THE *REAL* IMPACT OF THE *E-HEALTH ACT*

By Michael Vonn

Proponents of e-health say it is the single most important revolution in health care this century.[1] It is indeed, but unfortunately it is not the good kind of revolution.

Canada Health InfoWay Inc., a federally funded non-profit corporation, exists solely to promote centralized electronic health records for all Canadians. If you've heard of e-health, it is likely through InfoWay's advertising campaign promoting centralized electronic health records as the saviour of Canadian health care, purportedly improving efficiency, increasing patient safety and making health care sustainable. There is in fact very little evidence to support these claims, and rapidly growing evidence that these immensely expensive systems fail to deliver promised benefits and facilitate violations of medical confidentiality on a scale never before seen.

Patients' loss of control over disclosures of their data in a centralized electronic health records erodes trust in health care and creates formidable barriers to access. Two years ago, a Scottish study showed that 25 per cent of people were less likely to attend sexual health clinics if the records were shared in electronic databases, and almost half of the study participants didn't even want their GPs to have access to their sexual health information on a shared electronic database. The Royal College of Physicians and Surgeons in the United Kingdom, a country that was an early adopter of centralization electronic health records, recently reported that a staggering 79 per cent of over 3,500 surveyed physicians would not seek mental health treatment from the local National Health Service, the majority citing concerns about medical confidentiality.

British Columbia has just launched an e-health system. Under the *E-Health (Personal Health Information and Protection and Privacy) Act*, S.B.C. 2008, c. 38 ("*E-Health Act*"), the minister of health can create health information banks ("HIBs"). The architecture for e-health is a giant data distribution system of interoperable databases accessible from tens of thousands of access points. The personal health information in this system is known as an Electronic Health Record ("EHR").

The *E-Health Act* gives a HIB administrator the power to collect identifiable patient information from both public- and private-sector sources. One of the critical features of the *E-Health Act* is authorization for a massive

transfer of private-sector data, which is governed by the *Personal Information Protection Act* ("*PIPA*") into the government's HIBs, which are governed by the *Freedom of Information and Protection of Privacy Act* ("*FOIPPA*"). In British Columbia, the first stage in this massive data transfer into government databases is taking our personal health information from public- and private-sector medical laboratories and putting it into the first designated HIB, which is the Patient Lab Information System ("PLIS").

When personal health information is governed by *PIPA*, it can be shared with informed, implied consent to those in the "circle of care" (i.e., your referring physician, specialists, lab tech). Outside the circle of care, *PIPA* requires express consent for disclosures. These important privacy protections effectively disappear once the data is transferred into government custody. *FOIPPA* does not require patient consent for use or disclosures and it allows for broad sharing of data throughout government. Although HIBs also include information that is already held by a public body, where it takes information out of the private sector, patients lose the ability to control access to their health data by denying consent for disclosures. This is a critical violation of patients' right to control their health information and a loss of control by health care professionals, who are legally and ethically obliged to safeguard patient confidentiality.

Thus, our health information is being transferred to a vast governmental electronic distribution system without our consent. The available privacy "protection" in the *E-Health Act* is to provide for a written instruction, called a "disclosure directive", which provides some limited ability for patients to direct who gets access to their health information in the system. The *E-Health Act* requires that disclosure directives be provided for in the minister's designation order for a health information bank. But it also provides that the minister may severely limit the scope, and thus the privacy protection, of disclosure directives.

The only disclosure directive we have to comment on at this point is the one now available for PLIS (each HIB requires its own disclosure directive). Almost no one in British Columbia knows about the concept of disclosure directives, let alone how to go about putting a disclosure directive on their medical laboratory information about to be transferred to a government database. The Ministry of Health claims of "transparency" appear to be based on the extraordinary notion that members of the general public are all subscribers to the *Gazette* and/or frequently plug the words "disclosure directive" into online search engines on a whim. If you fail to make disclosure directives, the default is that your information will be accessible throughout the province to a vast array of people who work in health care and government.

And if, against all odds, you manage to get your hands on a disclosure directive form and brave the dire government warning that your attempt to protect your medical privacy creates a "barrier" that may delay your receipt of health services, your perseverance does not necessarily result in effective privacy protection. The disclosure directive for lab tests allows you to put a keyword "lock" on all your information that is contained in that database. It's all or nothing. If you allow a health care worker access to your lab results for the purposes of viewing your cholesterol counts, then all your other lab results are also accessible to them. There is currently not, and may never be, an option for what is called record-level masking to keep certain highly sensitive information off the general viewing screen. Further, there will be people who can simply ignore your express refusal to provide access to your records. Some people will get to override your keyword and see your records despite your disclosure directive.

The official line is to stress the use of the override for medical emergency situations in which you may be unable to provide consent to access records. But the issue of who is going to get override powers is currently being hammered out behind closed doors, and if the clinicians the government is consulting have their way, override privileges will be plentiful. What the government endlessly promotes as "The Right Information to the Right People at the Right Time" is likely to evolve into "All the Information to Most of the People at Any Time". The statement on the disclosure directive form that "[o]nly health professionals who are providing you with care, and need to know the information to do so, will be able to see your [electronic health record]" is incorrect. Without a disclosure directive, the roles-based access system that is planned is largely an honour system for health care workers who have access codes. But even where patients make disclosure directives to limit the scope of disclosures, the *E-Health Act* allows for access by some government officials and bureaucrats, and disclosures for "secondary purposes", including planning, evaluation, public health surveillance and research, vetted by government appointees to the Data Stewardship Committee.

