Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win/Win

March 2, 2012

Information and Privacy Commissioner, Ontario, Canada

Canada Health Infoway | Inforoute Santé du Canada

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Richard C. Alvarez, ICD.D
President & CEO
Canada Health Infoway

Canada Health Infoway / Inforoute Santé du Canada

Canada Health Infoway
1000 Sherbrooke St. W.
Suite 1200
Montreal, Quebec H3A 3G4
Web site: www.inforway-inforoute.ca

Information and Privacy Commissioner
Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

EMBEDDING PRIVACY INTO THE DESIGN OF ELECTRONIC HEALTH RECORDS TO ENABLE MULTIPLE FUNCTIONALITIES – WIN/WIN

by
Ann Cavoukian, Ph.D., Information & Privacy Commissioner of Ontario
and
Richard C. Alvarez, ICD.D, President & CEO, Canada Health Infoway

Introduction

Personal health information comprises some of the most sensitive and intimate details of one's life, such as those relating to one's physical or mental health and the health history of one's family. As such, it requires strong protections to ensure the privacy of the individual to whom it relates. Personal health information must also be accurate, complete, and accessible to healthcare providers in order to deliver necessary health care to individuals. At the same time, health information has long been used for invaluable secondary purposes that go beyond the care and treatment of the individual, for uses that are seen to benefit society as a whole. This includes such varied uses as population health monitoring, quality improvement, health research, and the management of Canada's publicly-funded healthcare system.

The question of how to maximize both personal privacy and the benefits that may be derived from secondary use becomes more challenging as information technologies like electronic health records (EHRs) become more prevalent in the health sector. While the objective of maximizing both values remains the same, technological advances that permit faster, less costly and more accurate uses of personal health information also pose novel challenges for privacy, security, and transparency. On the one hand, the transition from paper-based to electronic records can enable immediate access to large volumes of personal health information, often over great distances, which can vastly improve primary care and facilitate secondary uses. On the other hand, electronic systems pose unique risks to privacy and security, not least of all because information from diverse sources can be amassed and accessed in electronic format, by authorized users who may be far removed from the site of original collection. Information stored indefinitely in large-scale data repositories may more quickly and easily be linked to information from other data repositories, and may conceivably be used for an ever-increasing number of as-yet-undefined, future purposes.

The transition from paper-based records to EHRs raises a number of questions in relation to secondary use. How and by whom will decisions about secondary uses in the EHR environment be made? What safeguards are and should be in place to promote privacy and security? How do we promote transparency about uses and disclosures for secondary purposes? How do we maintain public trust and confidence in the ability of electronic systems to protect privacy, particularly given the growth of EHRs and the potential expansion in secondary use? Without public trust in the ability of these systems to safeguard our most sensitive information, we may be deprived of the rich stores of information that are essential, not only for vital secondary purposes but, even more importantly, for the primary care uses that keep our population safe and in good health.

This paper begins with an overview of some of the elements already in place or under development, which form the basis of a framework to govern secondary use in the EHR environment. These existing measures include statutory safeguards, independent privacy oversight, and principles set out in a statement of Common Understandings developed by the Pan-Canadian Health Information Privacy Group.

We propose that secondary use should continue in the EHR environment as it did with paper-based records, and that it may be done in a way that respects both individual rights to privacy and broader societal interests.

We endorse an approach to secondary uses in the EHR environment that incorporates *Privacy by Design* (*PbD*). *PbD* not only accommodates the values of individual privacy and confidentiality, but actually enables stronger privacy protections, thereby helping to ensure the continued availability of information for secondary purposes that benefit us all. This approach is premised on the view that the default condition should be one of de-identification: de-identified information should be used or disclosed for secondary purposes and, where de-identified information is insufficient for the purpose, additional safeguards must be introduced prior to the use and disclosure of personal health information for secondary purposes. In this paper, a distinction is drawn between personal health information, which refers to identifying information about the health and the provision of health care to an individual, and health information, which refers to de-identified information.

The Value of Electronic Health Information for Research and Health System Uses

Everyone is familiar with certain everyday uses of personal health information for purposes going beyond the direct care and treatment of an individual, such as claims processing, quality improvement, and health research. Privacy legislation recognizes the value of such uses by generally permitting the collection, use, and disclosure of personal information, including personal health information, for secondary purposes under appropriate circumstances. In Ontario, for example, the *Personal Health Information Protection Act, 2004* (*PHIPA*) establishes clear rules for the collection, use, and disclosure of personal health information for secondary purposes, including health research.

The enormous value of secondary uses was also underscored in the October 2002 report of Chair Michael Kirby's Senate Committee examining the state of the health care system in Canada [the Kirby Report][1] and the November 2002 report of a Commission led by Roy J. Romanow on the future of Canada's publicly-funded healthcare system [the Romanow Report].[2] These reports acknowledged the importance of secondary use in: improving our understanding of the determinants of health; informing and improving clinical practice guidelines; identifying and achieving cost efficiencies in the healthcare system; facilitating health promotion and disease prevention activities; assessing needs for health services, monitoring

1 Canada, Senate. Standing Senate Committee on Social Affairs, Science and Technology, *The Health of Canadians – The Federal Role. Final Report on the State of the Health Care System in Canada. Volume Six: Recommendations for Reform, Chapter 10: The Federal Role in Health Care Infrastructure* (Ottawa: October 2002) (Chair: Michael Kirby) [Kirby Report].

2 Canada, Privy Council. Commission on the Future of Health Care in Canada, *Building on Values: The Future of Health Care in Canada - Final Report* (Ottawa: November 2002) (Commissioner Roy J. Romanow, Q.C.) [Romanow Report].

and evaluating services, and effectively allocating resources; and educating the public about proactive steps to improve one's overall health. The reports also recognized that information collected in a publicly-funded health system could and should be used to benefit the health of Canadians as a whole, and to contribute to the public good.

