Medical privacy breaches rising

Privacy concerns influence where and when patients seek care, as well how much personal information they disclose to their caregivers, and it appears people have good reason to be worried. The use of portable electronic devices, many of which lack encryption, is increasing in hospitals and that, among other factors, is leading to more breaches of protected health information.

In the United States, there was a whopping 97% increase in the number of health records breached from 2010 to 2011, according to a new report from Redspin, a US company that assesses information technology security (www.redspin.com/docs/Redspin_PHI_2011_Breach_Report.pdf).

"That's a trend going in the wrong direction," says Daniel Berger, Redspin's president and CEO, who worries that breaches are hurting the entire US health care system. "The adoption and implementation and usage of information technology are foundational elements of transforming the whole system. The problem with security is a threat to that."

The number of patient records accessed in each breach has also increased substantially, from 26 968 (in 2010) to 49 394 (in 2011). Since August 2009, when the US government regulated that any breach affecting more than 500 patients be publicly disclosed, a total of 385 breaches, involving more than 19 million records, have been reported to the Department of Health and Human Services. A large portion of those breaches, 39%, occurred because of a lost, stolen or otherwise compromised portable electronic device — a problem that will likely only get worse as iPads, smartphones and other gadgets become more common in hospitals.

"A lot more of this data is now stored on devices that can walk out of your building every night," says Berger.

Are breaches of protected health information as big a problem in Canada as in the US? Nobody knows, as there is no federal law requiring health care providers to disclose that information — and that's a problem, says Khaled El Emam, Canada Research Chair in electronic health information at the University of Ottawa in Ontario and chief executive officer of Privacy Analytics, an Ottawa-based company that creates software to protect individual privacy with respect to sensitive data.

© 2012 Thinkstock

Increased use of portable electronic devices, such as computer tablets, by physicians and hospitals is contributing to rise of medical privacy breaches.

"All of these breaches are having an impact on patients and on health care providers. As a starting point, it would be really helpful to have data to understand how often it happens," says El Emam.

Anecdotally, however, breaches involving mobile devices also appear to be a problem in Canada, says El Emam, who suggests that health care providers could adopt certain practices to reduce the risk of that occurring. "One is to encrypt all mobile devices and to enforce that," says El Emam. "Another could be not to put any health information onto mobile devices, or to anonymize the data that goes on the devices. A key one, though, would be training the staff. If you do all these things, your risk will be low."

In the US, the government has taken several steps to encourage health care providers to improve the security of their information technology systems. In addition to requiring public disclosure of breaches — an incentive in the form of the proverbial "wall of shame" — the US government will be dropping in on some health care providers to kick the tires of their security practices. The Department of Health and Human Services' Office for Civil Rights will conduct 150 audits by Dec. 31, 2012, to check compliance with privacy requirements listed in the Health Insurance Portability and Accountability Act. Under the act, health organizations are required to have conducted a risk analysis and implemented policies to protect patient privacy. The maximum annual penalty for violating the act is US$1.5 million.

Canada has not yet followed the US down the road of strict enforcement and stiff penalties, and perhaps it doesn't have to, suggests El Emam, but that is impossible to determine without national data on privacy breaches. "For us, the first step is to have the data. Once we look at the data, if the numbers are low, we might not have to do anything."

But patients in Canada appear to be concerned about the privacy of their health information. A recent online survey of 1002 Canadian patients indicated that 43.2% have withheld or would withhold information from their health care provider because of privacy concerns, while 31.3% of Canadian patients have or would postpone care over privacy concerns, and 42.9% would seek care outside their communities for the same reason.

"Any friction in the free flow of information between care providers and patients, such as that caused by privacy concerns, prevents the patient from receiving the best possible care," states the survey, *Canada: How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes*, conducted by FairWarning, a US company that provides privacy auditing solutions for electronic health records (www.fairwarning.com/documents/Canada/2011-CanadaSurvey.pdf).

"We are entering an era where the information the patient provides has more impact than ever before on the nature of the care they receive. There has to be trust between the patient and the care provider," says Kurt Long, FairWarning's CEO. "Health care providers need to begin viewing privacy not only as a legal, ethical and moral obligation, but as a serious part of patient treatment and care." — Roger Collier, *CMAJ*

***CMAJ* 2012. DOI:10.1503/cmaj.109-4116**