In no way does the *E-Health Act* restrict viewing of your personal health information to those providing care. Section 5 of the Act does, however, limit the purposes for disclosure of information held in health information banks to purposes which are mostly health care related. There will undoubtedly be an issue about how broadly a "health care purpose" can be defined for purposes of disclosure, and there is a great likelihood that s. 5 will be amended in the future to facilitate the dissemination of personal health information broadly among an array of government ministries. This is likely because the architecture for the interoperability needed to allow

access to personal health information by other ministries is planned and under way.

B.C.'s centralized electronic health information infrastructure is meant to anchor a vast integration project called the Information Access Layer. This massive information-sharing project is to encompass the entirety of social services in the province and link information about citizens from the Ministries of Employment and Income Assistance, Children and Families, Health, Education, Justice and the private-sector contractors for these ministries. The province has already issued an RFP for this project. Widespread dissemination of personal health information throughout various government departments is apparently anticipated by those committees and consultants who are deciding who will have access to our medical information. A meeting of one committee I attended briefly as a guest kicked off with a casual reference to social workers being given access to the EHR. Access by social workers would, of course, be a public health catastrophe, severely limiting the ability of vulnerable populations to access a critical range of services from addiction treatment to counseling for post-partum depression. But social workers will be just one of many groups in the long line-up of those claiming "a need to know" and demanding access to the EHR (expect the police to be at the front of the line). And the decision whether to grant that access won't be ours to make.

The e-health "revolution" is a paradigm shift that takes decision-making about access to health information out of the hands of the patient and into the hands of government. "Enhanced service delivery" and "efficiency" rhetoric is attempting to mask a profound erosion of fundamental rights. The government's e-health vision is a promise of beneficent data stewardship, but the government should not be the "steward" of our health information. Privacy is a human right and a public good, and the basis for medical rights, including health privacy, is patients' informed consent, not government stewardship. To boot, the government's actions, as opposed to its advertising messages, do not bode well for the privacy protections it claims will be part of its stewardship model.

In addition to the devastating effects on health privacy, the centralization of electronic health records jeopardizes the security of the data in the ways that cannot be mitigated. A linked database system of this kind cannot be made secure. There are instructive lessons yet again from the U.K., which has had to stop even pretending that it can protect data in the face of tens of millions of records lost or compromised and the prime minister's own health data being illegally accessed and given to the media. As Ross Anderson, professor of security engineering at Cambridge University, stated in *The Economist*:

> Patient data held at a GP practice may be vulnerable to a security lapse on the premises, but the damage will be limited. You can have security, or functionality, or scale—you can even have any two of these. But you can't have all three, and the government will eventually be forced to admit this. In the meantime, billions of pounds are being wasted on gigantic systems projects that usually don't work and that place citizens' privacy and safety at risk when they do.

And the security of computerized medical information is a very real issue. Recently, despite e-health "security like Fort Knox", the personal health information of 11,582 people was captured by hackers who infected 150 Alberta Health Services computers with a virus that was undiscovered for two weeks. Also just reported from Ohio, spyware targeted at an ex-girlfriend infected the computers at the woman's workplace, sending more than 1,000 screen captures of medical information from Akron Children's Hospital to the perpetrator.

We are developing a system that severely diminishes patient privacy, dignity and autonomy and creates massive security risks. And these outcomes are entirely avoidable. There are alternative models of electronic health records that are deliberately being ignored.

As stated in the Rowntree Trust Report on 46 public-sector databases in the U.K., including their centralized electronic health records system:

> There is a developing consensus among medical practitioners that for safety, privacy and system engineering reasons, we need to go back from the shared-record model to the traditional model of provider-specific records plus a messaging framework that will enable data to be passed from one provider to another when appropriate.

In other words, the right model is one in which data is pushed from one health care provider to another, not pulled from every health care provider into a massive electronic data distribution system. Not only is a secure "push model" already available in Canada, it does not cost the billions of dollars we are spending on health data centralization. In fact, it's free.

As David Chan, M.D., associate professor of family medicine and director of information technology at McMaster University, has pointed out, Canadians have access to free open-source medical-records software that was developed by McMaster in collaboration with Harvard and MIT. In this system, doctors maintain an electronic patient record that can securely send electronic information to other health care providers in the circle of care and to patients themselves, who then become the joint custodians of their own medical information. This is an example of a non-commercial, personally controlled health record, a model that safeguards patient privacy and autonomy and leverages the benefits of electronic data sharing within the circle of care without incurring the massive costs and security risks of data centralization.

Why is the government instead choosing a model that requires, as one provincial privacy commissioner has put it, the "expropriation" of our personal health information? The only possible answer is because they want the personal health information "expropriated" and intend to use it.

The *E-Health Act* does not protect patient privacy, it deliberately erodes privacy by creating a new structure of health record custodianship with governmental control over health information dissemination. As H.M. Oetter, M.D., registrar of the College of Physicians and Surgeons of B.C. has stated, "[M]odels for sharing data must be built on the fundamental principle that patients have a right to consent—or withhold consent—to sharing of their health information." This is not the model that has been legislated under the *E-Health Act*.

ENDNOTE

1. See Jill Scott, "The Impact of the *E-Health Act*" (2009) 67 Advocate 495.