Personal Privacy and Confidentiality In an Electronic Environment

by Ida Critelli Schick

Information systems and technology are essential components in an efficient managed care organization. The question arises: Is it possible to develop an electronic system that is secure, that is, protects patient privacy and confidentiality? This question can be answered affirmatively if a proactive agenda based on sound ethical principles is developed and implemented.

Introduction

As the structure of the health care delivery system changes, a key component in any new system is an electronic information network. This is particularly true in the managed care environment in which information systems and technology are essential to support efforts to decrease cost and increase quality.[1]

In response to overall health care costs, managed care organizations attempt to reduce the cost of providing a service, limiting the number of times a service is rendered where possible, and cutting administrative overhead for delivering service (Kennedy 1994). As costs become more closely controlled, providers are demanding faster access to clinical information (data and images). The result is the increased computerization of data, not only within hospitals, but also within large clinics, among health care providers in different locations, and between providers and payers.

Many factors are affecting cost and quality positively: the demand for quality health care service; the development of practice guidelines by physicians to standardize treatment for diseases; the concern among providers and patients alike for preventive measures and health promotion. Likewise, by facilitating information exchange among constituents, an electronic health information network (HIN) enhances the opportunities for long-term cost reduction, for more effective and quick disease treatment, and for health promotion.[2]

Although an electronic network offers significant benefits, such as projected cost savings by reducing administrative overhead costs and rapid clinical information exchange, there are significant risks in terms of privacy and confidentiality. These concerns center on unauthorized access to and/or unauthorized use of patient-specific data (both medical and nonmedical). This paper will address such concerns by exploring the current, growing electronic environment in health care; by reviewing privacy concerns in health care; and by setting a proactive agenda for health care organizations in dealing with privacy concerns in an electronic environment.

Increased Access to Patient Information

Fourteen years ago, Mark Siegler, a Chicago physician and ethicist, responded to a patient's privacy concern by counting those health professionals and hospital personnel who had access to his patient's medical chart. Seventy-five people involved in providing or supporting the patient's

Ida Critelli Schick, PhD, FACHE, is associate professor in the graduate program in Health Services Administration at Xavier University, Cincinnati, Ohio, and chairperson of the task force on privacy, confidentiality, and security, a part of the committee developing the Cincinnati community health information network.

health care services had access to the patient's chart (Siegler 1982).[3] This occurred in a predominantly paper/manual environment.

In the ensuing years the number of health professionals and administrative personnel who have access to patients' records has increased steadily. More people are involved in patient treatment, and more care is coordinated through patient care teams. But increased access is most evident in electronic systems that record, store, and transmit patient information. These systems have largely replaced paper record keeping, and it is in this arena of electronic record keeping that patient confidentiality and privacy are most at risk.

Privacy and Confidentiality Concerns

In a recent article on patient privacy within an electronic environment, *The New York Times* reported that when IMS of America, a company that sells data to drug companies, purchases patient records from organizations such as medical clinics and drugstore chains, the company often finds that patient names are included. IMS stated that it deletes these names and identifiers, such as social security numbers.

The same article reported that in Maryland, Medicaid clerks tapped into computers and printed out patient names and addresses, including medical records and incomes, which they sold to recruiters for HMOs. Beverly Woodward, Ph.D., an ethicist at Brandeis University, noted that some Boston hospitals enter entire patient medical records on line without informing or asking patients for their consent. Any doctor can then log on and look at any patient record, including psychiatric records (Kolata 1995).

Electronic prescriptions, time savers for the pharmacist and patient, are another problematic area when exploring privacy issues. In this system, the physician's clerk can enter the prescription, select the chosen pharmacy from a menu, enter the patient demographic information and a code that indicates this order as originating from the physician, and send it off. The system eliminates illegible physician handwriting, countless phone calls, wait times on the telephone, and so on. Some systems have added drug formulary and drug interaction features, so that when the prescription is entered, the program automatically checks the drug against the patient's prescription record, drug interaction, and formulary databases to ensure the order is appropriate.

