Feasibility of Ensuring Confidentiality and Security of Computer-Based Patient Records

Council on Scientific Affairs, American Medical Association

Legal and ethical precepts that apply to paper-based medical records, including requirements that patient records be kept confidential, accurate and legible, secure, and free from unauthorized access, should also apply to computer-based patient records. Sources of these precepts include federal regulations, state medical practice acts, licensing statutes and the regulations that implement them, accreditation standards, and professional codes of ethics. While the legal and ethical principles may not change, the risks to confidentiality and security of patient records appear to differ between paper- and computer-based records. Breaches of system security, the potential for faulty performance that may result in inaccessibility or loss of records, the increased technical ability to collect, store, and retrieve large quantities of data, and the ability to access records from multiple and (sometimes) remote locations are among the risk factors unique to computer-based record systems. Managing these risks will require a combination of reliable technological measures, appropriate institutional policies and governmental regulations, and adequate penalties to serve as a dependable deterrent against the infringement of these precepts.

(Arch Fam Med. 1993;2:556-560)

Full computerization of patient records will change dramatically the manner in which records are created and used in patient care. However, the fundamental legal and ethical precepts related to medical records need not, and in fact should not, be altered in order to accommodate computerization. Among these fundamental precepts are the requirements that patient records be kept confidential, accurate and legible, secure, and free from unauthorized access.

Fully computerized patient records are records that are created and modified on a computer, signed or authenticated by computer, stored on computer media, and retrieved by computer.

From the Group on Science, Technology, and Public Health, American Medical Association, Chicago, Ill.

LEGAL AND ETHICAL CONFIDENTIALITY REQUIREMENTS

Patient records must be computerized in such a way as to preserve their confidentiality. The legal requirement that patient records be kept confidential arises from a variety of sources. From the perspective of physicians, the most important sources of the confidentiality requirement are state medical practice acts, physician licensing statutes, and the regulations implementing these statutes. A physician may be subject to professional discipline for failing to preserve in confidence patient records or confidential patient information. When a physician, as a member of the medical staff of a hospital, creates or obtains access to patient records, the physician becomes subject to the confidentiality requirements

found in state hospital licensing statutes and regulations and in the accreditation standards of the Joint Commission on Accreditation of Healthcare Organizations.[1]

Medicare regulations applicable to physicians, hospitals, and nursing homes require confidentiality of patient records.[2] Various federal and state laws impose additional confidentiality requirements with respect to records of patients with a history of alcohol and drug abuse, mental health and developmental disability records, and records containing results of testing for the human immunodeficiency virus.[3] The Federal Privacy Act and similar statutes in many states protect the confidentiality of patient records in the hands of governmental entities.[4] At least one state has an act protecting the confidentiality of health care information in general.[5]

Ethical standards articulated in the Hippocratic Oath, the American Medical Association's Principles of Medical Ethics, and the Opinions of the American Medical Association's Council on Ethical and Judicial Affairs require that patient records be kept confidential. Such ethical standards take on the force of law when they are expressly or by implication incorporated into physician licensure laws, or when they are used by courts to define the appropriate standard of professional conduct for physicians.

Risks to . . . confidentiality . . . can generally be reasonably, but not totally, controlled

In addition to the confidentiality requirements imposed by statute and regulation, courts generally have held that a trust or fiduciary relationship exists between a physician and a patient, and that this special trust relationship imposes on the physician the obligation to hold in confidence personal information concerning the patient, including information in the patient's record.[6] A physician making unauthorized disclosure of such information may be liable to the patient for breach of trust or confidence. In addition, many courts have found that unnecessary or unauthorized disclosure of confidential patient information constitutes an invasion of privacy, for which the disclosing party may be held liable.