The Kirby and Romanow Reports also explicitly recognized the role of healthcare technology, and specifically of EHRs, in making information available for research and related secondary purposes.[3] Both primary and secondary uses benefit from the widespread adoption of EHR systems, which offer many advantages over traditional paper-based records held by healthcare providers. In contrast to paper-based records, health records stored in electronic format require less space and fewer administrative resources to maintain, and can be shared and readily accessed by all of an individual's healthcare providers, regardless of location. They are also more likely to contain complete and up-to-date personal health information about an individual.

When EHR systems are built to coding and messaging standards that are consistent across Canada, these systems may also be used to support pan-Canadian studies. Nationwide consistency in coding, messaging, and other architectural standards has been a significant focus of the work of Canada Health Infoway. This federally-funded, not-for-profit corporation charged with coordinating the development and deployment of interoperable EHRs in Canada recognizes the need for access to reliable, accurate, longitudinal health information for research, analysis, and other purposes. Through its Privacy and Security Conceptual Architecture, it also promotes the incorporation of strong privacy and security features, including strong encryption, anonymization, and de-identification, in all EHR systems.[4]

As electronic systems become more widely implemented in the health sector, clearly the clinical benefits of using electronically-gathered personal health information are emerging. In Ontario, for example, a Canada Health Infoway-supported project in Sault Ste. Marie links physicians and pharmacists treating chronic disease patients by making electronic medical records (EMRs) in physicians' offices available to local pharmacists. The EMRxtra project enables the sharing of personal health information between healthcare providers, resulting in improved quality of care for chronic disease patients, and much higher rates of provider and patient satisfaction. The measurable clinical benefits include: increased rates of identification of drug-related problems; improved rates of active engagement with patients, as reported by pharmacists; better medication coordination with fewer medication list discrepancies; and higher rates of self-management and empowerment, as reported by patients.[5]

3 See Kirby Report, *supra*, note 1, pp. 171-184; Romanow Report, *supra*, note 2, Chapter 3: Information, Evidence and Ideas, pp. 75-90.

4 Canada Health Infoway, *An overview of the Electronic Health Record Privacy and Security Conceptual Architecture* (March 2006). Available online at: https://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security-Overview.pdf.

5 Canada Health Infoway, *Spotlight on Results: EMRxtra* (May 3, 2010).

In addition to the clinical benefits, electronic systems have the potential to facilitate secondary uses. In the absence of electronic systems, personal health information is often still held in non-standardized, paper-based formats, by individual healthcare providers. Even where personal health information has been digitized, it is often contained within local systems that are not interoperable. In order to leverage personal health information for secondary purposes, it must be either manually extracted from paper-based charts, or transferred electronically from local systems to centralized systems. Once the personal health information is received, it must then be translated into a standard format before it can be linked together, de-identified, and used for analysis.

Currently, individual healthcare providers are the gatekeepers of personal health information, and have the discretion to decide who may access information and for what authorized purposes. The experience of Ontario's Information and Privacy Commissioner has been that where a healthcare provider decides to use or disclose information for secondary purposes, it is often used and disclosed in identifiable form, even if de-identified information would serve the purpose, simply because the provider does not have the resources or capacity to de-identify the information before making it available for a secondary purpose. Even in cases where the healthcare provider has the resources and capacity to de-identify information, identifiable information is often required to link information that is scattered throughout the health system, across time and sources, in order to make it usable for the secondary purpose.

By contrast, EHRs can make secondary uses much safer, less costly and more accurate – including, for example, by eliminating the need to convert paper-based records into a digitized format for analysis, facilitating the de-identification of personal health information and enabling the creation of repositories of *de-identified* information for analysis and research purposes. Electronic transfers can also eliminate the privacy risks associated with transferring paper-based records containing personal health information, which have been the source of several well-publicized privacy breaches in recent years.[6,7]

Electronic systems also offer the potential to increase the speed and efficiency of research and other secondary uses, by automating the collection, extraction, and organization of common data elements from various repositories in the EHR. The EHR can provide a less privacy-invasive means of identifying potential research participants by automating initial screening processes on one or more diagnostic fields, thereby reducing the need for manual screenings of patient

6 Consider, for example, the investigation of the Saskatchewan Information and Privacy Commissioner into a breach involving over 180,000 records of personal health information found in a recycling bin in Regina. In a July 2011 investigation report, the Commissioner described the incident as the largest breach of patient privacy since the enactment of that province's health information legislation.

7 The Information and Privacy Commissioner of Ontario has also issued a number of orders in privacy breaches involving the unsecure transfer or disposal of paper records – see Orders HO-011 (involving unconfirmed courier deliveries of cancer screening reports affecting over 7,000 Ontarians), HO-006 and HO-001 (involving records containing personal health information found scattered on the streets), and HO-003 (involving records abandoned by a walk-in medical practice when it closed its practice).

charts by individuals who are outside the patient's circle of care.[8] Automated functions like these can significantly enhance privacy protections, while at the same time streamlining the research process. Electronic systems can also provide longitudinal data that can be readily used for research and analysis in quality assurance, epidemiological studies, and disease monitoring.

