Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

SPECIAL REPORT

A Prescription for Legislative Reform

Improving Privacy Protection in BC's Health Sector

APRIL 30, 2014

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

The purpose of this special report is encourage an informed dialogue among the public, health practitioners, researchers and government about the use of personal information in B.C.'s health care system, today and into the future.

This dialogue is urgently needed. New technologies and cutting-edge research are creating opportunities to improve patient care, while also making our health care system more efficient. It is in our collective interest to seize these opportunities, and the prospect of better health outcomes for all British Columbians.

These opportunities must be met with an investment in robust privacy protections, including a strong legislative framework to protect personal health information. Citizens have entrusted researchers, practitioners, and government with their sensitive health information – they have an expectation their data will be treated with care and respect.

B.C.'s current legal framework for the use of personal health information is increasingly strained in the digital era. The current laws have developed incrementally over the years, and are spread across many statutes. The result is a complex web of rules and regulations that are, in some cases, difficult to understand and result in a lack of transparency for the public about how their information is being used or shared.

Doctors treat the whole patient and not a specific condition; similarly, government needs to take a holistic approach to the collection, use, disclosure and protection of personal health information and patient data by introducing a health information law with clear and consistent rules for the public and the private sector.

In this report I have made 21 recommendations to ensure B.C.'s health information and privacy laws are up to the challenge.

In this time of innovation and change, we have the opportunity to embrace the potential to improve patient care and promote vital health research, but also to make a lasting investment in protections against inappropriate use of data, and improper access. Privacy, health care and research are not are not at odds; rather they are equally necessary for continued public trust and confidence in the health care system.

It is my hope that my prescription will stimulate dialogue, legislative action and meaningful reform.

EXECUTIVE SUMMARY

Personal health information is viewed by most British Columbians as being very sensitive, since it can convey extensive information about the personal situation of each citizen. Whether the information is about our most recent lab results or genetic information, it is generally volunteered for the purpose of receiving health services with the expectation that the personal health information will be protected.

In the age of paper records held only by our doctor's offices or our local hospital, protection of this information rested largely on the high ethical standards for patient confidentiality practised by health care professionals.

However, as with other sectors, the health care sector is undergoing significant changes due to digitization. Electronic records are becoming the norm, and a large volume of digitized personal health information is collected, stored, used and disclosed throughout the health care system – much of it stored in large databases.

New developments such as digital health, whole genome sequencing and big data present new opportunities to improve a patient's quality of life, and over the long-term, better health outcomes for all British Columbians and increased efficiencies in the health care system. They also present challenges for the protection of privacy.

The current legal framework to protect the data flows in the health sector has not kept pace with the new digital reality. B.C.'s current privacy laws of general application lack clarity and consistency, and are not tailored to the unique nature of personal health information and how it is managed in the health sector. Other narrow provisions scattered in various pieces of health legislation are targeted at specific data flows and are thus fragmented and confusing.

This report recommends that the Government of BC enact a comprehensive health information privacy law, with clear and consistent rules for the public and the private sector. The report makes 21 recommendations in relation to new health privacy law that would ensure B.C. can embrace the opportunity of technology and innovations in health research, while also protecting personal health information.

Specific recommendations include:

- Requirements for custodians to collect only the minimum amount of personal health information needed for specified purposes, ensure the accuracy of personal health information and institute privacy management programs;
- In relation to large electronic health record systems implemented by the Ministry of Health or health authorities, requirements for notification to the individual, role-based access, choices about who can access records (masking) and audit logs;

- In relation to health research, the establishment of a single research ethics board, a data stewardship committee responsible for ensuring a consistent approach to data access and specific authorities for disclosures to the Canadian Institute of Health Information and organizations like Population Data BC;

- In relation to individuals, rights to have access to their own personal health information and request correction;

- Significant fines for non-compliance; and

- Oversight by the Commissioner, including mandatory review of privacy impact assessments and breach notification.

The Commissioner urges government to fill her prescription for legislative reform at the earliest possible opportunity.

