

Los Angeles Times
Wednesday, April 09, 2008

THE NATION
Effectiveness of medical privacy law is questioned

Home Edition, Main News, Page A-10
National Desk
25 inches; 994 words

By Ricardo Alonso-Zaldivar, Times Staff Writer

WASHINGTON -- When Congress passed a federal medical privacy law more than a decade ago, it was hailed as a new level of protection for patients nationwide. But even though the government has received about 34,000 complaints of privacy violations since it officially began enforcing the law five years ago, only a handful of defendants have been criminally prosecuted.

The half a dozen or so cases mainly involved clerical workers who pilfered patient information, using it to open credit card accounts or selling it to crooks who tried to bilk Medicare and the Internal Revenue Service.

Moreover, although the federal Health and Human Services Department has the authority to levy civil fines on medical service providers for privacy violations, it has yet to do so.

The recent revelation of snooping by UCLA Medical Center employees into the files of Britney Spears, Farrah Fawcett, California first lady Maria Shriver and dozens of other patients, however, may force a second look at the federal law, widely known as HIPAA, the Health Insurance Portability and Accountability Act of 1996.

Critics say the government's approach -- which focuses on getting providers to correct violations -- may be too lenient, particularly at a time when medical records are increasingly being shifted from file folders to computers. In addition, a Justice Department legal opinion has stated that the law applies primarily to organizations -- hospitals, health insurance plans and doctors' offices -- and only secondarily to individuals such as the low-level clerks most often implicated in information theft.

"If you are punishing the [organization] but not the person who actually did the dirty deed, then we are missing the boat," said Doreen Z. McQuarrie, a Houston lawyer who specializes in healthcare issues and has studied the federal law.

The law was supposed to have had its greatest impact behind the scenes, ushering in a new era of sensitivity to patient privacy in the healthcare industry. But skeptics say that has not been the case.

"What the rules were supposed to do was regulate one of the most common conversations we have: 'How are you?' " said Dennis Melamed, editor of the Health Information Privacy/Security Alert, which tracks the law and its enforcement. "They did it with an incomplete set of instructions, and when you are talking about an industry as huge as healthcare, that gets to be pretty difficult."

Some privacy advocates say the law should be changed to give patients and their families explicit authority to specify who can -- and cannot -- see their medical records, although others in the industry argue that such stipulations would be very difficult to enforce.

Federal officials say they believe that implementation of the law strikes a balance between education and enforcement. Privacy violations are mainly investigated by the Health and Human Services Office for Civil Rights, and the office is required to try to resolve the problem before imposing fines or penalties.

"Where we have found noncompliance, we have been able to get systemic change that benefits all individuals," said Robinsue Frohboese, principal deputy director of the office. Health insurance plans and medical providers have had to retrain staff, make changes in computer systems and take other protective measures.

Enforcement of the law began almost five years ago, after a period of education and preparation. Of the 34,000 or so complaints received since then, only about 9,000 have actually led to investigations. Many of the others involved incidents that took place before the government started enforcing the law, Frohboese said. Of the 9,000 complaints her agency investigated, about 6,000 resulted in corrective measures; the remainder were dismissed.

In the five years of enforcement, the Health and Human Services Office for Civil Rights referred 426 complaints to the Justice Department for possible prosecution, Frohboese said. At first blush, the law seems rigorous, with criminal penalties of as much as \$250,000 and 10 years in prison.

But federal prosecutors are not required to act on such complaints, and it's unclear whether any of the referrals prompted the few prosecutions that have taken place. Some of the cases appear to have arisen from fraud investigations that agents were already pursuing.

The first conviction for a HIPAA privacy violation came in 2004, in an identity fraud case involving an employee of the Seattle Cancer Care Alliance. Richard W. Gibson admitted that he had used a cancer patient's name, birth date and Social Security number to get four credit cards in the patient's name. He racked up more than \$9,000 in debt buying video games, jewelry, groceries, gasoline and other personal items.

Frohboese said she could not comment on whether the agency would investigate UCLA Medical Center.

California has its own medical privacy law. Under the 1981 Confidentiality of Medical Information Act, any "person or entity" that "obtains, discloses or uses" patient information without authorization faces civil fines of \$2,500 to \$250,000.

But no one seems to know how often or even whether such fines have been levied.

The law leaves jurisdiction to the courts, not to state health officials. City attorneys, county district attorneys and the state attorney general can bring lawsuits on behalf of patients -- if they or the patients know about the breach.

The state Department of Public Health said last week that it had opened an investigation of UCLA Medical Center under a separate state law governing the licensing and certification of hospitals and other healthcare facilities.

The steps it can take under this law are limited. If state investigators find deficiencies, the institution under investigation must create a plan of correction. The state reviews the plan, then revisits the hospital to make sure the problems have been fixed.

"This doesn't mean that the state doesn't have some tools beyond the Department of Public Health," said Kim Belshe, secretary of the state's Health and Human Services Agency, on Tuesday. "My understanding is that we could refer the case to the attorney general to enforce the [Confidentiality of Medical Information Act], or to the local district attorney or the city attorney. We're looking at all three."

--

ricardo.alonso-zaldivar @latimes.com

Times staff writer Mary Engel contributed to this report.