Protecting Patients' Privacy

Health Information Networks Raise New Questions

BY IDA CRITELLI SCHICK, PhD

Dr. Schick is associate professor, Department of Health Services Administration, Xavier University, Cincinnati.

The rise of health information networks (HINs)—networks that allow the electronic exchange of financial and clinical information among the various components of the healthcare system, including hospitals, physicians, pharmacists, other healthcare providers, payers, and employers—has seen new questions develop regarding patient privacy, and the ways it might be safeguarded in an electronic world. Consider these cases:

- In Maryland, Medicaid clerks tapped into computers and printed out patient names, addresses, incomes, and medical records and sold them to recruiters for health maintenance organizations (HMOs).
- The teenage daughter of a hospital emergency room clerk printed out the names and telephone numbers of patients who had used the emergency room the previous weekend, called them, and falsely told them that they were either pregnant or HIV positive; one of those contacted attempted suicide.
- IMS of America, a company that sells data to drug companies, purchases patient records from medical clinics and drugstore chains; the company often finds that names and other identifiers are included in these records.

While these may be examples of extreme abuses of information systems, concerns about personal privacy in an electronic environment have also been raised by the Institute of Medicine's (IOM) Committee on Regional Health Data Network Report[1] and the Harris-Equifax study.[2] These concerns include:

- The release of inaccurate information. Inaccuracies occur not only through coding and data entry errors, but also through the benevolent actions of providers who wish to protect patients from stigmatizing diagnoses or to permit insurance coverage.
- Improper disclosure. Providers routinely release information to insurers, even when much of the information does not relate to insurance claims.
- The release of information to third parties without the patient's knowledge or consent. This includes information released to the Medical Information Board, as well as to supervisors in work situations. The public, as well as the IOM, is concerned that such information will be used to deny life or health insurance, jobs, or promotions, or will serve as a reason for dismissal from a current job.

Whether personally identifiable information exists in a paper medium or an electronic medium, the concerns are similar. First, will those who have authorized access use it appropriately, or will they use it to harm others and/or violate their privacy? Second, are the data secure from those who are not authorized? In an electronic environment those with unauthorized access are generally hack-

Summary Privacy is established as both a value and a right in our society, and as healthcare moves to improve quality and efficiency through the development of health information networks, which allow the electronic exchange of financial and clinical information, there will be a growing awareness of the necessity to protect patient privacy and confidentiality in these environments.

Dealing with these concerns will require that healthcare providers take steps to ensure the security of patient information through technological and physical measures, programs of orientation and education, and the careful development and implementation of clear policies and procedures.