INTRODUCTION

Personal health information that is collected by health care providers in the delivery of health care is extremely sensitive. Arguably, it is the single most sensitive type of personal information. It encompasses information about:

- the physical, mental and emotional status of individuals over their lifetime;
- lifestyle and behaviour;
- health conditions and concerns;
- history of health care procedures and medication use;
- results of medical tests;
- related information about family members and other individuals; and
- genetic information about individuals and their blood relatives.

A vast volume of such personal health information is collected, used and disclosed throughout the publicly-funded health care system in BC. Much of it is stored in very large databases. The size of these databases means that the potential magnitude of a privacy breach is much greater than in the days of paper-based records. Thousands, or even millions, of individuals could be affected by a single breach. Examples of such large-scale breaches have occurred in BC and are reported almost every week somewhere in the world.

Personal information is only disclosed by individuals to receive health services on the understanding that it will be protected. For this reason, one of the hallmarks of health care is that strict ethical standards regarding patient confidentiality have developed to govern the practice of health professions. This has resulted in an assumption by individuals that they can trust their health care providers to consistently maintain a proper degree of privacy protection.

Given these characteristics of personal health information, health sector privacy is considered to be unique—and robust privacy protection is recognized as being of great importance to British Columbians.

In Canada, privacy is recognized under the *Canadian Charter of Rights and Freedoms* as a component of the fundamental rights of the individual in a free and democratic society. Consistent with this, the legislative protection of personal information has become a legal responsibility of governments. Because of public expectations for privacy of their records, legislators have, over many years, enacted various legislative provisions in an attempt to ensure appropriate collections and use of this information.

Health information privacy laws have also spread internationally in recent years. In relation to the health sector, there are distinct or stand alone privacy laws that establish special rules to protect health information. In Canada, all provinces have health information privacy legislation in one form or another that is tailored specifically for that sector. These laws are intended to enable information flows necessary for the delivery of health services and management of public health, as well as permit appropriate secondary use such as billing and health research.

At the same time, and of equal importance, is the public interest in establishing appropriate privacy and security frameworks to regulate these information flows. It is important to remember that Canada's courts have recognized that health information is not "owned" by health custodians or governments; rather it is held in trust and used in accordance with law, policy and ethics.

New developments challenge the effectiveness of the current laws. The health sector is evolving at a rapid pace. For one thing, like other sectors, the health sector has undergone an IT revolution—we are in an age of e-health, with digitized and readily shareable records becoming the norm. For example, the provincial electronic health record system enables access to a tremendous amount of personal health information at various points of service throughout the BC health sector.

Further, new models of primary health care are evolving, incorporating inter-disciplinary practice and cross-sector linkages which reflect the social determinants of health (such as income and education). Even the types of personal health information are expanding to include such things as tissue samples preserved in biobanks and the results of whole genome sequencing for individuals.

Another significant change is that we are seeing a cultural shift away from a health care system that focuses on health care providers treating illness and disease to a system where individuals manage their own health care as part of a multi-disciplinary care team promoting wellness and managing chronic conditions. As well, largely as a result of new technologies such as patient portals, consumer health solutions and mobile health, individuals are becoming empowered to assume responsibility for their own personal health information.

There is also increasing pressure on data stewards who have custody or control of personal health information to make large collections of enormous and complex data sets, or big data, available for health research purposes. Big data analytics are seen as having tremendous potential to further knowledge about prevention and wellness and the efficacy of treatment modalities. Because of this, repositories of big data have become "honey pots" for health researchers and data stewards are being called upon to streamline their data access approval processes.

In recent months, this Office has devoted time and effort to address concerns regarding the disclosure of personal information to health researchers. Following a significant privacy breach at the Ministry of Health, we published an investigation report in June 2013 making recommendations to the Ministry regarding disclosure within, and externally from, the Ministry for health research purposes. This Office also hosted roundtable discussions on health research in 2012 and 2013 in an attempt to build consensus among data stewards and health researchers on appropriate privacy and security frameworks for the disclosure of personal information for health research purposes.

