hp96050.htm

LAW

Legal Implications Of Computerized Medical Records

BY CHARLES S. GILHAM, JD, LLM

Healthcare providers have come to value the benefits of computerized technology in records administration and medical record keeping. And this technology is likely to become even more vital as providers, organized in integrated delivery networks, rely on computerized systems to help them serve their patients within a continuum of care.

Mr. Gilham is senior attorney, Catholic Health Association, St. Louis.

Legal Liabilities of New Systems

Traditional legal theories of provider liability do not change simply because a medical record is in a computer instead of on paper. The standard requirements of patient records—that they be accurate, legible, and secure from unauthorized access—are as relevant to computer-based medical records systems as they are to a standard paper-based system.[1]

In fact, the potential legal liability of a computerized system may actually be much greater than that of a paper-based system, precisely because of the advantages the newer system affords. For example, if a paper medical record were to be altered or stolen by an unscrupulous employee, the only person hurt would be the one whose records were used without permission. But if the same employee were to alter or disseminate information on a computerized disk containing hundreds of medical records, the potential risks of exposure would obviously be compounded. The ease with which one can work with computerized records makes them more vulnerable to sabotage.

A Patchwork of Law

Both ethically and legally, a healthcare provider is required to preserve the confidentiality of computerized patient records. The primary sources of this legal requirement are state statutes, regulations, and the common law. Unfortunately, this patchwork of state law leads to inconsistent enforcement, as one state may have rigorous standards for the protection of patient information contained in computerized medical records whereas another may be lax. This uneven treatment has led organizations such as the American Hospital Association to ask for federal legislation that would override the various state laws and ensure uniform treatment of the confidentiality of each person's medical records.[2]

Last October, Sen. Robert Bennett, R-UT, introduced legislation that would create federal standards for protecting the privacy of medical records and healthcare information. Senate Bill 1360, the Medical Records Confidentiality Act of 1995, contains provisions regarding the creation, storage, and dissemination of medical records, both on paper and in computers. Section 213 of the bill deals specifically with electronic disclosure, requiring the U.S. Department of Health and Human Services to promulgate "standards for disclosing, authorizing and authenticating protected health information in electronic form."[3] Unfortunately, Congress is not expected to approve the measure during its current session. Passage of the Bennett bill would be a big step toward the setting of national standards.

Despite the absence of a controlling federal statute, there are, in addition to state statutes, federal regulations that impose strict confidentiality requirements on specific types of medical information. The medical records of patients treated for alcohol or drug abuse are governed by a regulation that strictly controls when and to whom those records can be disseminated and requires the use of a signed patient release form.[4] Medicare regulations also require providers to protect the confidentiality of the medical records of Medicare patients.[5]

Safeguarding the New Systems

Most professional organizations understand the ethical and practical—as well as legal—importance of preserving the confidentiality of computer-based patient records. For example, in 1992 the American Health Information Management Association (AHIMA) adopted the following position statement: "AHIMA believes that confidentiality does not have to be compromised with the advent of the computer-based patient record.

Safeguards for data security, privacy and confidentiality must be in place to protect against unauthorized access to patient health information."[6]

Similarly, the accreditation standards of the Joint Commission on the Accreditation of Healthcare Organizations require that medical records be "confidential, secure, current, authenticated, legible and complete."[7] The importance of preserving the security of automated records has been noted by the numerous committees, both governmental and nongovernmental, at work on the issue. These include the Congressional Office of Technology Assessment, the Institute of Medicine, the Physician Payment Review Commission, and the Department of Health and Human Services.

But a medical provider who installs a computerized medical records system must also deal with legal issues other than confidentiality. For computerized records to be admissible as evidence in court, the computer information system containing them must have safeguards that would allow a court to reasonably conclude that the records are reliable.[8] A plaintiff could successfully attack the accuracy of a provider's medical records if the system's safeguards were found to be lacking, either in design or in actual practice.

Keeping Viruses Out

Another potential problem with a computer-based medical records system is the threat of a computer virus. A virus can wipe out a healthcare provider's entire data base, especially if the data base is attached to an online system. To protect itself against such a potentially disastrous occurrence, the system should have antivirus capabilities. In addition, employees who have access to the system should be prohibited from bringing in programs or disks they have obtained from other computers, including their own home computers, since such disks could bear a virus.

Finally, because no set of safeguards can be guaranteed to keep viruses out of a computer system, providers should install separate backup systems. The backup would require additional investments of capital and time, but it could prove invaluable if there were to be a failure in the primary system.

Passwords Aid Security

However, the most serious threat to a health information system comes, not from an outside virus, but from the authorized users. Consequently, providers must design user security procedures that will minimize intentional breaches of security.

The most serious threat to a health information system comes, not from an outside virus, but from the authorized users.

At the least, such procedures will require the user to type in an individual password before he or she is admitted to it; this enables the provider to track use of the system. Authorized users should be allowed to access only those portions of the system they need to carry out their duties. Individual identification passwords can be set up on a read-only basis to prevent unauthorized users from changing a file.

As noted, such protective measures cannot make an information system entirely inviolate. But providers who install them will have a better defense against lawsuits alleging negligence because of a breach of information privacy or alteration or destruction of medical records.

A Changing World

Computerization of medical records could generate such efficiencies that the technology itself will set a new legal standard for providing access to medical records. Should this occur, a healthcare facility's failure to provide computerized access could, in the foreseeable future, expose that facility to legal liability for adverse medical results that might have been avoided through the use of the technology.[9] □

NOTES

1. Wendy E. Parmet, *Public Health Protection and the Privacy of Medical Records,* 16 Harvard C.R.-C.L. L. Rev. 265 (1981).
2. Robin E. Margolis, "Computerizing Medical Records: Is Uniform Federal Law Needed to Guard Patients' Privacy?" *HealthSpan,* January 1994, p. 15.
3. S. 1360, 104th Cong., 1st Sess., Section 213 (1995).
4. 42 C.F.R., Sections 2.1-2.5 (1991).
5. 42 C.F.R., Sections 482.24(b)(3) (1991).
6. American Health Information Management Association, Position Statement, *Confidentiality of the Computer-based Patient Record,* 1992.
7. Joint Commission on the Accreditation of Healthcare Organizations, *Accreditation Manual for Hospitals,* 1992.
8. Linda J. Gobis, "Protecting the Confidentiality of Computerized Medical Records—Preparing for Litigation," *HealthSpan,* September 1994, p. 11.
9. James R. Kalyvas, "Balancing Need for Access and Confidentiality: Five Tips for Building a Secure Integrated Information System," *Inside Health Law,* February 1996, pp. 10-12.