As noted, one of the most important features of the approach taken by Canada Health Infoway in the development of EHRs was the creation of a consistent architecture and standards for data collected across the country. Increasing standardization and integration facilitates interoperability and authorized information-sharing, across systems and across jurisdictions. The EHRs implemented by each jurisdiction may enable the establishment of data repositories that will house, manage, and disclose information for secondary use. These jurisdictional data repositories could become platforms for future research that, once created, would enable researchers to subsequently draw upon the same sources of data for any number of future research projects.[9]

At the same time, the advantages of storing vast amounts of electronic information and the ease with which digitized information may be linked for authorized purposes present some of the greatest challenges to privacy and security, and to the continued widespread public acceptance of the EHR. It is also apparent that while the health sector is abundantly aware of the need for secondary use of the EHR, ordinary Canadians are not as familiar with the concept. In order to ensure the continued availability of complete and accurate EHR data for secondary purposes, it is important to maintain public trust in the EHR. In order to do this, we must address the potential challenges to privacy and confidentiality that are commonly associated with increasing secondary uses.

The Challenges Associated with Research and Health System Uses in the EHR Context

Secondary use poses challenges for adhering to widely-accepted fair information practices, starting with the general proposition that personal health information should only be collected, used, and disclosed with the consent of the individual to whom it relates. Since personal health information is generally collected in the course of providing health care, often on the basis of implied consent, it may be difficult to ensure knowledgeable consent for its use and disclosure for secondary purposes that may occur years after the information has been collected. Safeguards, such as the de-identification of personal health information and transparency about secondary uses, are therefore critical. A framework to manage secondary

8 Willison, D., *Use of Data from the Electronic Health Record for Health Research – current governance challenges and potential approaches* (March 2009) [Willison], p. 2. Available online at: http://www.priv.gc.ca/information/pub/ehr_200903_e.cfm.p 2.

9 Kosseim, P. and Brady, M., "*Policy by procrastination: Secondary Use of Electronic Health Records for Health Research Purposes*" (2008) 2 *McGill Journal of Law and Health* 5 [Kosseim], p. 17.

use must address the challenges associated with safeguarding information in the EHR.

De-Identification Challenges

By its nature, personal health information is extremely sensitive, and its theft, loss, or unauthorized use and disclosure can have dire consequences for the individuals involved. Personal health information that falls into the wrong hands may result in discrimination, stigmatization, and psychological or economic harm to the individual. It is for this reason that fair information practices call for data minimization. Data minimization requires that identifying information not be collected, used, or disclosed if some other information would serve the same purpose, and that no more identifying information be collected, used, or disclosed than is reasonably necessary.

While identifiable information is clearly necessary in the context of delivering health care to individuals, personal health information is often not needed for secondary purposes – that should be the default. Therefore, personal health information should be routinely de-identified before it is used or disclosed for such purposes. To the extent that de-identified information may be used for a secondary purpose, privacy risks will be significantly minimized. The transition to EHRs presents new opportunities to build de-identification directly into processes and systems, consistent with *PbD*.

While the de-identification of personal health information will be facilitated by EHRs, the increased quality of the information available through electronic systems may also increase the risks of re-identification. Some researchers have found that it is sometimes possible to re-identify individuals from seemingly anonymous data.[10] However, contrary to detractors' claims about the ease of re-identification, it has been shown that the re-identification of properly de-identified information is not an easy task – quite the contrary.[11] Moreover, such re-identification takes a significant level of specialized knowledge and intent. While de-identification may not guarantee the total elimination of all privacy risks (as indeed, no tool can), de-identification remains the vital first step that drastically reduces the risk of personal information being used or disclosed for unauthorized purposes.

The use of proper de-identification tools and re-identification risk measurement techniques (such as the de-identification tool discussed shortly) reflects a *PbD* approach to the challenge of protecting privacy while at the same time making available quality information for critical secondary purposes. When done properly, de-identification remains one of our most important tools for offering what we

10 See, for example, Paul Ohm (*Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*), and others, cited in Cavoukian, A., and El Emam, K., *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy* (June 2011) [Dispelling the Myths Surrounding De-identification]. Available online at: http://www.ipc.on.ca/images/Resources/anonymization.pdf.

11 El Emam, K. et al., *A Systematic Review of Re-Identification Attacks on Health Data* (submitted for publication, 2011), cited in Dispelling the Myths Surrounding De-identification, *supra*, note 10.

call a "Big Privacy" response to "Big Data," where the ever-increasing power of computers and the greater availability of information make it easier to capture, communicate, aggregate, store, and analyze enormous datasets. We return to de-identification and other elements of a Big Privacy response to the challenges of Big Data elsewhere in this paper.

Unauthorized Access

There is concern that as information becomes more widely available for secondary purposes through EHRs, it may become more difficult to control the existing problem of unauthorized use and disclosure of personal health information by persons with access to this information. While the vast majority of the hundreds of thousands of EHR transactions that occur daily are for lawful purposes, privacy breaches can result from authorized healthcare providers with role-based access privileges accessing electronic records for purposes other than the provision of health care. This type of improper access by authorized users can be motivated by financial interests (as in the case of fraud, improper billing, or identity theft), or by curiosity or concern about the health of family members, neighbours, co-workers, or celebrities. These types of breaches can severely damage institutional reputation and, widely reported, can breed public mistrust in the ability of EHRs to protect patient privacy.