Although the advantages of such systems are clear, the risks are also evident. For example, an ethical concern is raised when electronic prescriptions are channeled to pharmacy benefit managers, who may change them to meet formulary guidelines. Although pharmacy benefit managers deny that they change prescriptions, they claim a mandate from clients to reduce the drug dollar. The Ohio Board of Pharmacy contests this position and maintains that what is on a prescription belongs to the individual and cannot be released without the individual's approval (Siwicki 1995).

Additional concerns were listed by the Committee on Regional Health Data Networks (1994). These concerns include the following:

- routine release of information by providers to insurers, when much of the information does not relate to the insurance claim;
- release to third parties without the patient's knowledge or consent. This includes sharing information between the medical information board and a second insurer, sharing the health record within one organization (for example, between human resource departments and supervisors) or within an industry (between current employers and potential employers), and offering self-insured employers access to patient-identified health claims information provided to the employer by third party administrators;
- insider trading, which is the sale of information by those who have legitimate access to records;
- release of inaccurate information; this includes not only inaccurate listing or coding of information, but also inaccurate documentation intended to protect a patient from a

> stigmatizing diagnosis or to permit insurance coverage for a test that might not be covered (Donaldson and Lohr 1994).

Actual patient and family concerns were documented in the 1993 Harris-Equifax Survey, which revealed that Americans are generally concerned about their privacy but specifically concerned "about the misuse of confidential medical information " (Harris-Equifax Survey 1993). The majority believed that health professionals can be trusted to protect the confidentiality of their medical records, but they were not so positive about insurers, employers, or government or medical researchers.

Simply stated, there is concern that personal information divulged to physicians and other health care providers in the process of receiving health care services will be 1) accessed by unauthorized persons, and 2) used by authorized persons for negative or undesired reasons.

Privacy as a Core Value

Americans cherish their privacy. It is essential for creative endeavors, for raising families without interference from government, for being secure against unwarranted government intrusion, and for individual self-development. Alderman and Kennedy observed: "Although we live in a noisy world of self-confession, privacy allows us to keep certain facts to ourselves if we so choose. The right to privacy, it seems, is what makes us civilized" (Alderman and Kennedy 1995, p. xiii).

Privacy is essential for the individual in the contemporary world. Samuel Warren and Louis D. Brandeis set the discussion in motion with their 1890 *Harvard Law Review* article:

> The intensity and complexity of life attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury (Warren and Brandeis 1890, p. 196).

Warren and Brandeis define privacy as the right to determine the extent to which a person will communicate thought, sentiments, and emotions (p. 198) and the right to be let alone (p. 205). They determined that the foundation for this right is not the principle of private property but the principle of an "inviolate personality" (p. 205). Privacy, then, is the control over another's access to oneself — control over access to one's body, thoughts, opinions, and attitudes. Privacy allows one to circumscribe oneself with an invisible fence, beyond which others should not enter.

Privacy is also a precondition for relationships based on trust, an essential element in a provider-patient relationship.

The fence, however, has a gate. An individual can determine whether to speak freely to a friend; to allow access to one's body, family history, financial condition, thoughts, and opinions to health professionals; to communicate one's mind and thoughts to priests and counselors. Privacy is an aspect of autonomy, the ability to implement plans for one's personal development.

Privacy is also a precondition for relationships based on trust, an essential element in a provider-patient relationship. Patients would not reveal personal information unless they trusted that the health care provider would respect patient privacy by keeping this information confidential. These private revelations are entrusted in confidence because the provider and patient have mutual ends to attain: enhanced health status for the patient and reducing a patient's sense of possible shame or vulnerability (Siegler 1982).

Privacy, however, is not absolute. Personal privacy can be superseded when harm to oneself or to others is imminent and there is no other more acceptable way to avoid the harm, other than revealing the confidential information.

Protection of Privacy and Confidentiality

Despite widespread concern, it is possible for privacy and confidentiality to survive in the contemporary health care environment. Survival depends on conditions which are essential for a secure electronic environment, that is, one that protects privacy and confidentiality. These conditions include recognition that

- the system is patient-centered
- administrators and providers bear serious responsibility to protect privacy and confidentiality
- technical measures must be supported by practical administrative policies and procedures thatare actually implemented
- education and public discussions are needed to prepare society for this electronic era

Patient Focused

Health care systems must be patient focused. Patient information, no matter what the medium, belongs to the patient; information should be shared only with his/her consent. Autonomy, not beneficence, is the ethical center of privacy and confidentiality. An essential ingredient in a patient-focused system is that the enrollee/patient must be informed about the multiplicity of persons who have legitimate access to personally identifiable information, and why they need to know this information.