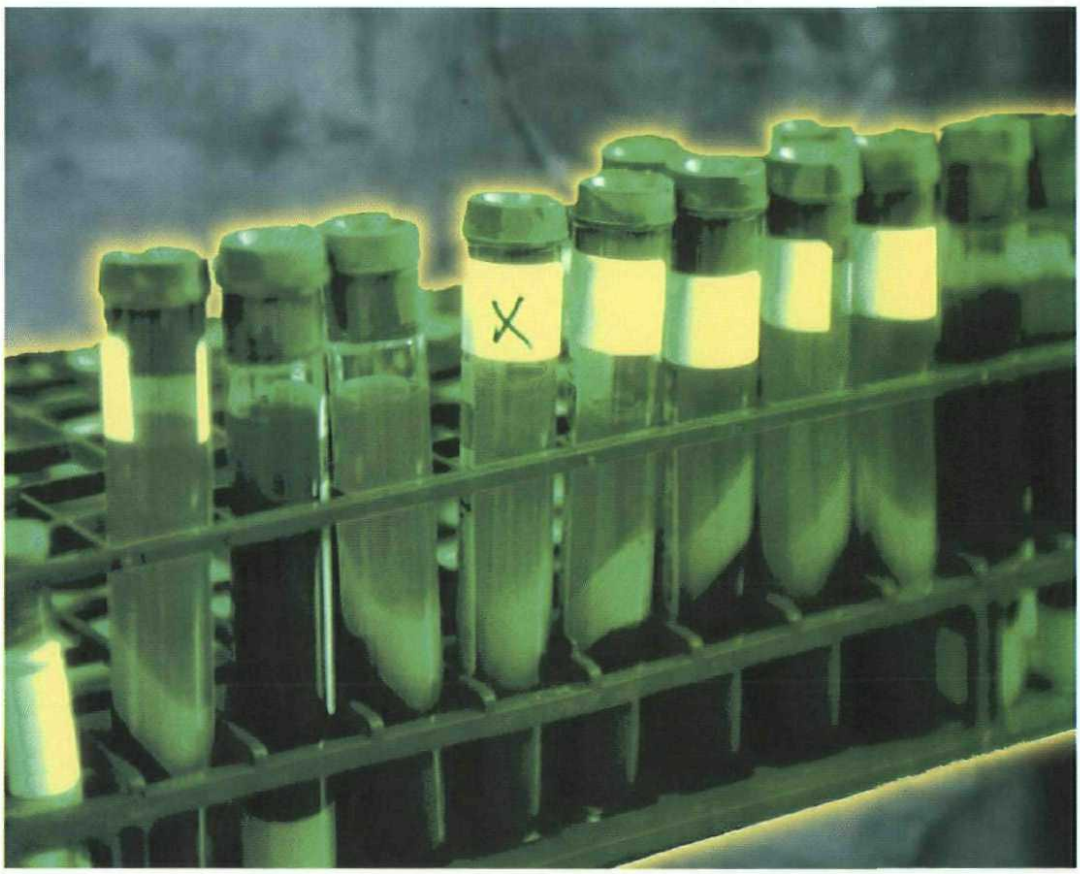
ers, who may simply wish to browse or who may have nefarious purposes. But the threat to privacy is greatest internally, from those who have authorized access, as the examples above illustrate. Of particular concern in the electronic environment is that once access has been attained, more data can be accessed with greater ease and speed than in the current paper or mixed paper-and-electronic environment.

Privacy: A Value and a Right

The plethora and popularity of "tell-all" radio and television talk shows seem to belie the statement that privacy is truly a concern and a value in our society. But Ellen Alderman and Caroline Kennedy, in their book *The Right to Privacy*, explain the phenomenon when they say, "Although we live in a noisy world of self-confusion, privacy allows us to keep certain facts to ourselves if we so choose. The right of privacy, it seems, makes us civilized."[3] These two attorneys echo the thoughts of their predecessors, Louis Brandeis and Samuel Warren, who, in an 1890 article in the *Harvard Law Review*, define privacy as the right to determine the extent to which a person will communicate his thoughts, sentiments, and emotions and the right to be let alone.[4] Brandeis and Warren identify the foundation of this right as the principle of private personality.

Several philosophical approaches justify the right to privacy and its flipside, the obligation to respect privacy. Tom Beauchamp and James Childress, in their book *Principles of Biomedical Ethics*, justify privacy as a rule and a right based on the principle of respect for autonomy.[5] Charles Fried emphasizes that privacy is a necessary condition for love, friendship, and trust.[6] Others justify rules of privacy based on its instrumental value for ends such as personal development or the expression of one's freedom.[7]

Although the foundation for privacy may be the subject of debate, the definition of privacy generally is not. Privacy is one's control over access to oneself—to one's body, thoughts, opinions, and attitudes. Control means that one may grant access to one's body, thoughts, opinions, and attitudes without waiving the right to privacy. As Beauchamp and Childress indicate, allowing access is not a waiver but an exercise of that con-



trol. In the physician-patient relationship there is a presumption of respect for privacy, and this presumption is one of the parameters essential to the relationship, a necessary condition for the relationship. Patients will not reveal personal information unless they trust the caregiver to respect their privacy by keeping the information confidential.* Patient and caregiver have mutual ends to achieve: enhanced health status for the patient and a reduced sense of vulnerability.[8]

Although privacy is a value and right in our society, it is not an absolute right. It can be overridden by values that our society has accepted as more important, such as public safety and public health. For example, these values override privacy when public safety requires reporting cases of communicable disease, gunshot and knife wounds, and child abuse. In the current healthcare environment, balancing the concerns for privacy focuses on the development of health information networks.