As discussed below, BC has a mixture of old and new legislative provisions spread out among several statutes. They are difficult to understand because they establish privacy rules that are, in places, opaque, complex, inconsistent and incomplete. This patchwork is also out of step with most other provinces in Canada which have comprehensive stand-alone health information privacy statutes. Increasingly, we are seeing a desire for inter-operable electronic health record systems across jurisdictions in Canada and the establishment of national registries. A comparable pan-Canadian approach is therefore desirable.

This Special Report is divided into three parts. Part 1 is a description of BC's health sector today. Part 2 is a critique of BC's current health information privacy laws. Part 3 is a prescription for health information privacy law reform.

PART 1: THE DYNAMIC HEALTH SECTOR

This Part highlights how new technologies and patient expectations are changing the delivery of health services in BC and creating the opportunity for better health outcomes and more efficiencies in the health care system.

☐ e-Health

The term "e-health" refers to information technology, particularly internet technology, which supports healthcare delivery.[1] The term is usually used in relation to digitized records.

The advent of e-health initiatives is a relatively recent phenomenon which is happening internationally. Canada, the United States, the United Kingdom, Denmark, Norway, Australia and New Zealand have all recognized value in creating electronic health

[1] BC eHealth Strategy Council, *British Columbia's 2010/11-2012-13 Provincial Health Sector Information Management/Information Technology Strategy*, 2011. Available online at: http://www.health.gov.bc.ca/library/publications/year/2011/Health-sector-IM-IT-strategy.pdf.

records that are capable of being shared across the health sector.[2] The common goal of e-health in all of these countries is streamlining the flow of health information in order to improve quality of care and service delivery, thereby reducing inefficiencies and costs.

In the United States, for example, health information technology was a key component of President Obama's 2009 stimulus package. Among other things, the package promoted the adoption of electronic health records by care providers and hospitals.

E-health in BC is fragmented and diverse and reflects the nature and scale of the health care system, which has both publicly-operated and privately-run components. The Ministry of Health, health authorities, hospitals, clinics, labs, pharmacies and private service providers (physicians, physical therapists and others) all deliver health services with personal health information flows across the various components.

Health authorities in BC each have their own electronic health records (EHR) systems.[3] In addition, there is a provincial EHR system which is a relatively recent initiative of the Ministry of Health and is still in progress. It will ultimately include the following repositories:

- PharmaNet (all prescriptions dispensed in the province and ePrescribing);
- Client Registry and Enterprise Management Patient Index (contact information and Personal Health Numbers for all individuals receiving publicly-funded health services);
- Provider Registry (registration information about all physicians, pharmacists and registered nurses in the province);
- Provincial Laboratory Information Solution (lab results from both public and private sector labs);
- Provincial Diagnostic Imaging Viewer (diagnostic images from both public and private sector imaging facilities); and
- Panorama (public health information).

[2] Canada Health Infoway. *Vision 2015 – Advancing Canada's next generation of healthcare.* Toronto: Canada Health Infoway; 2010. Available: https://www.infoway-inforoute.ca/.
[3] For example, the Vancouver Coastal Health Authority has eight core electronic information systems.

The following graphic illustrates this goal:

