution when dealing with medical records. If records are subpoenaed for a legal proceeding, they become a public record. Individuals should ask the court to allow only a specific portion of their medical records to be seen or that the record not be opened at all. A judge will decide what parts, if any, of one's medical record should be considered private. After the case is decided, individuals can also ask the judge to "seal" the court records containing this medical information.

- Determining whether health care providers have a policy on the use of cordless and cellular phones and fax machines transmitting medical information.

Cordless phones are essentially radio transmitters and can be listened to by simple, inexpensive radios. Fax machines offer far less privacy than the mail. Frequently many people in an office have access to fax transmissions. Staff members at all levels of the organization should take precautions to preserve confidentiality when sending and receiving medical documents by fax machine.

Concluding Thoughts

Computer technology has transformed the expensive process of using old mainframe records into a high-tech industry that compiles, cross-references, and exchanges private data instantaneously.

Recent studies have shown that privacy is the number one concern of Internet users and also the top reason that others avoid the Internet.[5] Nevertheless, over 40 million people have access to the Internet. Using this medium, banking, information, travel, manufacturing, and retail industries have brought their services to people's fingertips. People now have more information than ever before in making day-to-day decisions. At the same time, consumers' own lack of discretion may be the biggest threat to what they say is their primary concern: privacy.

Over 40 percent of all Internet users surveyed in a 1997 American Internet User Survey have sought and found medical information on the Net. In fact, medical sites are the third most anticipated site visit after online banking and adult education.[6] In another survey, researchers discovered that 80 percent of users have accessed medical information on the web and 36 percent of the users access medical sites monthly.[7]

Medical software vendors, aware of this trend, are making their applications available over the Internet. They are also working to provide personal reviews of the data. There is little doubt that in the near future individuals will have online access to their own medical records. Furthermore, individuals may be able to interact with this dynamic database and contribute to their own records. This trend will dramatically increase the availability of medical information.

Widespread availability increases the difficulty of assuring privacy and integrity of the information. As availability increases, so do the points at which the security of the information can be threatened. Further, the more convenient it is for people to access and leave information, the more likely they are to use those tools to voluntarily sell their own privacy in return for information.

It could be argued that people don't really care about the information they deposit on a daily basis, provided it is used ethically and for their own good.

A key to ensuring ethical use of information will be to implement systems that allow the individual to see what information they are depositing, who is accessing that information, and how that information is being used. Such a system should also allow the individual to intervene and to share in the resulting profits if authorized. These tools, combined with effective legislation that enables the individual to seek compensatory damages for unauthorized use, will give individuals the freedom to share, control, and profit from their own privacy.

Notes

1. Personal research. 1996.
2. Jeffrey Rothfeder. 1998. "You Are For Sale." *PCWorld* 16(9).
3. Gerard Nussbaum, and Star Ault. 1998. "Protecting the Security and Confidentiality of Healthcare Information." *The Journal of Healthcare Information Management Systems Society* 12(1).
4. Robert Davis. 1998. "Private Medical Records Make Public Rounds." *Final Edition* April 27, 1998.
5. http://www.cdt.org/privacy/guide/
6. http://etrg.findsvp.com/internet/netpr.pdf
7. 8th Annual GVU WWW User Survey. October 1997