*Often the terms *privacy* and *confidentiality* are used interchangeably. *Privacy* is defined as control over access to oneself. *Confidentiality* is the promise not to reveal another's entrusted information to a third party without the confider's permission.

Health Information Networks

Today, payers are pressuring the healthcare ministry to reduce costs without reducing quality. HINs are one way to do this, particularly in the context of rapidly forming integrated delivery networks. HINs can take one of several forms: They can be enterprise networks, community networks, or regional networks. In the United States, there are well over 100 HINs in the planning or implementation stages: 52 HINs were represented at

DEVELOPING A CULTURE OF PATIENT PRIVACY

Amid rising concerns for patient privacy, the corporate ethics committee of the Franciscan Health System of the Ohio Valley–Cincinnati (FHSOV–C) sought to evaluate its two hospitals' practices that protect patient privacy. To evaluate the culture and practice of privacy, the ethics committee formed a task force consisting of a vice president, the director of risk management, the ethics consultant, and an intensive-care unit nurse. Before focusing on actual practices related to patient privacy, the task force first reviewed the corporation's current policies and procedures related to patient privacy. There were two key documents: the system's "Ethical Directives" and its "Statement on Patient Rights and Responsibilities" (see **Boxes**, pp. 30 and 31).

After studying these documents, the task force developed questions for one-on-one interviews with nurse managers and members of the nursing staff. The purposes of these informal meetings were to explore actual practices regarding patient privacy, to discover whether there were any problem areas, and to solicit staff recommendations for handling those problems.

There were six interview questions:

1. *Do we respect the patient's right to wear clothing of his or her choice?*
2. Do we allow the patient to read his or her chart?
3. Do we honor the patient's right to refuse visitors?
4. Do we examine patients in surroundings that provide visual and auditory privacy?
5. Do we keep patient information confidential?
6. Do we secure the patient's chart from those who are not authorized?

In two areas performance exceeded expectations. First, patient requests to wear personal clothing, even street clothes, are honored unless the clothing interferes with access to intravenous lines or monitoring leads. (Even in these cases, if the patient insists, the request is honored.) Second, the patient's right to read his or her chart is respected, although the physicians and nurses prefer that a professional be available to help the patient or surrogate read the chart.

Although patients have a right to refuse visitors, it is a difficult policy to enforce. At a patient's request, a "No Visitors" sign can be placed on the door, but on a busy unit it is hard to intercept unwanted visitors.

The interviews also indicated several areas that needed significant improvement. There were several problems related to visual and auditory privacy in examination areas in various locations within the hospital. Drawing curtains before examining a patient secures visual privacy, but not auditory. Also, doors in examination and treatment rooms are often left open so the staff can hear patients, but, as a result, patients may become visible to passersby. Further, fragile, elderly patients who may be waiting in a corridor or examination room may become uncovered and visible to those passing through the corridors.

The most difficult policy to implement was preserving the privacy of patient information. The task force noted in its discussions and visits to units the role the physical design of the facilities played in protecting—or not protecting—privacy. For example, telephone lines are installed in the hospital corridors between patient rooms, for the various caregivers to coordinate treatment. However, their conversations can be overheard quite easily by patients, visitors, or passersby, thus endangering privacy when patient names or room numbers are used. A similar concern was raised regarding the location of dictation cubicles; these are also located in the corridors between patient rooms. Communication boards on some units are located in public areas, such as oppo-

the summer 1996 annual meeting of the Community Medical Network Society. The networking systems include the hardware and software technology that moves the data, the content capabilities, and the advanced clinical technologies, such as telemedicine.