Of course, the requirement that medical records be kept confidential is not absolute but is subject to many exceptions. The most important is that records can be disclosed with the consent of the patient or the patient's authorized representative. Another important set of exceptions permits the reporting to public health authorities of child abuse, acquired immunodeficiency syndrome, controlled substance prescriptions and abuse, occupational diseases, abortions and resulting complications, birth defects, cancer, certain communicable diseases, and knife and gunshot wounds (when such reporting is mandated or permitted by law). Disclosure may also be required to government reimbursement programs, state licensing bodies, and peer review organizations. A court may require disclosure of patient records pursuant to a valid subpoena or court order. Disclosure made pursuant to any exception to the general requirement of confidentiality may generally be made only under controlled circumstances and often must be restricted in accordance with the purpose of the disclosure.

THE LEGAL NECESSITY OF COMPUTER SECURITY

Breaches of security in computer-based patient record systems may not only result in breaches of confidentiality, but may also create other adverse legal consequences. If a computerized patient record system lacks reasonable security either in design or in operation, a court may find that records stored on the system are not sufficiently reliable to be introduced as evidence in court. Such a finding by a court could devastate a physician's defense to a malpractice claim or could harm a patient's case in which the patient's health status is at issue. Introduction of computer viruses and other breaches of system security can compromise the accuracy of patient records, creating the possibility of harm to the patient, with attendant liability exposure, and generating possible reimbursement and peer review problems. Security breaches also create the possibility that the system will crash or slow down—whether through deliberate sabotage or inadvertence—or that users will be denied access to the system. Patients may be harmed by the consequent inaccessibility of their records.

While computerization poses unique risks to record confidentiality and security, in general these risks can be reasonably, but not totally, controlled. No security system will withstand an individual who is determined to break into the system and who has the expertise to do so.

The standard of computer security legally required for computerized patient record systems is not always clear.

Nevertheless, computer security in patient record systems must be reasonable at a minimum. As computer security techniques and technology improve in the future, the security of computerized patient record systems will need to be enhanced periodically in order to meet legal requirements.

KEEPING COMPUTERIZED RECORDS CONFIDENTIAL AND SECURE

The necessity of keeping patient records confidential and free from unauthorized access exists regardless of whether the records are kept on paper, preserved on microfilm, or stored in computer-retrievable form. However, computerization poses special challenges to the confidentiality and security of patient records. These challenges arise from several characteristics of computers and computerized patient record systems, including characteristics of computerized records themselves and of the computer and communications technology used in connection with the records. In addition, computerization of records often introduces new players into medical records processing whose involvement creates additional confidentiality and security concerns.

The computer has the capacity to collect, store, and access large quantities of information. The health information available from such systems is becoming increasingly sophisticated and, in the future, can be expected to include highly sophisticated information such as genetic information. The quantity and sophistication of the health information that may exist in computer-based records, along with the increasing nonhealth uses to which information concerning a person's health status are being put, may make computerized patient records especially tempting targets. Because the computer can store and copy records en masse, a single breach of a record system's security can result in disclosure of a large number of records and resulting liability for such disclosure.

Creation of computer-based patient records in hospitals and other institutional settings and even some physicians' offices requires that multiple people input information into the record. Full computerization requires computerization of each area in a hospital or medical office where portions of a record are generated, which means that a record can be accessed from multiple locations. Similarly, use of computer-based records in the treatment of patients may result in access to a single record from multiple locations. Communications technology, which permits networking of computers, creates the possibility that access to a record may also be gained from remote (off-site) locations. By contrast, a paper record, once assembled, can generally be accessed only from one central location.

Security for a patient record system should be designed to balance the need for confidentiality against the need for quick and easy access to patient records by those involved in providing patient care. For users of a patient record system, there should be a security system that, as far as practicable, permits only authorized users to access medical records. This may be accomplished through use of passwords or, better yet, through a system that uses passwords and key cards similar to the cards used in automatic teller machines. The best access control would be provided by a system that identifies users biometrically, but the cost of such security technology is generally prohibitive.

