



## policypoints

**Strict—or stricter—confidentiality** Regardless of which proposal for governing confidentiality of medical records becomes law, the new year will bring changes in medical records management and the doctor-patient relationship.

BY JEFF ATKINSON



New layers of laws and regulations regarding the confidentiality of medical

records are in the forecast for the coming months. The technical details may seem dull, but the underlying issues are of fundamental importance. These laws will affect everything from how medical offices and their computer systems are set up to patients' confidence in the ability of their physicians to protect their privacy.

"We [physicians] are the guardians of medical records. The whole foundation of the doctor-patient relationship could crumble because of impingements [of the patient's

right to confidentiality]," said Dr. Margo Goldman, a Boston-area psychiatrist, who is the director of policy development for the National Coalition for Patient Rights in Lexington, Massachusetts.

Dr. Goldman is concerned that the physician's ability to be a guardian of records and to protect the rights of patients may be eroded, depending on which confidentiality laws and regulations are enacted.

Confidentiality issues have recently come into the spotlight thanks to the federal Health Insurance Portability

and Accountability Act of 1996. That law, often referred to as HIPAA, provides that if Congress did not enact comprehensive health privacy legislation by August 21, 1999, the Secretary of Health and Human Services must issue regulations on confidentiality by February 21, 2000. The August 21 deadline came and went without Congress enacting any of the competing confidentiality bills.

Even if the Department of Health and Human Services issues regulations in the coming months, Congress still has the

ultimate power to enact laws on confidentiality. If Democrats and Republicans manage to come together to pass confidentiality legislation (and if President Clinton signs the law), the new law can supersede administrative regulations issued by the Department. But until Congress enacts a new law, confidentiality of medical records will be governed by a mix of federal regulations, state laws, and rules issued by private regulatory bodies such as the Joint Commission on Accreditation of Healthcare Organizations.

### Competing bills

Perhaps Congress has not acted because it has too many choices. At least seven different

---

The bills differ regarding the right of individuals to file civil actions for monetary damages and injunctive relief for violation of the confidentiality laws.

---

*Continued*

## POLICY POINTS

*Continued from previous page*

proposals are before Congress. Two of the leading ones are the Medical Information Privacy and Security Act (S. 573), introduced by Senator Patrick Leahy (D. Vt.), which is generally backed by medical associations and patient privacy advocates, and the Medical Information Protection Act (S. 881), introduced by Sen. Robert Bennett (R. Ut.), favored by many insurance companies and employer groups. The seven bills take similar approaches on some issues, such as patients' access to their own records, but differ on others, such as access to records by law enforcement and whether the law will set minimum requirements or a universal standard for confidentiality.

One area in which the bills' authors all seem to agree is the right of patients to access their own records. Generally patients would have a right to inspect and copy their medical records. Exceptions are made, however, if disclosure of the information could reasonably be expected to lead to endangering the life or safety of any individual or if information in the record was obtained from a person who provided the information under a promise of confidentiality.

The American Medical Association supports a right of patients to have access to their medical records, but the AMA would like to see more explicit exception to patients' right of access in order to protect the integrity of clinical research projects.

Like the consumer protection laws regarding credit records, patients would have the right to object to information in a medical record and file a statement presenting the patient's version of the facts. The patient's statement would become part of the medical record unless the health-care provider gives written reasons for refusing to include the patient's statement.

Under all the major bills, information about a patient may be disclosed to next of kin, consistent with sound medical practice, unless the patient objects to

sharing the information. Information also can be released to protect the patient or others from serious, imminent harm.

In addition, the bills allow release of protected health information to public health officials for the purpose of preparing injury and disease reports. The bill backed by privacy advocates would impose more detailed limitations on the use of information which could be used to identify individual patients.

### **Exception for research**

All the main bills allow release of patient information for research purposes. The bills generally require that institutional review boards establish safeguards for use of the information and monitor compliance with confidentiality rules. In addition, the Secretary of Health and Human Services would develop more detailed standards for maintaining patient privacy in research projects.

An important issue when releasing patient information for research purposes is the degree to which the records are "de-identified." It is common practice to delete a patient's name, address, telephone number, and social security number before researchers are given access to patient information. Dr. Goldman of the National Coalition of Patients Rights says, however, that may not be enough to truly protect the patient's identity.

If a patient's records still list the patient's occupation, workplace, date of birth, and zip code, for example, it may be comparatively easy to link that information to a specific individual.

The bills differ in their level of detail for establishing safeguards for health-care information. Some bills require only that providers take reasonable steps to insure confidentiality and to protect against threats to the security of information.

Other bills are more specific, requiring, for example, that information systems maintain audit trails of each access or attempted access "whether authorized or

unauthorized, successful or unsuccessful" and the identity of the person seeking access. By this method, a person who improperly obtains information will be easier to track.

Another proposal would require that information systems be capable of keeping particularly sensitive information in segregated files. For example, at one HMO, the full mental health records of patients were once kept in the patient's central electronic file. If the patient consulted a dermatologist, the dermatologist and his staff would have complete access to the patient's mental health records. Under a new policy at the HMO, mental health records are now in segregated electronic files and access is on a need-to-know basis.

