William Pascal

Khaled El Eman

# Public Accountability and Transparency — the Missing Piece of the Privacy Puzzle

By William Pascal, Khaled El Emam, and Maryan McCarrey

*William Pascal, Associate Editor, is the Chief Technology Officer of the Canadian Medical Association in Ottawa, Ontario*

*Khaled El Emam is the Canada Research Chair in Electronic Health Information and CHEO of the Research Institute and University of Ottawa in Ottawa, Ontario*

*Maryan McCarrey is the Assistant Director of IT Policy at the Canadian Medical Association in Ottawa, Ontario*

*If you once forfeit the confidence of your fellow citizens, you can never regain their respect and esteem. It is true that you may fool all of the people some of the time; you can even fool some of the people all of the time; but you can't fool all of the people all of the time.*

***—Abraham Lincoln***

It is well understood that protecting the privacy of patient information is essential to the success of our electronic health record agenda and, from an IT system and solution architecture perspective, the "privacy by design" approach is widely accepted as the industry standard. Privacy protection features, mechanisms and Privacy Impact Assessments (PIAs) are present in most if not all health information "technology" solutions.

But the missing piece of this health information privacy puzzle — and a necessary prerequisite for widespread adoption and acceptance of these systems by the Canadian public and health professionals — is getting "privacy by design" built into the "people" side of the equation. By this we mean making sure that governments are accountable to the public and transparent about how large-scale, interconnected electronic health record (EHR) systems will handle personal health information, and what rights patients can exercise over their personal information in these new electronic record environments.

The bottom line is that we need to build public trust and acceptance if we expect to benefit from patients' willingness to continue to confide personal health information. There will always be threats to data security and privacy — and the larger the database or network, the more at-risk it becomes — but there are three key things we can do to manage these risks and build public confidence: (1) ensure that the privacy features and mechanisms within our IT systems are turned on; (2) ensure that the individuals who use these systems are properly trained and compliant with privacy practices and protocols; and (3) fully and properly engage the public so that they have a voice in these deliberations and so that there is transparency about what they can expect and what options they have.

It is in relation to this last measure that we should heed Abraham Lincoln's comment. We worry that the lack of engagement of the public in this public policy agenda is becoming an Achilles heel. So why do we worry?

## Just how vulnerable are we to privacy and security breaches?

In the United States and Canada, between January 2007 and the end of August 2009, there were at least 115 publicly known privacy breaches involving 2.7 million patient records.[1] These numbers are increasing rapidly, because breaches become easier and more records are affected when the data is in electronic format. Electronic records are generally more complete than paper records and hold more longitudinal health data about the patients; eventually, they will contain almost everything.

Individuals feel violated if there is a breach of privacy of their health information and respond by adopting more privacy-protective behaviors, such as not seeking care; lying to their physicians so as not to reveal embarrassing or sensitive information; seeing multiple doctors so no one will have a complete record; paying out of pocket so that insurers do not have a record of a particular encounter, procedure or prescription; self-treating or self-medicating instead of seeking care; and asking the

doctor not to record certain information or to record different information (something many physicians admit to doing).[2] There is also evidence that such privacy-protective behaviors will be adopted by the most vulnerable people: teens, battered women, people with or at risk of contracting HIV/AIDS, and people with genetic conditions.[3]

Examples of privacy breaches by health care providers' staff include "snooping" into the medical records of famous people or people they know; selling information to others (e.g., providing information about accident victims to lawyers); or accidentally losing information.[4] However, there are also people outside medical offices who are actively trying to access other people's health information. Why would they want health information?

## What factors lie behind these threats?

In general, an individual's identity information is not worth much in the underground market. (For a simple assessment of the value and risk of online identity theft, visit Symantec: http://www.everyclickmatters.com/victim/assessment-tool.html) Accordingly, medical records with such information are only useful and worthwhile to hackers if they are available in large quantities. Intruders would be more interested in databases of records rather than an individual record.

### *Financial value of medical records*

However, some medical records contain financial information (e.g., data used for billing purposes) or other information that is useful for financial fraud, such as date of birth, address, and mother's maiden name. In some cases in the US, the medical record may contain Social Security numbers, which are often used as an unique identifier. All of this information is useful for committing financial crimes.

