The risks of electronic health records

Gordon Atherley

In Canada, governments have a near monopoly on the provision of medically necessary services. As health care costs are a serious concern for governments, they rely on information technology to monitor and control costs. Electronic health records, a form of information technology, are seen by governments as an instrument for better managing health care. But in pushing electronic health records on the public, governments are ignoring the risks associated with this technology.

As with so many forms of technology used in health care to the benefit of many—such as ionizing radiation—electronic health records have risks that must be acknowledged, researched, and confronted. Not acknowledging, not researching, and not confronting them is an instance of what Clemens and his colleagues (2007) have termed government failure.

The risks of electronic health records arise because of the need to accurately identify the individuals to whom the electronic health records relate. Accurate identity data avoids mix-ups such as patients with similar names receiving transfusions of the wrong blood type. And accurate identity data is exactly what hackers and fraudsters seek in identity theft.

Electronic health records give governments the ability to micromanage the delivery of health care. For example, eHealth Ontario, a government agency, seeks to “control and manage diabetes more effectively to reduce associated complications and costs” (eHealth Ontario, 2009).

Armed with this power, governments and their agencies can access the detailed personal and health information of individuals and, thanks to record linking, of their families and caregivers, the back-stops of Canada’s health care system. How is that electronic information being handled? Is it being adequately safeguarded and fairly used?

Electronic information in the hands of government

In his 2008 annual report, the Auditor General of Alberta observed that the government of Alberta manages huge volumes of sensitive and confidential information, including medical records, which are all stored electronically. He found that even though the government has a duty to safeguard this information properly, it is “not doing so,” and that the government’s information technology security is “inadequate” (Auditor General of Alberta, 2008).

The dangers of inadequate security in centralized databases have been demonstrated many times by instances of identity theft from the private sector. For example, the Canadian Bankers Association tracked credit card data from 1983 to 2008 and published the number of credit cards used fraudulently—through identity theft—in Canada for 1983 to 2006. The year-over-year percentage changes in these totals, the grey line in figure 1, demonstrate that centrally stor-

By centralizing the storage of personal data, information technology facilitates fraudsters in the wholesale stealing of identity data for impersonation.

- Counterfeiting, which involves forging paper slips and double swiping;
- Skimming, which involves reading magnetic stripes or recording key strokes; and,
- Shifting focus and locus: for example, moving from credit card fraud to
debit card fraud and switching regions to exploit regional variations in security.

The vulnerability of big computer systems is underscored by two recent events. The first is the credit card fraud of customers of retail giant TJX, whose stores include Winners and Home Sense. The scale of this fraud, which TJX disclosed in January 2007, was vast: at least 45.7 million Canadian, American, and British credit and debit cards were fraudulently used (Nakashima and Mui, 2007, Mar. 30).

A second example came to light on January 13, 2009, when US-based Heartland Payment Systems Inc., a credit and debit card processor, contacted the US Secret Service and Department of Justice about a data breach (United States Attorney’s Office, 2009). This breach resulted in the exposure of personal information associated with over 100 million credit and debit card transactions.

Government systems are not immune. As of May 7, 2009, the FBI was investigating the alleged hacking of a government website, the Virginia Prescription Monitoring Program, which tracks prescription drug abuse and contains 35.5 million prescriptions. In a ransom note, the hacker or group of hackers announced that they had stolen 8.3 million patients’ personal and prescription drug information and demanded $10 million for the safe return of that information (Merrill, 2009, May 6).

The opportunistic nature of the attacks stands out in the spikes in figure 1. Fraudsters will find and exploit a gap in the defences until the gap is plugged. Sooner or later they will find a different gap in the defences and the process will repeat itself. Unless the authorities responsible for defences can confidently claim that all gaps are currently plugged and will continue to be in the future, prudence demands the anticipation of further threats.

By 1999, Canada’s governments, which regulate the financial sector, knew—or should have known—that by centralizing the storage of personal data, information technology facilitates fraudsters in the wholesale stealing of identity data for impersonation, and that health care data would not be immune to the robbery, harm, and prying enabled by information technology.

**Inadequate safeguards harm health**

One challenge currently facing our health care system is crime that targets prescription medications, especially opioids. Derived from the opium poppy or chemically synthesized, opioids include oxycodone, morphine, codeine, and heroin. Used chiefly for pain relief, the adverse effects of opioids include dependence and addiction. For this reason, opioids are subject to strict controls. In a 2006 study, Fischer and his colleagues found that over the prior decade, abuse of prescription opioids had pulled ahead of heroin use in Canada. They also found that while heroin was bought from drug dealers, prescription opioids for illicit use were obtained directly or indirectly from sources in the medical system.

The consequences of this shift to prescription drug abuse have been dire, including, among other harms, death by overdose, home invasion (Vaillancourt, 2009, Apr. 17), and the overuse and mixing of prescription drugs with alcohol by post-secondary students (BC Centre for Social Responsibility, 2008).

Prevention of prescription drug abuse relies on vigilant communication between pharmacists and physicians. Currently, they depend (though perhaps not often enough) on low-tech methods of fax and telephone communication, which maintain personalization and are effective when used. Governments, on the other hand, prefer high-tech, depersonalized methods. BC’s Pharmanet is working on electronic prescribing through its eDrug Project.