In addition to unauthorized access by healthcare providers, there is also the risk of improper use and disclosure by authorized secondary users, such as health researchers. However, it is important to note that, in the case of secondary users, the transition to electronic systems may actually help to minimize the risk of unauthorized access since it will be relatively easy to de-identify electronic personal health information prior to its use for secondary purposes. Moreover, every transaction in the system is logged and is subject to audit, making it much easier to detect unauthorized activity. Coupled with a zero tolerance policy, logging and audit practices can dramatically minimize unauthorized activity.[12]

Data Governance

Another question that must be addressed with respect to secondary use in the EHR environment is that of data governance. While currently, healthcare providers have control over their own paper-based and electronic records, they will have less control over who may access personal health information, and for what purposes,

12 In the U.S., one family physician with a large group practice of 200 physicians in 75 sites across two states has implemented a policy of zero tolerance for physicians and staff who access personal health information in an unauthorized manner in the secure EMR used in the group practice. The EMR system is retained in a data centre that requires individuals to pass through multiple levels of security in order to access personal health information stored in the EMR; in addition, the system is built with the ability to monitor for access to servers in real time, and audit logs are maintained of all accesses to the EMR by physicians and staff. These safeguards and the practice's zero tolerance policy have helped to detect and to prevent further unauthorized access. As reported to the Information and Privacy Commissioner of Ontario, the number of breaches dropped from 11 in the year the zero tolerance policy was introduced to two breaches the following year. Since then, the group practice has terminated between two and four employees annually under the zero tolerance policy.

in the context of shared EHRs. It may be argued that this control is best left in the hands of individual healthcare providers, who understand the wishes of their patients and are committed to acting in their best interests. On the other hand, one may argue that providing individual healthcare providers with this discretion has resulted in inconsistent practices and incomplete information being made available for valuable secondary purposes. We return to the issue of data governance as we discuss elements of a proposed framework later in this paper.

The Need for Transparency

Despite public education initiatives, such as Canada Health Infoway's *Knowing is Better* campaign to inform Canadians about progress in implementing EHRs in Canada,[13] there is still little public understanding of how personal health information is used and disclosed in the health sector, particularly in the EHR environment. While secondary use is a complex topic, jurisdictions must be open and transparent about how EHR data will be used for secondary purposes. To be anything less than transparent risks eroding public trust in the EHR.

Encouragingly, research indicates that Canadians generally believe in the importance and value of using EHR information for certain secondary uses – they have some degree of comfort with the idea as long as privacy and security protections are in place. For example, a 2007 survey jointly sponsored by Canada Health Infoway, Health Canada, and the Office of the Privacy Commissioner of Canada[14] found that while awareness and support for EHRs was high and increasing,[15] those who were opposed to the development of EHRs based their objections almost entirely on concerns about the ability of EHRs to protect the security and confidentiality of personal health information stored in these systems.[16] A number of measures, such as the existence of audit trails, strong penalties for unauthorized access, and notification of privacy breaches, raise their comfort levels.

Furthermore, roughly three-quarters of Canadians are very comfortable using EHRs to prevent improper use of the healthcare system, to anticipate or address health issues, or to plan, monitor, and evaluate the healthcare system.[17] More than eight in 10 (84%) support the use of EHRs in health research if the information is de-identified; there is much less support if identified information is used (54%), and somewhat more (66%) if they provide consent in advance.[18] Their comfort in sharing de-identified information varies depending on the recipients of the information. Support is higher for sharing with groups such as governments,

13 See Canada Health Infoway's public education campaign microsite: www.KnowingisBetter.ca.

14 EKOS Research Associates, *Electronic Health Information and Privacy Survey – What Canadians Think* (August 2007) [EKOS 2007 Survey]. Available online at: https://www2.infoway-inforoute.ca/Documents/EKOS_Final%20report_EN.pdf.

15 From EKOS 2007 Survey, *supra*, note 14, p. 4: Nearly one in two Canadians (49%) has heard of EHRs (up eight % since 2003) and one in three (31%) has interacted with this type of system. Close to nine in 10 Canadians (88%) support the development of EHRs (up five percentage points since 2003).

16 Ibid, p. 47.

17 Ibid, p. 69.

18 Ibid, p. 71.

researchers, healthcare organizations, and statistical organizations, than it is for sharing with the private sector.[19]

It is vital that we continue to build public trust and confidence in the ability of EHR systems to safeguard privacy. Research has shown that individuals concerned about the inappropriate use and disclosure of their personal health information may engage in privacy-protective behaviours – including, for example, withholding or providing incorrect information to healthcare providers, avoiding needed treatment or diagnostic testing for certain conditions, or electing to pay for certain drugs and services out-of-pocket rather than submitting a claim through an insurer.[20] These behaviours can result in the collection of inaccurate or incomplete personal health information, which can hinder both healthcare efforts and secondary uses. Although the public appears to accept the importance of certain secondary uses of EHR information, continued availability of this information depends on maintaining the public's trust in the ability of secondary users to protect it.

Towards a Governance Framework for Research and Health System Uses in the EHR Context

We turn now to examining potential elements of a governance framework for privacy-protective secondary uses in the EHR context. *Privacy by Design* (*PbD*) and the Common Understandings paper set out principles upon which a framework for secondary use should be built. Other elements are tools and mechanisms that are already available but should be more widely adopted as part of this governance framework. Still other issues require further discussion and debate among stakeholders. As such, the framework will not be static, but will evolve over time. Regardless, the framework adopted must protect individual privacy while making quality health information available for critical secondary uses. This approach is based on *PbD*, a doubly-enabling, positive-sum model in which both values – privacy and data quality – are maximized.

Privacy by Design

In the health sector, the traditional zero-sum paradigm pits the privacy of patients against the broader public interest in accessing quality health information for research purposes and other uses, leading to a win-lose scenario in which one interest is inevitably subordinated to the other. *PbD* rejects the traditional zero-sum paradigm and calls for privacy to be built proactively into the design of information technologies, networked infrastructures, and information practices, by default, to ensure not only that privacy is an essential component of the core

19 Ibid, p. 27.

20 As reported by California HealthCare Foundation and Forrester Research, Inc. *National Consumer Health Privacy Survey 2005* (November 2005). Available online at: http://www.chcf.org/publications/2005/11/national-consumer-health-privacy-survey-2005.

functionality being delivered, but to enable other equally-important functionalities to co-exist.