### *Medical identity theft*

Even if medical records do not contain personal information that is suitable for financial fraud, records with health insurance details can be very valuable. Medical identity theft occurs when someone gets health care insurance under another individual's name. This is most likely to happen in situations where a person has no medical insurance, either because they cannot afford it or because they cannot get it (e.g., illegal immigrants or individuals running from the law). Canadian health insurance numbers are especially useful for illegal immigrants who cannot obtain it legitimately under their own identity.

A Canadian example[5] comes from Alberta where a fraudster was creating new identities, complete with passports and health insurance cards, in the names of Canadian children who had died a few decades prior. The presenter described how uninsured Americans bought these identities and came to Canada to receive expensive medical care for free.

### *Monetizing medical records through extortion*

Medical records are a good source of revenue for those in the extortion business. One example concerns Express Scripts,[6] a pharmacy benefits management company that was hacked by extortionists who threatened to publicize clients' personal information. The company was using production data for software testing, and there was a breach on the testing side of the business (unfortunately, using production data for testing is common). The initial extortion attempt was based on the breach of 75 records. It later was revealed[7] that 700,000 individuals may have been affected by the breach.

In another example,[8] an extortionist demanded $10 million after hacking into a database of prescription records at the Virginia Department of Health Professions. This database contained highly sensitive information that was intended to allow pharmacists and health care professionals to track prescription drug abuse, such as incidents of patients who go "doctor-shopping" to find more than one doctor to prescribe narcotics.

### *Attempts to make health records publicly available*

There are a number of efforts underway to make health information publicly (or at least very widely) available. This is particularly true for research data. The authors of a research paper on protecting privacy published in the Journal of the American Medical Informatics Association,[9] offer an extensive review of the various initiatives to make health information publicly or at least more generally accessible. One supporting argument is that data collected using public funds should be made available to maximize the return from the initial investment, because making data widely available means many more people can analyze it and discover new things from it. To the extent that these efforts are successful, the personal health information of individuals who participate in research initiatives may become much more widely available. If that data is not properly de-identified, there would be a greater likelihood (i.e., risk) of re-identifying an individual's personal information.

### *Custodians and vendors selling medical records*

There is increasing interest by data custodians to package data, de-identify it in some way, and sell it. Here are a few examples:

- Some vendors are providing electronic medical records (EMRs) for free to medical practitioners, but then selling the accumulated patient data to generate revenue. For example, US-based EMR and practice management system vendor Practice Fusion began offering both systems free of charge, with the physicians' costs offset in part by the company's sale of their patients' data (aggregated and de-identified, according to a company spokesman).[10] In Australia, the largest retailer of specialist software for general practitioners recently faced controversy over the sale of anonymized patient information from electronic records to consultants advising the drug industry.[11]
- Some providers have seriously considered, are planning to, or already are selling data about their patients. This is done directly or by creating subsidiary companies responsible for the commercialization of data. For example, Partners Healthcare in Boston,[12] the Joint Commission

on Accreditation for Healthcare Organizations,[13] the Cleveland Clinic,[14] and the Geisinger Health System[15] have considered or are engaging in such initiatives.

The problem is that it is not clear whether this de-identification is sufficiently robust, and whether these organizations have used de-identification best practices. In the examples cited above, the organizations have not been forthcoming with details about how they have de-identified their data, which amplifies patient concerns about how their health information is being used. This lack of transparency is further complicated by the fact that many patients would not know or be informed that their health information is being sold.

## What can we do to offset these threats?

### *Privacy by design*

As these risks materialize in a Canadian context, and as the public becomes aware of them, one would expect to see a negative reaction to the electronic collection, storage, and exchange of personal health information. Resistance to electronic health records will come from individuals and providers unless we start to address those risks in the systems, policies, and procedures involved in deploying EHR systems. In the absence of proactive efforts, we will start to see organized efforts to slow down the adoption of EHRs, which is what has happened in the United Kingdom and to some extent in British Columbia.