HINs are being planned, developed, and implemented to assure the integrity of data so that data are complete, accurate, and current; to provide information to those who need it to do their jobs, including nurses, doctors, therapists, pharmacists, billers, and insurers' claims clerks; and to simplify administration transactions.[9] A HIN will include the following data: insurance eligibility and enrollment, patient encounters, quality measurements, risk assessment, outcomes, and peer review data and research results. HINs electronically connect physician offices, hospitals, insurers, employers, and researchers.

The technologies that underlie HINs range from client-server technologies to intranet technologies and the Internet. IBM has developed HealthVillage, a healthcare information service on the Internet. Blue Cross and Blue Shield of Massachusetts offer on-line healthcare information and enrollment services to its members using an Internet-based system.[10] Software applications for transmitting patient records over the Internet are being developed, while the National Library of Medicine is sponsoring development of an intranet system in West Virginia. Elsewhere five corporations are sponsoring a three-part study of the Internet in healthcare.[11] Progress continues to be made in telemedicine, which transmits digitized images across long distances in electronic publishing and in computerized patient records.

However, the right to privacy is in tension with the speed of the development of information

site the elevators. These boards list patient names and schedules and are so positioned for the convenience of the staff, particularly the medical staff.

The final problem the staff interviews disclosed was the accessibility of the patient's chart in the "nurserver" cabinet located outside the patient's room. Charts are easily accessible if they are left lying open on the desk of the nurserver. It became clear to the task force that preserving the privacy of the patient's chart on the floor was not a defined responsibility.

The ethics committee task force undertook to verify that the chart in a nurserver was truly vulnerable. As a trial, the ethicist and a nurse on one unit in each hospital arranged for the ethicist to come anonymously to the unit and randomly read half a dozen charts, lingering at each chart for several minutes. The ethicist was dressed in a suit, with no identification tag or instrument, such as a stethoscope. In each instance the ethicist was able to read the charts. She even greeted hospital staff members when they needed the particular chart she was reading in order to write in it. At no time did anyone question her.

Later, the nursing staff on each unit met to discuss the ethicist's experience in this test and ask: How can we improve the situation? Their recommendations included:

- Try a central location for the charts on one unit. Monitor and evaluate the trial.
- Include a detailed segment on privacy of the chart in the orientation program for the staff. The risk management department should be responsible for this.
- Develop continuing education on personal privacy and the privacy of the chart and patient information for each unit and department.
- Study the placement of the nurservers. In one hospital, the nurservers are flush against the wall; in the other, they are at right angles to the corridor wall. In the latter configuration, it is very difficult to see a person reading or working at the nurserver.
- Consult with the facilities management staff about developing a spring-loaded catch on the drawer in which the chart is kept, so that the drawer will automatically close.
- Consult with the facilities management staff about the location of the corridor telephones. Could they be moved to more private locations?

These recommendations are already being acted on. The director of risk management, who is a member of the study task force and the ethics committee, worked with the appropriate divisions within the corporation to discuss and implement the recommendations. Interdisciplinary quality action teams have been formed to develop the spring-loaded drawers for the nurservers and to develop alternate locations for the corridor telephones. Communication boards throughout both hospitals have been moved so that they are visible only to those involved in patient care. Human resources personnel will work with the director of risk management to develop a videotape on privacy, since commercially available videotapes do not meet the system's needs; this video will be used for orientation and continuing education.

Another team is being formed to address the issue of insurance representatives' review of patient charts. Authorized persons must have some type of security clearance to access charts. It is also clear that there are different standards for accessing patient charts on nursing units and in the medical records department. The ethics committee proposed that a quality action team be formed to look at the issue, detemine who is responsible for security of the charts, and initiate a process for securing them.

technology and the ease of access to contemporary HINs. The role of networks is to make great amounts of data accessible to great numbers of users, yet the ease of access to such a wealth of information causes great concern about privacy and confidentiality. Is it possible to accommodate an acceptable level of privacy within this electronic network? It would be simplistic and unrealistic to say that absolute privacy can be guaranteed in any system. However, it is possible to assure a significant and acceptable level of privacy within an electronic environment.