As we move into an era of "Big Data," *PbD* offers a holistic, proactive approach to privacy protection that can help to anticipate and address the "big harms" to privacy that are a foreseeable danger of Big Data. At the same time, *PbD* recognizes and aims to facilitate the benefits of harnessing Big Data for socially useful applications. In the context of designing and implementing EHR systems, *PbD* seeks to protect the privacy of individuals whose personal health information is contained in EHRs while enabling multiple goals – privacy *and* security, individual *and* societal benefits, confidentiality *and* data quality. In this way, *PbD* facilitates access to health information for secondary purposes while at the same time protecting the privacy and confidentiality of health information held in the EHR. This is accomplished by embedding privacy and security directly into EHR systems, through the routine de-identification of personal health information for secondary purposes, end-to-end security, and other mechanisms discussed elsewhere in this paper. *PbD* offers a means of elevating privacy in the Big Data world to an effective countervailing force that we are calling "Big Privacy" – a method of ensuring that privacy is embedded as a *first consideration* in all Big Data transactions. Consistent with *PbD*, the Pan-Canadian Health Information Privacy Group proactively considered the privacy implications of secondary use in its paper outlining general principles for information governance in the EHR environment.

Pan-Canadian Common Understandings

In its first Common Understandings paper,[21] the Pan-Canadian Health Information Privacy Group (formed in December 2008 of a subset of members of the Pan-Canadian Privacy Forum on EHR Information Governance) articulated 33 principles to support appropriate and privacy-protective, trans-jurisdictional disclosures of EHR information. These common understandings are statements of general consensus of the Health Information Privacy Group members toward the goal of promoting consistency and informing jurisdiction work on health sector privacy legislation, associated e-health policies, information-sharing agreements, and business and technical requirements for EHR systems.[22]

The principles articulated in the Common Understandings paper provide guidance toward the development of a practical framework for managing secondary use in the EHR environment. In addition to common understandings on trans-jurisdictional disclosures for health care and treatment, and on accountability for information governance of the interoperable EHR, a number of understandings

21 Canada Health Infoway, Pan-Canadian Health Information Privacy Group, *Privacy and EHR Information Flows in Canada: Common Understandings of the Pan-Canadian Health Information Privacy Group* (June 2010) [Common Understandings]. Available online at: https://www2.infoway-inforoute.ca/Admin/Upload/Dev/Document/Common_Understandings_Privacy_EN.pdf.

22 Common Understandings, *supra*, note 21, p. 5.

relate specifically to trans-jurisdictional disclosures for secondary use.[23] These common understandings propose:

- The aggregation or de-identification of personal health information as the *default* condition for secondary uses;
- The use of risk assessment processes, data disclosure agreements, security practices, and other safeguards to minimize privacy risks of disclosing information for secondary uses;
- The inclusion in patient notices of information about trans-jurisdictional disclosures for secondary uses, and record-keeping of trans-jurisdictional disclosures of identifiable information so that reports can be made to patients upon request;
- The use of agreements setting out obligations and conditions for the management of health information being disclosed to other jurisdictions for secondary purposes;
- That entities and individuals responsible for handling requests for trans-jurisdictional disclosures of EHR information for secondary uses have up-to-date expertise in the use and application of de-identification tools; and
- Pan-Canadian deliberation of secondary use issues and the development of recommendations for consideration by all jurisdictions in an effort to promote a degree of consistency in approach across the country.

The principles of *PbD*, in conjunction with the Common Understandings, must form the foundation of the framework for research and health system uses of personal health information in the EHR context. In fact, many of these principles have already been incorporated into existing safeguards to protect privacy in the context of secondary use, as described below.

Existing Elements of a Governance Framework for Research and Health System Uses

Privacy Legislation, Policies, and Procedures

All provinces and territories have in place legislation to protect personal information; eight have also enacted health-specific privacy legislation.[24] These statutes generally authorize secondary use under appropriate circumstances and treat information that does not relate to an identifiable individual as falling outside the scope of the legislation.

23 Ibid, pp. 20-25.

24 These are: Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland, Nova Scotia, Ontario, and Saskatchewan.

There are often special rules for research. Health sector privacy legislation, like Ontario's *PHIPA*, permit the collection, use, and disclosure of personal health information for research purposes both with consent, and without consent subject to compliance with stated, detailed requirements. While they may vary in detail and stringency across jurisdictions, the requirements typically include the preparation of a research plan, the approval of the research plan by a research ethics board, identification of the privacy-related issues that must be considered by a research ethics board in approving a research plan, and an obligation on data custodians or trustees to enter into written agreements with third-party researchers.[25] Other guidelines governing research include the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans,* the *ICH Guideline for Good Clinical Practice*, and applicable professional and legal obligations. Legislation in some provinces mandate the creation of special data stewardship committees to manage the disclosure of information contained in provincial data banks for health planning and research purposes.[26]

Additional statutory protections may be necessary as personal health information in EHRs becomes more widely available for a broader range of secondary uses. For example, it may be necessary to establish clear legislative authority for making decisions about the use and disclosure of personal health information in the EHR for secondary purposes, since no single custodian may have the authority to do so in the context of a shared record.

Privacy Oversight

Independent privacy oversight is an important element of any framework for the governance of secondary use in the EHR environment. All jurisdictions have privacy oversight bodies in place to review compliance with privacy statutes and to investigate complaints. The powers of these oversight bodies vary by jurisdiction – some have powers to make recommendations, while others, as in Ontario, have order-making powers.