To avoid these pitfalls, we must make proactive efforts to incorporate privacy and confidentiality into the initial design of electronic record systems and the way in which individual data is collected, used, and disclosed. Doing so now will be more cost-effective and will maintain whatever goodwill exists toward the adoption of EHRs. There are several things to consider:

- There must be a transparent process for formulating privacy and confidentiality recommendations and guidelines for EHR design and implementation. This would allow stakeholders, including patients and providers, to make their voices heard and have their views incorporated.
- Privacy and confidentiality must apply to primary as well as secondary use of data. Once electronic repositories of health information are created and their data quality improves over time, there will be significant demands for that data for research, policy making, public health, and marketing. The rules of the game need to be defined at the outset so that patients and providers are not surprised at how their data is used in the future.
- Governments need to be more open and transparent, and proactively engage the public in this debate. To date, no government has done a good job of engaging members of the public regarding the EHR agenda, how patient information will be shared, managed and disclosed, or what rights individuals have concerning what happens to their information.

Conspicuously absent in every government's e-health agenda is the proper respect for individuals — their interests, expectations and rights — as primary users of and data "contributors" to large-scale health information systems. As we proceed to link more systems with larger numbers of patient records, the benefits and risks (and especially the strategies to mitigate those risks) need to be clearly articulated to the public.

Instead we are seeing governments taken to task for making patients' rights with respect to their information available only in theory, but not in practice. Privacy controls, such as opt-out provisions or lock-boxes and masking features, must be properly communicated and readily accessible to patients.

To be successful in our transformation into an electronically enabled health care system — which depends on a robust EHR environment — we must not only build privacy into the technology but also ensure that we build it into the "people" side of the equation: into the policies, frameworks, governance and practices that we employ to manage and protect patient health information in this new electronic environment. ●

[1]Electronic Health Information Laboratory (CHEO Research Institute) Data Breach Analyzer. Available at http://www.ehealthinformation.ca/dataloss

[2]Association of American Physicians and Surgeons, New Poll: Doctors Lie To Protect Patient Privacy. Available at http://www.aapsonline.org/press/nrnewpoll.htm Accessed Dec.7, 2009.

[3]Sankar P, Moran S, Merz J, Jones N. Patient perspectives on medical confidentiality: A review of the literature. Journal of General Internal Medicine, 2003; 18:659-669.

[4]Allen, M. Hospital privacy leak could harm patients. Available at http://www.lasvegassun.com/news/2009/nov/20/umc-has-patient-privacy-leak/ Accessed Dec. 7, 2009.

[5]Pendleton J. The growing threat of medical identity theft in Canada. Available at http://www.enhealthinformation.ca/documents/EHIP2008.pdf. Accessed Dec. 5, 2009.

[6]http://www.ehealthinformation.ca/blogs/extortion_plot_threatens.mht

[7]http://www.computerworld.com/s/article/9138723/Express_Scripts_700_000_notified_after_extortion

[8]http://ehip.blogs.com/ehip/2009/05/hacker-threatens-to-expose-health-data-demands-10m.html

[9]El Emam K, Dankar FK. Protecting privacy using k-anonymity. JAMIA. 2008;15(5):627–37. Available at http://www.jamia.org/cgi/content/abstract/15/5/627. Accessed Dec. 5, 2009.

[10]Conn J. Advertising, data sales subsidize EMR products. Available at http://www.modernhealthcare.com/article/20071008/FREE/310080003#. Accessed Dec. 5, 2009

[11]Burton B. Software company defends sale of patients' data to drug companies. Available at http://www.bmj.com/cgi/content/full/331/7509/128-c. Accessed Dec. 5, 2009

[12]Bailey S. Your data for sale? Available at http://www.boston.com/business/healthcare/articles/2006/03/24/your_data_for_sale/ . Accessed Dec. 5, 2009.

[13]Weeks K. Accrediting agency under fire for sale of patient data. Available at http://www.allbusiness.com/health-care/health-care-facilities-hospitals/10579564-1.html . Accessed Dec. 5, 2009.

[14]Dolan PL. Searchable database of patient records to go commercial. Available at http://www.ama-assn.org/amednews/2009/11/30/bisc1130.htm . Accessed Dec. 5, 2009

[15]El Emam K. Is there a secondary use market for health information? Available at http://www.ehealthinformation.ca/knowledgebase/article/AA-00103/6/De-identification-Practices/Is-there-a-secondary-use-market-for-health-information-.html . Accessed Dec. 5, 2009.