Moreover, in an electronic environment, those who have legitimate need and access should not have access to all the information, but only specific levels of information. The "role" assigned to a user through the computer software should allow that user access only to specified data and not to the entire file.

Additionally, the electronic system can be and should be designed so that the information can be shared only with the patient's permission.[4] The electronic system can be designed from a "push" perspective. For instance, if a primary care physician finds that the patient needs the services of a specialist, then the appropriate test results can be transmitted to the specialist with the patient's authorization. The patient in the physician's office can authorize transmission through the use of a magnetic stripe card or authorization number and then the data can be transmitted. The data on the server cannot be "pulled" or accessed by another physician.

Administrators' and Providers' Responsibility

Administrators and providers should be scrupulous in protecting patient privacy and confidentiality. Those who have legitimate access to patient data (whatever the medium) should sign confidentiality documents. These documents must be updated on a regular periodic basis.

An electronic system can log authorized access to data and attempts to access unauthorized segments of patient records. Those who have authorized access can develop unauthorized databases, but these unusual accesses can be logged electronically. These logs must be monitored by supervisors regularly and used as part of the employee's performance evaluation. The trustworthiness of individuals who will have access to patient data should be a pivotal criterion for hiring and for continued employment.

In addition, administrators and managers must develop policies requiring training in the use of the electronic system, the importance of privacy and confidentiality, and the system methods to protect these. As electronic systems continue to develop and evolve, security measures must also evolve and remain integral elements within those advances; education and training are necessary to stay abreast of these developments.

Further, administrators and others must not permit flaws in the present system to be replicated. What currently happens may be "accepted" but not "acceptable" ethically. For instance, many patient test reports and diagnostic test results are currently transmitted via fax. There are no technical measures (and realistically few authoritative administrative policies in place and enforced) which protect the patient's privacy in this context. This situation may be tolerated currently, but it need not be tolerated in an electronic environment. The latter can be designed so that only those who need to know (which is dependent on their "roles") can access the information. Electronic systems can be more secure than the current systems, if they are so designed and supported.

Technical Measures and Privacy

Technical measures alone cannot guarantee privacy and confidentiality. Numerous technical security measures can be implemented in an electronic system, ranging from the use of passwords and encryption to work station authentication devices, workstation inactivity time out. Technical measures, however, must be supported by administrative policy and by managerial and staff implementation. For instance, a password is a security measure thatallows access to authorized personnel; encryption of the password is used to thwart unauthorized persons from accessing the password to gain access to the system. Neither of these — password or password encryption — is effective when an authorized person gives his or her password to a colleague who is not authorized. The best technical security system can be undermined by human intervention. It is essential, therefore, that strict security measures be enforced administratively.

Implementing an Electronic System

Adequate preparations must be made to implement an electronic system. We are not ready technically or as a society to develop and implement centralized databases containing entire computerized medical records. Those who believe that we are ready, particularly from a technical perspective, do not have experience with the lack of standardized formats and the varieties of records and the multiple locations for records, even within a single facility such as a hospital. Although technical expertise may exist on the theoretical level, it must be linked with the practicalities of the health care environment.

This linkage has already begun and is evolving slowly. For instance, identifying a patient definitively in an electronic system may be difficult if the manual systems are not uniform. At Emory University System of Health Care, a project team discovered that the data among the EUSHC facilities are unexpectedly diverse. The data field length, definitions, and requirements varied. The team selected five identifiers and required a match across all five identifiers. Out of the 233,000 records, the system reported 4,034 possible duplicates. Ninety percent of these records were duplicates; ten percent did not belong to previously identified patients. Within the ninety percent, the most common errors were on the date of birth and the first name (Dardeen 1994). Matching a patient across a multiplicity of sites and their respective records is sensitive and tedious, but it is essential that the matching be correct. Developing a master patient index with strict matching across all identifiers is essential.