In Ontario, the Information and Privacy Commissioner has order-making powers and has used them in a number of cases of unauthorized access to personal health information held in electronic records. For example, an order was issued in the case of a hospital nurse who accessed a patient's records and shared this information with the patient's estranged husband, an employee of the hospital, despite the fact that the nurse was not providing care to the patient and the patient had specifically raised her privacy concerns to the hospital at the time of her admission.[27] In a subsequent case involving the same hospital, the Commissioner

25 Canadian Institutes of Health Research (Kosseim, Patricia, ed.), *Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research* (Ottawa: Public Works and Government Services Canada, 2005), pp. 60-61. Available online at: http://www.cihr-irsc.gc.ca/e/documents/ethics_privacy_compendium_june2005_e.pdf.

26 Kosseim, *supra*, note 9, p. 11, citing B.C.'s *E-Health (Personal Health Information Access and Protection of Privacy) Act.* See also Alberta's *Health Information Act*, which establishes a provincial EHR data stewardship committee to make recommendations on rules related to access, use, disclosure, and retention of prescribed health information accessible via the Alberta EHR.

27 Order HO-002 of the Information and Privacy Commissioner of Ontario. Available online at: http://www.ipc.on.ca/images/Findings/up-HO_002.pdf.

found that the hospital's efforts to prevent unauthorized use and disclosure of personal health information by agents and employees of the hospital had not been effective.

In light of the proliferation of EHRs, the powers and authorities of privacy oversight bodies may need to be reviewed and expanded to ensure effective oversight for all secondary use of personal health information.

Privacy-Protective EHR Architecture

As noted, an appropriately-designed EHR can be more privacy-protective than traditional paper-based records. Privacy and security safeguards can be embedded by default directly into EHR systems. The Privacy and Security Conceptual Architecture developed by Canada Health Infoway was based on a set of more than 100 privacy and security requirements. The Architecture helps to ensure that interoperable EHR systems comply with federal, provincial, and territorial privacy and security requirements, as well as with trans-jurisdictional requirements relating to both health care and treatment and secondary use. The Architecture features many privacy and security safeguards, which are applicable not only to the EHR in general but also specifically to the secondary use of information. For example, the anonymization services referenced in the Architecture address the need for systems to allow for the removal of identifiers from a record to enable secondary use of the information; the encryption services address the need for safeguarding information while it is stored or transmitted; and the secure auditing services ensure that all transactions are recorded to enable the tracking and reporting of uses and disclosures for any purpose, including secondary use.

There are also applications, like commercial breach detection and fraud management software, available to address the growing risk presented by users with authorized access. These tools can help prevent and detect unauthorized use and disclosure by recording patterns of user access and activity in electronic records, monitoring and analyzing user behaviour for patterns that may indicate misuse, and generating alerts or reports in order to contain unauthorized activity and to trigger further auditing. These tools offer the potential of automating manual processes to more effectively review and audit usage patterns in EHRs that could indicate unauthorized access or other non-compliance issues.

De-Identification Protocols

As noted, routine de-identification is one of the most valuable tools for protecting privacy. De-identification can assist in complying with data minimization principles and in avoiding privacy breaches as a result of theft, loss, or unauthorized access to personal health information. At the same time, de-identification can enable the use of health information for important secondary purposes, such as health research. De-identification becomes an even more powerful tool in the EHR context: de-identification techniques are easier to apply to electronic records than to paper records, and software tools are available that can automatically remove or suppress direct identifiers in a dataset. Some de-identification methods aim

to simultaneously minimize both the risk of re-identification and the degree of distortion to the original database, such as the excellent privacy-enhancing tool developed by Dr. Khaled El Emam, which can be applied directly to databases of personal health information.[28] When done in a manner that minimizes the risk of re-identification while maintaining the level of data quality appropriate for the secondary purpose, and through continuous research and refinement to address new risks as they arise, de-identification embodies a *PbD* approach that maximizes the interests of data custodians, secondary users, and most importantly, the individuals to whom the information relates.

Governance of Information Held in EHR Repositories

Jurisdictions are already addressing data governance issues related to the secondary use of information held in EHRs. A number of jurisdictions have established Chief Data Stewards and/or Data Stewardship Committees to review requests for access to information and to control disclosures of information for analysis. It is expected that continued efforts will be required to build the policies and best practices necessary to govern use of information held in the EHR – as data stores grow in size, their value for research and analysis will increase, as will the pressure to access them for a wide array of studies.

Data Warehouses

A number of jurisdictions have established data warehouses to collect, use, and disclose personal health information for secondary purposes. Data warehouses may offer the advantage of up-to-date expertise in implementing privacy and security safeguards, including de-identification, in the context of Big Data. The bodies responsible for such warehouses are also subject to strong rules that require them to put into place practices and procedures to minimize the privacy and security risks associated with the information they collect, use, and disclose.

Ontario's *PHIPA*, for example, establishes the special designations of "prescribed person" and "prescribed entity" for bodies that may receive personal health information for specified purposes without explicit consent, including for analysis or compiling statistical information with respect to the management of the health system.[29] However, before any disclosures may be made to these bodies in Ontario, they must be prescribed in the regulations and they must have in place strong practices and procedures to protect privacy and maintain the confidentiality of the personal health information they receive. These practices and procedures must be

28 Dr. El Emam's de-identification tool sets out a practical methodology for using de-identification techniques and re-identification risk measurement tools to achieve a level of data quality necessary both for the recipient's purposes and for the level of risk exposure acceptable to the information discloser. See Cavoukian, A., and El Emam, K., *A Positive-Sum Paradigm in Action in the Health Sector* (March 2010). Available online at: http://www.ipc.on.ca/images/Resources/positive-sum-khalid.pdf.