A hospital or medical practice should have policies against disclosing or sharing passwords, access codes, key cards, and the like. This policy should be strictly enforced. When an employee or physician leaves a hospital or practice, the password and access codes for that person should be deactivated immediately. Passwords and codes of more characters are harder to guess than ones containing fewer characters. Passwords should be changed frequently, and a user should be permitted to log on to only one user device (eg, terminal, work station) at a time.

It is generally advisable to limit the access of each user to only the portions of the patient record related to the user's functions in the hospital or medical practice. The computer should restrict access to particularly sensitive records or parts of records to those who have a need for such access. Examples of such records include results of tests for the human immunodeficiency virus antibody, records of patients with a history of drug and alcohol abuse, psychiatric and developmental disability records, records containing information about abortions, and records of celebrity patients.

If possible, the system should be programmed so that a person attempting to retrieve records beyond his or her clearance or with the repeated use of an improper access code will be locked out of the system until readmitted by someone who knows how to unlock the system. The system can also be programmed to sound an alarm at any workstation or the system operator's console when such a violation occurs.

The system should track access to records by each user as a disincentive to unauthorized viewing of records. Permitting curious employees to browse through medical records increases the possibility that confidentiality will be breached.

Preventing unauthorized access to patient records that can be accessed from multiple and even remote locations is much more difficult than preventing unauthorized access to records from one centralized location. Dial-up access makes it possible for outsiders to try repeatedly to gain access without being visible to the provider or practitioners using the system. Some possible responses to this challenge include having the computer system call back users requesting remote dial-in access and requiring remote users to have physical "keys" such as encoded disks for dial-in access. However, the protection offered by dialing back dial-in users can be illusory because of the call-forwarding feature that many telephones have.

Wide-area networking creates unique confidentiality problems, because patient information may be transmitted through such networks over public channels of com-

munication, including telephone lines, radio waves, and microwaves. As communication protocols become more standardized, the potential for unauthorized tapping of these communications channels will increase. One possible solution to confidentiality problems created by wide-area networking is encryption of patient information communicated over such networks.

The computer's capacity for mass storage and copying presents another challenge to patient record confidentiality because thousands of records can be copied at a time. One possible safeguard against such massive breaches of confidentiality is to restrict use of software functions that permit copying of more than one record at a time.

Viruses and other forms of computer sabotage can result in alteration or destruction of data or the creation of false data on a patient record system, or can cause the system to slow down, crash, or otherwise make patient records inaccessible. Either inside or outside users can introduce viruses into a patient record system or carry out other computer sabotage. The biggest sabotage risk from inside users comes from disgruntled employees. In fact, inside users often pose the biggest threat to system security.

The risk of sabotage by outside users can be substantially reduced by eliminating all networking and sharing of electronic data with outside computers and by not using any disk or other storage medium from an outside source. However, such isolation of a patient record system is usually impractical and may preclude such potentially beneficial developments as computer linkages among practitioners and providers at different levels of the health care system, and may otherwise limit beneficial exchanges of information. Antivirus software is available to assist in blocking and detecting computer viruses and other forms of sabotage. Physicians should not ignore the possibility that software provided by vendors may contain keylocks or other mechanisms permitting the vendor to disable or lock the system in the event that a dispute with the vendor results in withholding of payment.

Whether physicians use outside computer services or acquire their own patient record systems, third-party vendors and consultants will usually be involved in some way in developing, installing, operating, maintaining, and supporting the patient record system. These third parties may have access to the patient record system where the computer is located or from remote locations. When an outside computer service is used to process patient records, the third party will have possession of the patient records.

These third parties have neither the legal nor the ethical obligations that health care providers and practitioners have with regard to the confidentiality of patient records. If a third-party vendor or consultant improperly discloses patient record information, the provider or practitioner permitting third-party access to the patient records will likely be held responsible for the disclosure unless the provider or practitioner has taken all reasonable precautions to prevent such disclosure. The patient whose information has been disclosed will almost always sue the provider or practitioner maintaining the record rather than the party who made the improper disclosure. In many cases, the contract between the third party and the provider or practitioner will disclaim the third party's liability for all damages of the type sustained by the provider or practitioner in the event of the third party's improper disclosure of confidential patient information.