### **Access by law enforcement**

Law enforcement officials' access to health-care records is another area of controversy. Some bills would allow law enforcement officials to access patient records with comparative ease, including through administrative subpoenas and summons issued without oversight by a court.

Advocates for patient privacy would impose much more rigorous requirements for the release of information, such as mandating that a law enforcement agency's request for information be approved by a court or grand jury. For this approval, law officials must present clear and convincing evidence that the information is necessary and that it cannot reasonably be obtained by other means. In addition, the person about whom information is sought would have the opportunity to contest release of the information unless notice of the request could result in destruction of the records.

### **Penalties for violation**

Each of the bills provides criminal and civil penalties for disclosure of information in violation of the act. Comparatively low-level offenses could result in fines in

## POLICY POINTS

*Continued from previous page*

the range of \$500 to \$50,000 and imprisonment for up to one year. If a violation is committed under false pretenses, the penalties escalate (such as to a fine of not more than \$250,000 and imprisonment for not more than five years).

The most severe penalties would be imposed on persons who disclose protected health information for purposes of commercial advantage, personal gain, or malicious harm. Those penalties are in the range of fines of \$500,000 and 10 years of imprisonment.

The bills differ regarding the right of individuals to file civil actions for monetary damages and injunctive relief for violation of the confidentiality laws. The consumer-oriented laws provide for such causes of action; the bills backed by insurance companies and certain employer groups do not.

### **Floor or ceiling**

The most controversial issue in the debate over confidentiality legislation probably is whether a new law will constitute a floor or a ceiling. In other words, would a new law provide minimum requirements for confidentiality (a floor) for which states could then provide more stringent requirements if they wished, or would the federal law create a ceiling, preempting or prohibiting state laws that would impose different requirements?

Privacy advocates generally favor the former approach, giving states freedom to provide extra protections for privacy. Insurance companies and employers generally favor the latter approach in order to avoid more stringent requirements and to be able to work with a single set of rules rather than separate rules for each state and the federal government.

Georgetown University's Institute for Health Care Research and Policy has issued a report, "The State of Health Privacy: An Uneven Terrain," describing privacy laws in all 50 states. That report, along with a substantial amount of other

information about health-care privacy issues, is available on line at <http://www.healthprivacy.org>

Janlori Goldman, the director of the Institute's Health Privacy Project said the report "shows tremendous unevenness, inconsistency, confusion, and lack of coherence across states in their protection of basic privacy principles." The report notes that it is not unusual for states to have as many as 60 different laws governing health-care privacy issues.

States often have different statutes with different standards depending on who is using the information, including physicians, hospitals, HMOs, insurance companies, employers, schools, and state agencies. The manner in which the information is handled, and the right of patients to access it, often varies with the user. In addition, the means by which patients can consent to disclosure and the circumstances in which a patient's consent is not necessary also vary considerably.

Almost all states have special rules for specific conditions and types of medical information, including: AIDS/HIV, tuberculosis, other communicable diseases, mental illness, alcohol use, drug use, and genetic information.

### **Impact on physicians**

Obviously, implementation of confidentiality protections can carry significant burdens for physicians and others who maintain patient records. E. Ratcliffe Anderson, Jr., speaking for the American Medical Association, cautions against "intrusive and unnecessarily onerous regulatory micromanagement." Anderson's report also suggests that new laws need to "maintain flexibility to accommodate differing levels of a health-care facility's size and sophistication, as well as the individual needs of patients who receive medical care there."

Physicians, particularly those responsible for managing their own office or that of a group, will need to monitor new rules for pa-

tient consent and disclosure, as well as new requirements for computer programming capabilities and computer security. Information systems, for example, may need a particular level of sophistication for passwords or key-cards. Systems also probably will need technology that can provide the audit trails to identify who obtained or attempted to obtain information at what time.

Regulations also may specify the types of physical security necessary for an information system. For example, would file cabinets and computer terminals need to be in a locked room or under constant surveillance? (Probably so.) Would a portable computer, such as a Palm Pilot carried by a physician, be considered sufficiently secure to store patient information? (Perhaps not.)

New regulations or laws also may require that personnel handling patient information receive training regarding confidentiality issues. Physicians and others handling patient information may be encouraged to think twice before entering embarrassing or sensitive information in patients' records in order to be sure that the information will significantly advance the patient's medical care.

Health-care confidentiality laws are designed to encourage patients to be open and honest with their health-care providers and to advance the right of patients to keep personal matters private. The laws need to balance the patients' interest in privacy with the need for efficient administration of health care, the advancement of research, and the protection of the community.

No matter what new laws and regulations are issued during the coming months, lawmakers are unlikely to achieve the perfect balance between competing interests. They will need to keep an open mind and be willing to fine tune the system of protecting patients' privacy. ■

*Jeff Atkinson teaches courses in health-care reform and health-care contracts at DePaul University College of Law in Chicago, where he graduated summa cum laude. He also writes on legal, medical, and ethical issues.*