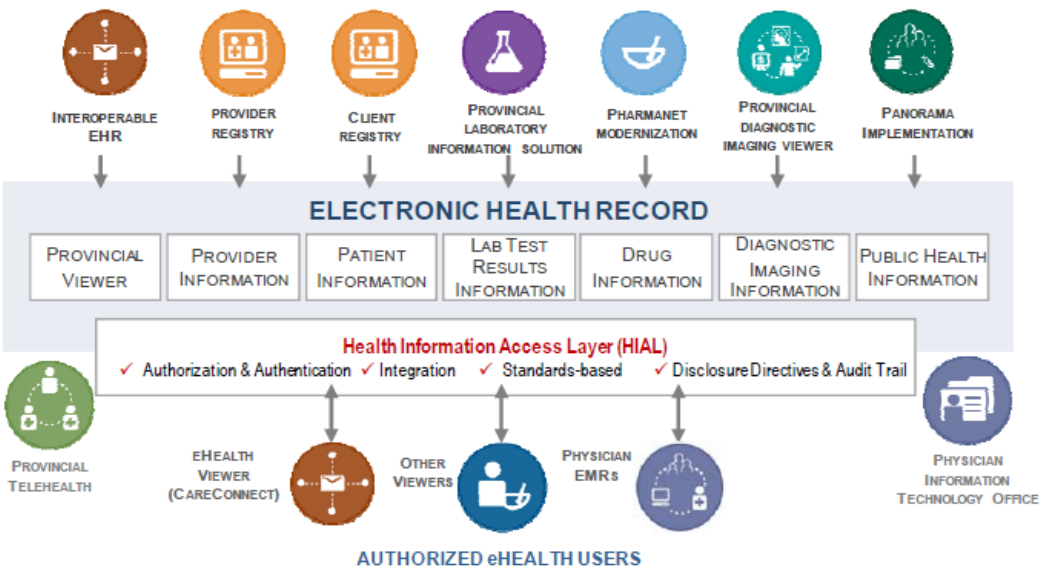

Figure 1: eHealth Overview[4]

In addition to the EHRs, there are increasing numbers of physicians replacing their paper files with electronic medical records (EMRs).[5] This provides opportunities for EMR and EHR integration such as the current roll-out of the Provincial Laboratory Information Solution to physicians' offices.

Apart from the EHR, the Ministry of Health has a number of other databases, including:

- discharge abstract database (patient-related hospital data such as admissions and discharge summaries);
- fee for services claims (health care providers' fee for service claims payment under the Medical Services Plan); and
- mental health and addictions minimum reporting requirements (data from health authorities regarding community mental health services delivered to individuals).

[4] Ministry of Health Services. *eHealth Quarterly Status Report: October-December, 2011.* Available: http://www.bcauditor.com/files/publications/2010/report9/files/ehealth-executive-report-december-2010.pdf

[5] There is funding for EMRs through the Physician Master Agreement which is administered by the Physician Information Technology Office established by the BC Medical Association and the Ministry of Health.

These databases are compiled within an integrated data warehouse (known as Health*ideas*) for analysis purposes. The Ministry of Health also discloses information from its databases to Population Data BC and to the Canadian Institute for Health Information for research purposes.

The Provincial Health Services Authority, which is a public body, maintains chronic disease registries such as:

- BC Cancer Registry;[6]
- BC Renal Agency's Patient Record and Outcome Management Information System ("PROMIS");[7] and
- BC Perinatal Database Registry (clinical information on all births collected from obstetrical facilities).[8]

It also has a Surgical Patient Registry which prioritizes surgeries and tracks patients waiting for surgery.[9]

There is one provincial registry that is linked to national transplant registries maintained by Canadian Blood Services.

☐ Changes in service delivery

The delivery of health services is becoming increasingly interdisciplinary as a result of changes in primary health care models. Moreover, increasing recognition of the social determinants of health and the need to coordinate services to individuals with multiple needs are driving cross-sectoral service delivery models in government.

There is also an increasing acceptance and integration of complementary practitioners. There is a greater interest in, and demand for, preventative and holistic health care which means individuals are receiving services from a variety of practitioners.