Prudent physicians and medical groups will enter into contracts with all third parties having access to their patient records providing that the third party will (1) keep the records in strict confidence; (2) use the records only for the purpose of providing services under the contract; (3) disclose the records only to those of the third party's employees *(a)* needing access to the records in order to provide services under the contract and *(b)* having signed a confidentiality agreement protecting the records (and *not* to make disclosure to contractors or other third parties); (4) return the records in usable form on request or at the end of the contract; and (5) indemnify the physician or medical group for all breaches of these obligations. If it is not possible to obtain indemnification, the contract should, at least, place no limit on the third party's liability for breaches of its obligations.

Some outside computer services may wish to obtain access to patient records for reasons that conflict with the physician's duty to keep patient records confidential. For example, an outside computer service may wish to use patient records to create information products such as databases. The computer service will seek to own and control such information products and will want to be able to distribute them as it sees fit, which will not be in keeping with the physician's confidentiality obligation unless the information product could not be used directly or indirectly to identify individual patients. All contracts with an outside computer service should address whether the computer service will be permitted to use patient record information for its information products and what confidentiality precautions the computer service will take *if* the contract permits patient record information to be used for the computer services' information products.

inside users often pose the biggest threat to system security

CONCLUSIONS

Computerization of patient records raises numerous computer security and record confidentiality issues. Acceptable resolution of these issues generally combines technological and practical measures. Factors such as the costs of security systems and the necessity that records be easily accessible by health professionals will sometimes limit

or conflict with security measures that would otherwise be desirable. Any legal standards adopted with respect to computer-based patient records should address confidentiality and computer security issues and should balance the need to protect patient confidentiality and record security and integrity with the practical constraints on achieving perfect computer security or confidentiality of computer-based records. Physicians and other health care providers should be expected to use reasonable, but not fail-safe, security mechanisms for computer-based patient records.

Accepted for publication March 9, 1993.

Presented at the Annual 1992 House of Delegates Meeting as an informational report of the Council on Scientific Affairs, Chicago, Ill, June 1992.

This report is not intended to be construed or to serve as a standard of medical care. Standards of medical care are determined on the basis of all the facts and circumstances involved in an individual case and are subject to change as scientific knowledge and technology advance and patterns of practice evolve. This report reflects the scientific literature as of October 1991.

Reprint requests to the Group on Science, Technology and Public Health, American Medical Association, 515 N State St, Chicago, IL 60610 (Jerod M. Loeb, PhD).

REFERENCES

1. *See, eg,* 28 Pa §115.27 (1991) (hospitals); 49 Pa §16.61 (1992) (medical doctors). *See also,* Joint Commission on Accreditation of Healthcare Organizations, *Accreditation Manual for Hospitals* MR 3, MS 1.1.3 and MS 2.1.1 (1992).
2. 42 CFR §482.24(b)(3) (1991) (hospitals); 42 CFR §483 (long-term care facilities) (1991).
3. *See, eg,* 42 USC §§290dd-3 and 290ee-3 (1992); 42 CFR §2.1 *et seq* (1991); 740 ICLS 110/1 *et seq.* (Smith-Hurd 1992); Calif Health & Safety Code §§199.20-199.24 (1992); 410 ICLS 305/4 (1992); NY CLS Pub Health §2782 (1992).
4. 5 USC §552a (1992); with respect to state privacy statutes *see, eg,* Minn Stat Ann §13.02 (1992); Ohio Rev Code Ann 1347.01 *et seq* (Baldwin 1992).
5. Mont Code Ann §§50-16-501 to 50-16-611 (1991) (Uniform Health Care Information Act); Rev Code of Wash §70.02.005 *et seq* (1991) (Uniform Health Care Information Act); Calif Civil Code §§56-56.37 (1992).
6. *See, eg, Doe v Borough of Barrington,* 729 F Supp 376 (D NJ 1990).