Medical Privacy Law Nets No Fines
Lax Enforcement Puts Patients' Files At Risk, Critics Say

By Rob Stein
Washington Post Staff Writer
Monday, June 5, 2006; A01

In the three years since Americans gained federal protection for their private medical information, the Bush administration has received thousands of complaints alleging violations but has not imposed a single civil fine and has prosecuted just two criminal cases.

Of the 19,420 grievances lodged so far, the most common allegations have been that personal medical details were wrongly revealed, information was poorly protected, more details were disclosed than necessary, proper authorization was not obtained or patients were frustrated getting their own records.

The government has "closed" more than 73 percent of the cases -- more than 14,000 -- either ruling that there was no violation, or allowing health plans, hospitals, doctors' offices or other entities simply to promise to fix whatever they had done wrong, escaping any penalty.

"Our first approach to dealing with any complaint is to work for voluntary compliance. So far it's worked out pretty well," said Winston Wilkinson, who heads the Department of Health and Human Services' Office of Civil Rights, which is in charge of enforcing the law.

While praised by hospitals, insurance plans and doctors, the approach has drawn strong criticism from privacy advocates and some health industry analysts. They say the administration's decision not to enforce the law more aggressively has not safeguarded sensitive medical records and has made providers and insurers complacent about complying.

"The law was put in place to give people some confidence that when they talk to their doctor or file a claim with their insurance company, that information isn't going to be used against them," said Janlori Goldman, a health-care privacy expert at Columbia University. "They have done almost nothing to enforce the law or make sure people are taking it seriously. I think we're dangerously close to having a law that is essentially meaningless."

The debate has intensified amid a government push to computerize medical records to improve the efficiency and quality of health care. Privacy advocates say large, centralized electronic databases will be especially vulnerable to invasions, making it even more crucial that existing safeguards be enforced.

The highly touted Health Insurance Portability and Accountability Act -- known as HIPAA -- guaranteed for the first time beginning in 2003 that medical information be protected by a uniform national standard instead of a hodgepodge of state laws.

The law gave the job of enforcement to HHS, including the authority to impose fines of $100 for each civil violation, up to a maximum of $25,000. HHS can also refer possible criminal violations to the Justice Department, which could seek penalties of up to $250,000 in fines and 10 years in jail.

Wilkinson would not discuss any specific complaints but said his office has "been able to work out the problems . . . by going in and doing technical assistance and education to resolve the situation. We try to exhaust that before making a finding of a technical violation and moving to the enforcement stage. We've been able to do that."

About 5,000 cases remain open, and some could result in fines, Wilkinson said. "There might be a need to use a penalty. We don't know that at this stage."

His office has referred at least 309 possible criminal violations to the Justice Department. Officials there would not comment on the status of those cases other than to say they would have been sent to offices of U.S. attorneys or the FBI for investigation. Two cases have
resulted in criminal charges: A Seattle man was sentenced to 16 months in prison in 2004 for stealing credit card information from a cancer patient, and a Texas woman was convicted in March of selling an FBI agent's medical records.

Representatives of hospitals, insurance companies, health plans and doctors praised the administration's emphasis on voluntary compliance, saying it is the right tack, especially because the rules are complicated and relatively new.

"It has been an opportunity for hospitals to understand better what their requirements are and what they need to do to come into compliance," said Lawrence Hughes of the American Hospital Association.

"We're more used to the government coming down with a heavy hand where it's unnecessary," said Larry S. Fields, president of the American Academy of Family Physicians. "I applaud HHS for taking this route."

But privacy advocates say the lack of civil fines has sent a clear message that health organizations have little to fear if they violate HIPAA.

"It's not being enforced very vigorously," said William R. Braithwaite of the eHealth Initiative and Foundation, an independent, nonprofit research and advocacy organization based in Washington. "No one is afraid of being fined or getting bad publicity. . . . As long as they respond, they essentially get amnesty."

The approach has made health-care organizations complacent about protecting records, several health-care consultants said. A recent survey by the American Health Information Management Association found that hospitals and other providers are still not fully complying, and that the level of compliance is falling.

"They are saying, 'HHS really isn't doing anything, so why should I worry?' " said Chris Apgar of Apgar & Associates in Portland, Ore., a health-care industry consultant.

Goldman and others also questioned why the government is not conducting more independent audits of compliance in addition to investigating complaints.

"It's like when you're driving a car," said consultant Gary Christoph of Teradata Government Systems of Dayton, Ohio. "If you are speeding down the highway and no one is watching, you're much more likely to speed. The problem with voluntary compliance is, it doesn't seem to be motivating people to comply."

Wilkinson's office has conducted just a "handful" of compliance reviews, an HHS spokesman said, and completed one -- a case involving a radiology center that was dumping old files of patients into an unsecured trash bin. The center agreed to hire a company to dispose of records and no fine was levied, the spokesman said.

Wilkinson said the size of his staff limits its ability to do much more than respond to complaints.

"We've had challenges with our resources investigating complaints," he acknowledged, saying they are complaint-driven. Wilkinson added, "We've been successful with voluntary compliance, so there has not been a need to go out and look."

But other government regulators take a different approach, privacy advocates say.

"The Securities and Exchange Commission, the Federal Trade Commission -- they find significant and high-profile cases and send a message to industry about what is permitted and what isn't," said Peter Swire, an Ohio State University law professor who helped write the HIPAA regulations during the Clinton administration.

Goldman and other privacy advocates point to numerous reports of health information being made public without patients' consent -- the recent theft of millions of veterans' records that included some medical information, a California health plan that left personal information about patients posted on a public Web site for years, and a Florida hospice that sold software containing personal patient information to other hospices.

In the meantime, Goldman said, surveys continue to show that for fear that their medical information will be used against them, people
avoid seeking treatment when they are sick, pay for care out of pocket, or withhold important details about their health from their doctors.

"The law came about because there was a real problem with people having their privacy violated -- they lost jobs, they were embarrassed, they were stigmatized. People are afraid. The law was put in place so people wouldn't have to choose between their privacy and getting a job or going to the doctor," said Goldman, who also heads the Health Privacy Project, a Washington-based advocacy group. "That's still a huge problem."