At the same time, scopes of practice are expanding. Pharmacists are now able to administer injections, provide emergency prescription refills, renew and extend prescriptions, and change drug dosages.[10] Since nurse practitioners were first

[6] http://www.bccancer.bc.ca/HPI/CancerStatistics/default.htm#bccanreg.
[7] http://www.bcrenalagency.ca/professionals/promis/default.htm.
[8] http://www.phsa.ca/AgenciesAndServices/Agencies/perinatalservicesbc.htm.
[9] http://www.phsa.ca/AgenciesAndServices/Services/Surgical-Services/BC-Surgical-Patient-Registry/default.htm.
[10] Canadian Pharmacists Association, *Summary of Pharmacists' Expanded Scope of Practice Activities across Canada.* 2012. Available online at: http://blueprintforpharmacy.ca/docs/pdfs/pharmacists'-expanded-scope_summary-chart---cpha---oct-29-2012.pdf.

introduced in BC, their scope of practice has been expanded in relation to diagnoses and admission to mental health facilities.[11]

There are also new and emerging health care practitioners such as personal trainers and health coaches who advise individuals on how to manage their chronic health conditions.

Another way in which models of care are changing is through new modes of communication. Technological advances are making it easier for health professionals to communicate with their patients or clients. The Ministry of Health reports that, TeleHealth, which includes TeleHomecare, TeleOpthamology, TeleThoracic, and TeleOncology, is 100% complete.[12] Individuals can connect with their health care providers via on-line video visits, email and instant messaging services.

The Ministry of Health has also developed a provincial home health monitoring solution where individuals with certain chronic health conditions are provided with a tablet computer and a variety of devices that collect health data. The data is then transmitted to care providers for assessment and monitoring.

☐ Cultural Shift

There is a distinct cultural shift in the health care sector away from a paternalistic model towards increasing involvement of individuals in their own health care. Just over 20 years ago, it took no less than the Supreme Court of Canada to decide that an individual is entitled to examine and copy their own medical records in a physician's office.[13] Since then, there has been a trend towards individual control over personal health information. We now see individuals not only viewing, but in some cases actively contributing to, their own health records.

Access to one's own health records helps many individuals manage their own health care. An example of the changing role of individuals in managing their health care is the "Patients as Partners" policy and philosophy of the Ministry of Health. The guiding principle is "nothing about me without me", which underscores the belief that patients should collaborate with health care professionals both in their individual health care and also in how health care is delivered in the province.[14]

---

[11] British Columbia Medical Association, *Policy Statement: Nurse Practitioners.* 2012 available online at: https://www.bcma.org/files/WEB%20Nurse%20Practitioners.pdf.

[12] Ministry of Health Services. *eHealth Quarterly Status Report: October-December, 2011.* Available: *http://www.bcauditor.com/files/publications/2010/report9/files/ehealth-executive-report-december-2010.pdf*.

[13] *McInerney v. MacDonald*, [1992] 2 S.C.R. 138.

[14] http://www.impactbc.ca/patients-as-partners.

☐ Tools for personal health management

A wide range of tools, applications and electronic solutions now allow individuals to actively participate in their health management. Applications that allow individuals to track and manage their health care, mobile health technologies, and personal genomic services are all evidence of the trend toward patients being active participants in their health care.

☐ Patient Portals

Patient portals allow individuals to access their health information and are becoming more prevalent and more interactive. These platforms can facilitate direct electronic communication with care providers and enable individuals to do things like book their own appointments and request prescription renewals. There are a number of patient portal projects implemented in BC. Examples include Health eGateway at a medical clinic in Vancouver and myeHealth at Excelleris.

The degree of interaction between patient portals and EMRs varies. Some are directly "tethered" or connected to the patient's EMR and allow the individual to see a virtual copy of their EMR. Others are linked with specific aspects of the EMR such as lab results. Some patient portals may include a personal health record component which allows patients to manage their health through tools such as journals and lab result charting.

There is some debate among health care providers about how much information should be shared with individuals, and the impact of sharing on how physicians conduct their practice. For example, the information and opinions that physicians may or may not include in case notes when they know that those notes will be accessed by the patient. Many agree that this shift will have an impact on the practice of medicine.

Were an individual to print a record they have accessed through a patient portal, they would assume control of that record. Individuals may permit family members or other caregivers to also access their personal health information through a patient portal. In that case, individuals are exercising powers similar to those of a custodian because they are authorizing the disclosure of their own personal health information to a third party. Presumably, they also set the terms and conditions under which they have given access to their family members or other caregivers.