Protecting Privacy and Confidentiality in a HIN

Within a HIN, security protections can be either technological or physical or rely on human support. These latter can involve programs for orientation and education of personnel, as well as programs for organizational development and implementation of policies and procedures. But ultimately the foundation for security, privacy, and confidentiality lies in the commitment of the organization. Without strong organizational commitment, even the most sophisticated physical and technological security measures can be undermined by human actions.

Technological Security Numerous technological security measures are available, such as restricting system access to users who have a user ID and password. Such a system can stipulate password characteristics (length, the use of multiple characters, the requirement that new passwords differ from previous passwords) and allow only the system administrator to change the password. The system can be set up to require verification of a user's status before allowing access to any application, and programmed to display a warning about the importance of privacy at an early point of entry. Biometrics, a recent development, uses signature verification or finger image technology to identify users.[12]

Many other technological steps can be taken to ensure security. The system can be developed with "firewalls," or computers that examine and restrict incoming and outgoing communications. The system can group users into classes with limited access to specific data. Individual workstations can be restricted to specific transactions; for example, the system can be set up so that billing can be done only from a workstation in the billing office, and nursing notes can be added only at the nursing workstation. Inactivity periods—the period between the end of active use and disconnection from the program, requiring a log-on to reactivate the program—can be tailored to specific workstations, so that workstations likely to be unattended for long periods of time have a very short inactivity period. To avoid mass printing, the system can limit the number of records that can be printed, and passwords, identifiers, and sensitive information can be encrypted. Transactions and attempted transactions can be logged and audit trails provided at regular intervals.

Physical Security Physical means to protect information systems and their data include securing the telephone lines in electronic closets, physically securing any backup tapes, and properly and completely destroying old backup tapes. Workstations can also be secured so that they cannot be removed or used in another location. Finally, in a client-server technology, the hub, which may be physically remote, should also be physically secure.

Orientation and Education Actions to ensure the human element of security include both orientation and education. Everyone who will have

PATIENT RIGHTS AND RESPONSIBILITIES

The FHSOV–C "Statement on Patient Rights and Responsibilities" states:

The patient has the right, within the law, to personal and informational privacy, as manifested by the following rights:

a. To refuse to talk with or see anyone not officially connected with the hospital, including visitors, or persons officially connected with the hospital but not directly involved in his/her care.

b. To wear appropriate personal clothing and religious or other symbolic items, as long as they do not interfere with diagnostic procedures or treatment.

c. To be interviewed and examined in surroundings designed to assure reasonable visual and auditory privacy. This includes the right to have a person of one's own sex present during certain parts of a physical examination, treatment, or procedure performed by a health professional of the opposite sex and the right not to remain disrobed any longer than is required for accomplishing the medical purpose for which the patient was asked to disrobe.

d. To expect that any discussion or consultation involving his/her case will be conducted discretely and that individuals not directly involved in his/her care will not be present without his/her permission.

e. To read his/her own medical record and to have his/her medical record read only by individuals directly involved in his/her treatment or in the monitoring of its quality or as otherwise permitted by law. To have the information on his/her medical record explained or interpreted as necessary except when restricted by law. Except as required/permitted by law, other individuals can only read his/her medical record on his/her written authorization or that of his/her legally authorized representative.

f. To expect all communications and other records pertaining to his/her care, including the source of payment for treatment, to be treated as confidential.

authorized access to records in the electronic network should have initial and continuing training and education about the system itself and also about the importance of privacy and confidentiality. Users must understand that passwords cannot be shared or written down where others can find them. They must also understand that the most extensive technological and physical security systems can fail through human failure. Finally, as the technology (including security) is upgraded, user training must be updated.

