US health information breaches up 137%

More than seven million health records in the United States were affected by data breaches in 2013, an increase of 137% over the previous year, according to the annual breach report by Redspin, an information security company based in Carpinteria, California.

Since 2009, there has been a rapid rise in the adoption of electronic health records in the US. There have also been 804 breaches of health information affecting nearly 30 million patient health records reported to the secretary of Health and Human Services, as required by law. Similar information is not available in Canada, which has no federal law requiring that breaches be reported or made public.

"Data breaches can cause significant financial and reputational harm to an organization as well as undermine consumer confidence," states the report. "In health care, that risk is not limited to an individual hospital, provider, or business associate. It is an industry-wide threat to the success of the electronic health record initiative."

The most common causes of breaches are theft or loss of unencrypted laptops and portable devices containing personal health information, states the report. In 2013, the five largest breaches accounted for 85% of all affected health records. One incident involved the improper disposal of microfiche. Another was caused when paper records were sent to the wrong address. The theft of four desktop computers storing more than four million unencrypted records resulted in a class action lawsuit.

With databases of health records growing in size, the potential for larger breaches is only going to increase. There are measures, however, that health care providers can take to make their records more secure.

"Are we going to eliminate breaches completely any time soon? Probably not. But there are definitely better ways to secure the data. We just need to get them adopted more broadly," says Khaled El Emam, Canada research chair in electronic health information and founder of Privacy Analytics, a company based in Ottawa, Ontario, that specializes in data anonymization.

dolgachov/Thinkstock

Theft of laptops and portable devices containing unencrypted patient data remains a major source of breaches of personal health information.

To reduce the risk of a breach, suggests El Emam, holders of personal health information should encrypt all computers and mobile devices, prohibit the transfer of patient data offsite, anonymize data and have continuous training of staff so employees internalize the importance of securing patient information.

Otherwise, breaches will continue, eroding public trust and potentially affecting the sharing of health information that could help drive medical research and improve public health policies.

"Fantastic things can happen by sharing this data," says El Emam. "But there has to be trust that it is being managed responsibly." — Roger Collier, *CMAJ*

***CMAJ* 2014. DOI:10.1503/cmaj.109-4731**

More News online

To read more *CMAJ* news articles, visit cmaj.ca/site/home/news.xhtml