29 Namely, to compile or maintain a registry of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances, in the case of a prescribed person (per *PHIPA*, s. 39(1)(c)); or, in the case of a prescribed entity, for the purpose of analysis or compiling statistical information with respect to the management, evaluation, or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services, provided certain other requirements are met (per *PHIPA*, s. 45(1)).

formally approved and reviewed every three years by the Information and Privacy Commissioner of Ontario. Bodies authorized as prescribed persons or as prescribed entities under *PHIPA* include the Canadian Institute for Health Information, the Institute for Clinical Evaluative Sciences, and Cancer Care Ontario.

Data warehouses outside Ontario include Population Data BC (a resource holding individual-level, de-identified longitudinal data on British Columbia's four million residents), the Newfoundland and Labrador Centre for Health Information (a Crown corporation established to integrate and house data from all components of that province's health and community services systems), and research institutes affiliated with universities, such as the Population Health Research Unit at Dalhousie University in Nova Scotia, the Centre for Health Services and Policy Research at the University of British Columbia, and the Manitoba Centre for Health Policy, affiliated with the University of Manitoba's Faculty of Medicine. Data warehouses with special status under provincial legislation are authorized to handle and prepare raw data for secondary use, subject to strict protocols and ethics review mechanisms to limit access to identifiable data to authorized individuals, and to ensure that proper data management practices are in place.[30]

Privacy and Security Training

Comprehensive privacy and security training is another important component of a framework for privacy-protective secondary uses in the EHR environment. Ongoing privacy and security training and awareness can help to reduce the frequency of human error and carelessness that is often the cause of many privacy breaches.

Training can help to ensure that employees and agents are aware of their obligations under privacy statutes and organizational privacy and security policies and procedures applicable to the authorized collection, use, and disclosure of personal health information and the safeguards that must be implemented to protect the personal health information with which they have been entrusted.

Privacy and security training in the context of secondary use raises additional issues. Secondary users will require specialized, and role-based, training that reflects the nature of the secondary use and the relationship of secondary users with the data custodians from whom they receive personal health information for secondary purposes. There is also the question of responsibility for training secondary users. These matters and others may be addressed in the data disclosure agreements that set out the conditions for specified secondary uses.

Data Breach Policies and Procedures

Many jurisdictions in Canada and individual organizations dealing with personal health information have already established data breach policies and procedures to address the identification, reporting, containment, notification, and investigation of data breaches. Such policies and procedures can help to prevent breaches,

30 Willison, *supra*, note 8, p. 22.

ensure an expeditious and coordinated response to any breaches that may occur, clarify the roles and responsibilities of employees and agents in dealing with data breaches, and minimize the damage from any breaches that do occur.

Data breach policies and procedures should also specifically address the roles and responsibilities of secondary users, who may or may not be employees and agents of the data custodian, in dealing with breaches that arise. For example, data breach policies that call for the notification of individuals whose personal health information has been breached may not be appropriate in the case of a breach by a secondary user with no direct relationship to those individuals. In that case, the data breach policy could call for secondary users to notify the data custodian, who can then take steps to notify the affected individuals. Data disclosure agreements governing the relationship between the secondary user and the data custodian should also provide clarity on the application of a custodian's data breach policies and procedures to secondary users.

Additional Issues for Discussion

We have discussed a number of elements of a governance framework for privacy-protective secondary uses in the EHR environment. These elements are either already in place, or are available but need to be more comprehensively adopted. There remain, however, other issues to be resolved and a number of elements to be considered for future implementation. There are also questions concerning how to effectively manage differences in legislation and in policies and procedures governing secondary use between provinces and territories, within a single province or territory, and even among healthcare providers themselves.

While some guidance is provided in the Common Understandings paper, critical decisions have yet to be made on what an overall governance structure for secondary use in the EHR environment will look like. For example, more clarity is needed in the area of accountability. Whether it is a shared record or an EHR repository, it is important to know who is accountable for the record, who the custodian is, what the custodian's responsibilities are in relation to the record and for notifying individuals of potential uses of the record, what authorizations the custodian has to disclose information from the record, and what conditions must be met for the disclosure of information for a secondary purpose.

More efforts are also required to achieve transparency about existing and future secondary uses in the context of the EHR. The approval and registration of data repositories, for example, may serve as a means of not only systematically documenting their existence but of applying common criteria as to who may develop and manage these data repositories and under what conditions.[31] In addition, a reporting structure could be developed by which the public and potential secondary users can be notified of the existence of data repositories, including through online posting of a list of these repositories, and by which they may be

31 Ibid, p. 23.

notified of any uses and disclosures made. For example, a registry may be created to publicize, on an ongoing basis, the existence and nature of research studies using information in the EHR and the results of this research.[32]

Another challenging issue is that of consent approaches to secondary use in the EHR environment. Some commentators have proposed alternative approaches to consent, recognizing that conventional consent models calling for either full project-specific consent or exemptions from consent fit poorly with the broader range of potential future uses made possible by the EHR. Policy alternatives have been proposed ranging from removing consent requirements altogether, to broadening exemptions for consent, to retroactively deeming consent, and to broad generalized consent for all future and as-yet-unspecified uses and disclosures.[33] Another proposal is for a tiered consent model that would apply different default consent options for different types of secondary uses depending on the nature of the use, the societal benefit of the use, the risks to the individual, the potential for commercialization, and other factors.[34]