Policies and Procedures To guide both technological and human security measures, the organization that employs the technology must establish policies and procedures that delineate the purpose of the technology, the parameters for appropriate use, and the procedures for proper use of the technology, including e-mail and Internet etiquette. Departmental policies and procedures should complement organizational policies and procedures. Such policies and procedures, however, are only as effective as their implementation, which can involve several methods.

First, it is essential to hire individuals who respect patient privacy, particularly for positions where there is access to patient information. Second, job descriptions for these positions should specifically cite respect for patient privacy and confidentiality among the job qualifications. Third, during the annual employee evaluation process, one standard by which the employee should be evaluated is his or her demonstrated respect for patient privacy and confidentiality. Fourth, on an annual basis, all employees who have access to patient information and/or those who deliver patient care services should be asked to sign a confidentiality agreement, just as many employees are asked to sign a conflict of interest statement. Fifth, organizational policies should guarantee that technology measures are monitored; policy statements should indicate that the system is monitored and that those who violate patient privacy and confidentiality are subject to dismissal. Departmental policies should indicate how use of the system will be monitored in the department and specify how violations will be handled. Finally, organizational policy should state that the patient has access to his or her record (see **Sidebar**, "Developing a Culture of Patient Privacy"). □

FSHOV-C ETHICAL DIRECTIVES

The FSHOV-C "Ethical Directives" state:

We will respect the personal privacy of all patients and residents and protect the confidentiality of their information.

The "Standards of Conduct" within the directives state:

All employees shall be prudent in the use of information acquired in the course of their duties. They shall not use confidential information for any personal gain nor in any manner which would be contrary to law or detrimental to the welfare of (system's name).

All employees, in the practice of their profession and responsibilities, shall be ever mindful of their obligation to maintain the high standards of competence, morality, and dignity.

Several organizations have produced documents helpful in formulating policies. These include the American Health Information Management Association, Chicago; the Computer-Based Patient Record Institute, Schaumburg, IL; the Joint Commission on the Accreditation of Healthcare Organizations, Chicago; the American Society for Testing and Materials, West Coshohocken, PA; and the Community Medical Network Society, Atlanta. For more information, contact Ida Critelli Schick at 513-745-3716.

NOTES

1. Molly Donaldson and Kathleen Lohr, eds., *Health Data in the Information Age*, National Academy Press, Washington, DC, 1994.
2. Louis Harris and Alan Westin, *Health Information Privacy Survey 1993*, Louis Harris and Associates, New York City, 1993.
3. Ellen Alderman and Caroline Kennedy, *The Right to Privacy*, Alfred A. Knopf, New York City, 1995, p. xiii.
4. Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review*, vol. 14, no. 5, 1890, pp. 205, 208.
5. Tom L. Beauchamp and James F. Childress, *Principles of Biomedical Ethics*, 4th ed., Oxford University Press, New York City, 1994.
6. Charles Fried, *An Anatomy of Values: Problems of Personal and Social Choice*, Harvard University Press, Cambridge, MA, 1970, chapter IX.
7. Jeffrey Reiman, "Privacy, Intimacy, and Personhood," *Philosophy and Public Affairs*, vol. 6, 1976, pp. 26-44.
8. Mark Siegler, "Confidentiality in Medicine—A Decrepit Concept," *New England Journal of Medicine*, vol. 307, no. 24, 1982, pp. 518-521.
9. Lawrence Gostin, "Health Information Privacy," *Cornell Law Review*, vol. 80, no. 101, 1995, pp. 101-184.
10. "Blue Cross and Blue Shield of Massachusetts First to Offer Internet-Based Health Care Solutions: First Health Services Company Nationwide to Implement Healtheon's On-Line Access to Health Plan and Health Care Information," in *Med NewScan*, taken from *Business Wire*, accession no. b062510450, 1996.
11. "Records and Data Are Moving On-Line; HIMS Should Stake Out Their Role Now," in *Med NewScan*, taken from American Health Consultants, accession no. b0328001, 1996.
12. Polly Schneider, "Emerging Technologies from Fascination to Application," *Health Informatics*, January 1997, pp. 43-44.