Society is not ready for an intricately integrated electronic world. We have only begun to make progress in health care in the area of informed consent so that the patient becomes the decision maker (or, at least, a participant in the decision-making process) relative to his/her care. We will regress in this process if we do not continue to emphasize patient-centered control in an electronic environment.

The public must have opportunities to voice concerns and to understand in lay terms what information systems can do, who can access them, what the purpose of access is, and so on. Since the information carried by systems is private information belonging to members of society, health care professionals must address their own concerns regarding information systems with the public (Bok 1989). For instance, the electronic information system raises questions concerning ownership of the data. Does the insurance company own the data on its claims database? Or is the claims database simply an extension of the medical record? Public involvement in answering these questions is needed.

Conclusion

The electronic era is rapidly evolving. The health care arena has accepted computerization, particularly in billing and accounting. The extension into the patient record keeping has already begun. However, the change must not occur haphazardly or without enrollee/patient input. It is essential for health care providers and managers to place the issue of computerization and protection of patient privacy and confidentiality in the public arena for discussion. Some of this work is being done through the efforts of institutional ethics committees and community health ethics centers. Once the patient and provider privacy/confidentiality issues are recognized, it will be possible to devise technical security measures to protect privacy. It is possible to develop a secure electronic system that is more secure than the current paper or mixed system. But we must be ready to work together to do so — provider, patient, insurers, and technical experts.

Endnotes

1. In a recent survey, information systems professionals in leading health care organizations cited managed care as the most significant force driving increased computerization (Aldrich 1995).

2. A health information network can be an enterprise (or system-specific) health information network (HIN) or a community health information network (CHIN). An HIN links its various system constituents who deliver and finance health services: physicians, hospitals, laboratories, pharmacies, payers, third party administrators, and others. A CHIN links HINs, unaffiliated providers, payers, and employers in a geographic area. The geographic area of existing and developing CHINs may be a city, county, region, or state. It is possible in the future that a number of these CHINs may be connected into a national network.

3. This number could be applied to any patient in that hospital unit, since it was based on employee positions with authorized access and the numbers of employees in each position, by shift, who would care for or provide support service to the patient.

4. There are at least two electronic age environments: 1) intra-institutional, that is, the presence of patient-specific information as individual institutions become more computerized internally, and 2) inter-institutional, that is, the presence of patient-specific information within multiple health systems, payers, and others, as these organizations are electronically connected (Schick 1996). Privacy/confidentiality concerns are, for all practical purposes, the same in both environment.

References

Alderman, Ellen, and Caroline Kennedy. 1995. *The Right to Privacy.* New York: Knopf.

Aldrich, Nancy. 1995. "Information Systems Professionals Cite Trends in Healthcare Computing." Special Report. *Healthcare Informatics* 12 (5): 16a-24a.

Bok, Sissela. 1989. *Lying: Moral Choice in Public and Private Life.* New York: Vintage.

Dardeen, Kathy. 1994. "ERNIE: Emory's Record Number Integrity Effort." *Journal of AHIMA* 65 (12): 26, 28, 30.

Donaldson, Molly, and Kathleen Lohr, eds. 1994. *Health Data in the Information Age.* Washington, D.C.: National Academy Press.

Harris, Louis, and Allan Westin. 1993. *Health Information Privacy Survey 1993.* Conducted for Equifax. New York: Louis Harris and Associates.

Kennedy, Robert. 1994. "The Value of CHINs" in *Community Health Information Networks,* ed. Ralph Wakerley. Chicago: AHA, 37-52.

Kolata, Gina. November 15, 1995. "When Patients' Records Are Commodities for Sale." *The New York Times* CXLV, 50,246: A1, B 7.

Schick, Ida Critelli. 1996. "Community Health Information Networks: Opportunity or Threat in the Doctor-Patient Relationship?" *Physician Executive.* Accepted for publication.

Siegler, Mark. 1982. "Confidentiality in Medicine — A Decrepit Concept." *The New England Journal of Medicine* 307 (24): 518-521.

Siwicki, Bill. November 1995. "Electronic Prescriptions: Just What the Doctor Ordered." Special Report. *Health Data Management* 62-68.

Warren, Samuel D., and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 14 (5): 193-220.