# United States medical privacy rules deemed inadequate

Previously published at www.cmaj.ca

Reuters/Jason Reed

United States Secretary of Health and Human Services Kathleen Sebelius (centre) takes part in a meeting with health insurance company executives and related industry officials in the Roosevelt Room of the White House in Washington, DC, in March. With Sebelius are (left to right) Chairman and CEO of Aetna, Ron Williams, Kansas Insurance Commissioner Sandy Praeger, Pennsylvania Insurance Commissioner Joel Ario and West Virginia Insurance Commissioner Jane Cline.

In Tennessee, the theft of 57 computer hard drives at a health insurance call centre exposed personal information on as many as one million people. In Virginia, the hacking of a government prescription database compromised millions of records. In California and beyond, peepers have snooped on the medical particulars of celebrities.

This is already a digitized world, as the health system juggles vast volumes of the most deeply private information. Add to that the acceleration in United States doctors' offices of electronic record-keeping, spurred by hefty aid from a government eager to reap efficiencies in medical care.

Trying to keep all of that information properly corralled is a tall order. And President Barack Obama's administration has backtracked on a major attempt to sort out the thicket of privacy rules supporting that effort.

The Health and Human Services Department published a set of regulations governing how health care providers must respond when medical privacy is breached. The rules, although not final, had the force of law. But now the department is retracting them. "This is a complex issue," the department said by way of understatement.

Privacy advocates and members of Congress had sharply criticized the controls as inadequate. After a period of reflection — and reportedly pressure from the White House — the department appeared to agree.

The regulations specified when doctors, hospitals, insurance companies and other providers must notify patients that there had been a "significant" leak of their personal medical information.

But reasoning that a harm threshold was needed so people would not be continually advised about and worried by inconsequential disclosures, the administration left it to providers to determine if a breach was significant.

Watchdogs asserted that health professionals should not be the judge of whether a breach is significant enough to a patient's livelihood or reputation. "That puts the foxes in charge of the hen coops," says Dr. Deborah C. Peel, founder and chair of the Patient Privacy Rights Foundation, which presses for strict consumer safeguards. "It shows the incredible overbearing influence of industry in the crafting of regulations. The idea that someone else knows when you're harmed better than you do, doesn't make sense."

> "The systems that we have today are not even minimally prepared to keep our information private." — Dr. Deborah C. Peel, chair, Patient Privacy Rights Foundation

Health and Human Services Secretary Kathleen Sebelius hopes to produce new rules this fall. The goal, says her department, is to ensure health information is protected to the extent possible and individuals are "appropriately notified" when incidents occur.

The Privacy Rights Clearinghouse has chronicled more than 300 breaches compromising 14.5 million medical records since 2005 (www.privacyrights.org/data-breach/new),

Among those leaks was one in Denver, Colorado, in which a hard drive was taken that detailed medical care and conditions for more than 100 000 people receiving Medicaid, the federal-state health insurance program for the poor.

In California, a UCLA School of Medicine researcher was sentenced to four months in prison for digging into the medical files of actors Tom Hanks, Drew Barrymore, Leonardo DiCaprio, other public figures and his own coworkers. And in Oceanside, California, hospital employees were caught gabbing about patients on Facebook.

Some breaches happen the old-fashioned way: papers swirling around

a parking lot or thrown away carelessly. Outside Boston, Massachusetts, records of thousands of patients at four hospitals were available for the plucking at a public dump.

Absent stricter standards, some providers opted not to notify patients after investigating breaches, instead telling authorities and the public generally, as was the case with a hospital in South Weymouth, Massachusetts reporting in September on its investigation into the loss of boxes containing back-up computer files with personal, health and financial information for roughly 800 000 people. It concluded there was little or no risk that information on the files could be accessed or misused (www.southshorehospital.org/news/notice/news_statement.htm).

In spurring the conversion to electronic records, the US government set a regimen of conditions for the use of personal information. But Peel is far from convinced all that information will remain reasonably secure. "It doesn't look too good for a rapid-force buildout of the health IT [information technology] system," she says. "The systems that we have today are not even minimally prepared to keep our information private."

Other medical information streams are coming online, too, bearing their own risks. Flowing from the National All Schedules Prescription Electronic Reporting Act, signed by then-President George W. Bush in 2005, 43 states have now passed laws to establish databases to thwart drug users who go from doctor to doctor or across state lines, feeding an addiction or otherwise obtaining meds under false pretenses.

In California alone, doctors, pharmacists and other professionals have been checking patient prescription histories online at four times the rate of the recent past, when they were only available by phone or fax.

But that system has also proved to be another vein for exploiters of private medical information to tap. In April 2009, a thief made off with millions of such records from Virginia's database. — Cal Woodward, Washington, DC

DOI:10.1503/cmaj.109-3680