**Figure 1: Retail volume and fraudulent credit card use (Visa and MasterCard) in Canada, yearly change (%)**

Net retail volume
- Number of fraudulently used cards

Source: Canadian Bankers Association, 2009; calculations by author.
which will “improve medication management and patient safety” and “provide broader authorized access to comprehensive patient medication history information” (BC Ministry of Health Services, 2008: 1). Meanwhile, eHealth Ontario is planning to implement “online management of prescription medications to minimize preventable adverse drug events” (eHealth Ontario, 2009: 2).

A centralized government prescription and medications management system would provide criminals with opportunities to impersonate not only physicians and patients, but also the medications management system itself. What would happen if criminals gained access to a large electronic database that contained information on what drugs people were taking and in what quantities, and when they last filled their prescriptions?

In Canada, the security threat is real. Information technology systems in the hands of government can be and have been pierced by opportunistic attacks.

Early in 2007, the Public Health Agency of Canada experienced a security attack in the form of a “worm,” a malicious computer program that can run and spread itself. It immobilized 80% of the agency’s computer system for a month and disabled 543 additional workstations in five of Health Canada’s Ottawa-area offices through the department’s data network (Canadian Press, 2008, Mar. 31a, b). A November 2007 post-mortem report on the emergency warned that if the incident had occurred during a public health crisis, loss of life could have resulted. But neither the attack nor the report on it came to public attention until March 2008, when the Canadian Press succeeded with its Access to Information request.

Late in 2008, two federally funded, quasi-non-governmental organizations, the Canadian Institutes of Health Research and the Canadian Institute for Health Information, experienced “phishing” attacks (Greyhead Associates, 2009a) used by hackers for mischief and misappropriation and, if an insider is involved, malfeasance. A phishing attack usually takes the form of an e-mail, sent out by an individual falsely claiming to be from a legitimate organization, which attempts to deceive the recipient into surrendering private information for the purpose of identity theft.

In January 2009, Vancouver Coastal Health warned clinical personnel, among others, of a phishing attack aimed at harvesting their account information and passwords (Greyhead Associates, 2009a). The attack put at risk the identity data of persons in the care, scope, and employ of the networks of primary health care, community care, and acute care, serving some one million people in the Vancouver area.

The Vancouver attack demonstrates that electronic health record systems are not immune to identity theft by fraudsters who are skilled enough to opportunistically outwit the credit card industry.

Canada’s privacy legislation

Health information privacy legislation provides the primary prescription for safeguarding personal health information. But Carman Baggaley, the Strategic Privacy Adviser at the Office of the Privacy Commissioner of Canada, holds that the privacy laws of Canada are inadequate against identity theft (Baggaley, personal communication, 2007) which, according to Jennifer Stoddart, Privacy Commissioner of Canada, “has become a serious and very real threat for Canadians” (Stoddart, personal communication, 2009).

Canada’s privacy legislation suffers from two main weaknesses.

First, the privacy legislation enacted federally and provincially since 2002 has enabled governments to define privacy in ways that support electronic health records. As a result, health information privacy is whatever governments want it to be. If a government wants to grant a department, agency, or quasi-non-governmental organization access to the personal health information of identifiable individuals, all it needs to do is enact an enabling regulation. While this power is not unique to privacy legislation, it nonetheless carries with it important consequences for how secure and private health information is when managed by government.

Second, at the time of writing (May 2009), identity theft was not even a crime in Canada.

The Health Council of Canada (2009: 35) notes that we “have been slow to adopt some developments that might stimulate more evidenced-based care … such as electronic health records.” Yet, as figure 1 shows, there are opportunistic risks associated with information technology (see, for example, Greyhead Associates, 2009b). However inadvertently, the council is perpetuating the myth that electronic health records entail no risks, as it does not acknowledge the risks to personal safety and security described in this essay anywhere in its promotion of the electronic health record.

Publicly expressed concerns

Given the risks associated with information technology, it should not be surprising that privacy concerns are evolving into popular resistance to electronic health records in Canada.

BC’s Big Opt Out (2009) has demanded that the BC government ensure the “right of every British Columbian to determine … whether or not to participate in eHealth by giving or withholding informed consent.” Opt Out’s intention is to “rally British Columbians against the threat to privacy rights” under the new eHealth system. The organizations involved with Opt Out include the BC Civil Liberties Association, BC Persons...

In April 2009, the Consumers Association of Alberta (2009) called on the Alberta government to clearly identify who will have access to Albertans' electronic health records and related personal and financial information, partly out of concern for protecting citizens from harm resulting from losses of confidentiality. Organizations sharing these concerns include the Privacy Commissioner of Alberta, the College of Physicians and Surgeons of Alberta, the Alberta College of Pharmacists, the Canadian Mental Health Association, AIDS Calgary and HIV Edmonton, and the Sheldon Chumir Foundation for Ethics in Leadership.

**Conclusion**

In their attempt to control costs and better manage health care, Canada's governments are looking at establishing electronic health records. For broad protection against the risks of information technology—including robbery, harm to individuals' health, and general privacy breaches—the governments provide only privacy laws. The laws are arbitrary in their provisions and application, and insufficient for combating the risks. Especially troubling is the fact that governments themselves have failed to safeguard their own data holdings, including electronic health records. Concerns about privacy and safety are growing across a broad base of organizations.

None of this is to say that electronic medical or health records are not a valuable endeavour. Nor is this to say that electronic management of information should be avoided in health care. However, it is critical to understand and recognize the risks that are associated with electronic health records before changing down the path of creating such a system for all Canadians.

As they seek to increase the holdings of personal health information in electronic form, governments should attend with greater diligence to one of their core duties: protection of individuals, families, and family caregivers against the transgressions of others, including the government.

It's all a matter of patient safety.

**References**