Although a practical, workable model has yet to emerge, the debate surrounding this issue is critical as it will inform the future of secondary use. Further, even if the policy approach ultimately adopted for secondary use is consent-based, at a practical level, the issue remains of how the EHR will record individual consent preferences for secondary use, including for future purposes that may not yet be defined. A Canada Health Infoway project on consent management anticipates that the EHR may be used to record consent for research in the future, and consequently has identified it as a business and architectural requirement of any consent management solution.[35] Another option could be the use of patient portals or other electronic means to enable individuals to document and register their preferences regarding secondary use and to be notified of any such uses. Moreover, digital rights management technologies may be implemented to control the duration of consent for secondary purposes and to circumscribe the conditions under which the individual consents to the use and disclosure of his or her information for secondary purposes. One future model for achieving ultimate control of personal information is the "SmartData" model created by Dr. George Tomko at the University of Toronto.[36]

There are also calls for a fundamental reconsideration of certain concepts in the new EHR environment. Some have called for the re-conceptualization of current distinctions made between primary use and secondary use, and between

32 Kosseim, *supra*, note 9, p. 24.

33 Ibid, pp. 20-43.

34 Caulfield et al. and Singleton et al., cited in Willison, *supra*, note 8, pp. 9, 18-21; Kosseim, *supra*, note 9, p. 45.

35 Canada Health Infoway, *Business and Architecture Considerations for Interoperable Consent Solutions, a discussion document* (forthcoming).

36 SmartData involves the use of embodied, virtual agents in IT systems that will act as an individual's proxy online, securely storing one's personal information and intelligently disclosing it based on one's personal criteria for disclosure. SmartData would permit the disclosure of information based on the context of data requests, in accordance with instructions authorized by the data subject. See Tomko, George J. et al., *SmartData: Make the data "think" for itself* (2010) 3:2 *Identity in the Information Society* 343. Available online at: http://www.springerlink.com/content/1883257206825632/fulltext.pdf.

certain types of secondary use, such as research and quality improvement. Some writers propose that health research, typically considered a secondary use, be re-conceptualized as a primary use because of the relationship between the health of individuals and of populations, and between publicly-funded health care and publicly-funded health research. They note that progress in information technology, genomics, and other fields have contributed to rapid advances in health care, making it increasingly likely that individuals may see direct benefits to themselves or to their families within their lifetimes as a result of participation in research.[37] Similarly, the distinction between research and other secondary uses such as systems planning and quality improvement, which do not require consent and attract a lower level of ethics scrutiny, is being challenged.[38] Some commentators have noted that current models for authorizing research remain largely geared towards discrete research studies with defined research goals that can be tied to specific data collections, which may not readily apply to data holdings in the EHR that can serve as research platforms for a wide range of possible uses.[39] It has also been argued that variations in research rules[40] and in decisions of research ethics boards across the country[41] create inconsistency and uncertainty, which may hamper progress towards using interoperable EHR systems for inter-jurisdictional research.

As single-purpose research projects give way to the development of data repositories that will serve as platforms for a variety of future secondary uses in the EHR, some have called for the dissolution of boundaries between different kinds of secondary purposes. Along with this suggestion are calls for the implementation of a common, proportionate approach to ethical review of all secondary uses, depending on the level of risk posed to those whose information is the subject of such uses.[42]

Addressing these issues and many more requires the ongoing input of all stakeholders, including legislators, policymakers, healthcare providers, secondary users, system designers, and most importantly, the public, as part of a national conversation about how the framework for secondary use in the EHR context should evolve. It will also require the adoption of *PbD,* which is sufficiently flexible to respond to new issues as they arise, in order to protect individual privacy while enabling appropriate secondary use.

37 Kosseim, *supra*, note 9, pp. 31-35; Willison, *supra*, note 8, pp. 15-17.

38 Willison, *supra*, note 8, pp. 7-8.

39 Willison, D., *Data Protection and the Promotion of Health Research: If the Laws Are Not the Problem, Then What Is?* (2007) 2:3 *Healthcare Policy* 39, pp. 40-41.

40 Kosseim, *supra*, note 9, p. 36.

41 Willison, *supra*, note 8, pp. 9, 24.

42 Ibid, p. 16.

Conclusions

We have seen how the very features that make EHRs valuable tools for modernizing information systems in the health sector also present challenges to maintaining the privacy and confidentiality of personal health information contained in these systems. In spite of these challenges, we recognize the value of harnessing the power of EHR systems to enable faster, safer, and more powerful uses of information for both primary and secondary uses.

The long-term project of deploying a common, interoperable EHR is well underway. Canadian provinces and territories are at various stages of implementing the components that will make up their EHR systems. With the increasing adoption of information technologies, and greater awareness of the benefits of using electronic information for health care and other purposes, we can anticipate growing numbers of data repositories, more data integration, and increased requests for access to electronic information for broader purposes.

Continued support for secondary use in the interoperable EHR environment will depend on the ongoing development of a governance framework that supports appropriate, coordinated, and privacy-protective secondary uses of electronic health information, both within and across jurisdictions. While we have argued that many elements of this framework are already in place, the national discussion on a clear and coherent framework to enable continued secondary use must continue. This discussion should be premised on an essential feature – the default condition should be one in which only de-identified information is used or disclosed for secondary purposes, and, where de-identified information is insufficient, additional safeguards must be put in place prior to the use and disclosure of personal health information for secondary purposes. This discussion must take place sooner rather than later, to ensure that everything that can reasonably be done, will be done, to ensure continued secondary use in the most privacy-protective manner possible – positive-sum, win/win.

Information and Privacy Commissioner of Ontario
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8
Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

Canada Health Infoway
1000 Sherbrooke St. W.
Suite 1200
Montreal, Quebec H3A 3G4
Web site: www.inforway-inforoute.ca

March 2, 2012

Information and Privacy Commissioner, Ontario, Canada

Canada Health Infoway / Inforoute Santé du Canada