☐ Personal health management applications

Applications like Microsoft's Health Vault, or Telus' HealthSpace in Canada, allow individuals to collect, store and share their health information and that of their families.[15] These products are meant to help people get a complete view of their

[15] http://telushealthspace.com/en/telushealthspace.

health status and needs, prepare for doctor's visits and set and achieve fitness goals.[16]

When individuals use this type of consumer health product, they become responsible for protecting their own personal health information. Should there be a privacy breach, individuals would have no recourse except in a civil action through the courts. Privacy laws do not apply to individuals and Privacy Commissioners do not have jurisdiction over the actions of individuals. This means that individuals have the responsibility to be aware of the privacy risks of using consumer health solutions and to take steps to mitigate them.

The concept of individuals being responsible for their own personal health information is something new in the health care context. Traditionally, health care providers or hospitals and clinics have had custody and control of personal health information. The trend towards individuals assuming responsibilities for their own personal health information reflects the evolution we are seeing towards greater involvement by individuals in their own health care. All of the privacy implications of this are still unfolding but it seems reasonably clear that responsibility for ensuring the accuracy, integrity and currency of records becomes that of the individual the information is about.

☐ Health management applications offered by employers

Some employers are providing health tracking tools and encouraging employees to get more involved in their own health management. The BC Public Service Agency offers My Good Health which encourages employees to answer a series of health-related questions and then offers information, tools and resources designed to target current or potential health concerns.[17] In this case, the individual the information is about and the third party vendor who is storing the information share responsibility for protecting the personal information.

☐ Mobile health

There is a new market for devices that allow individuals to monitor their own heath. The intersect between mobile devices and personal health monitoring is referred to as mHealth (mobile health). mHealth includes a plethora of devices and applications ranging from those that offer simple reminders of medication or appointment times, to medical devices that can link with a smart phone to measure, track and transmit information such as blood pressure and blood glucose.[18] Other common mHealth devices allow individuals to monitor and share their daily activity, sleep patterns and

[16] http://telushealthspace.com/en/telushealthspace.
[17] http://www2.gov.bc.ca/myhr/article.page?ContentID=5d96706a-1cec-3c5b-1d1f-55f51ecb94f9.
[18] http://www.ihealthbeat.org/articles/2013/4/2/more-doctors-starting-to-prescribe-mobile-apps-for-chronic-conditions.aspx.

eating habits. Examples include the Fitbit,[19] Nike+ FuelBand[20] and Jawbone Up,[21] to name just a few.

☐ Personal genomics

A growing number of companies offer various genotyping services direct to consumers. These services include tracing ancestry, building family trees and even genetic screening. 23andMe offers to compare an individual's DNA against approximately one million genetic variants, providing ancestry results for only $99.[22] The company's research arm, 23andWe, gives individuals the opportunity to contribute their data to a number of research projects.[23]

There are also large-scale health research projects in many countries that involve the collection of whole genome sequencing data. In Canada, the Personal Genome Project spearheaded by the McLaughlin Centre of the University of Toronto and the Hospital for Sick Children in Toronto is, with consent, placing individuals' genome sequencing in an online database, allowing it to be used in any number of research projects.

☐ Tele-monitoring by manufacturers of implants

Manufacturers of implantable devices such as an implantable cardioverter defibrillator remotely monitor patients. If there is a concern (for example, fluids building up inside a chest cavity), a physician can receive an alert from the manufacturer. Over time, the manufacturer will have collected a lot of personal health information about individuals.

☐ Big data and analytics

EHRs and technological advances in storage of and access to information (including through cloud-based services) contribute to the health sector generating vast volumes of information. The growing pool of raw information is referred to as big data. The process of mining that data is data analytics. Often the term big data is used interchangeably to refer to the information and the analytics. The potential benefits of big data and the answers that analytics can provide are predicted by some as being immense. Big data is seen as a powerful tool for tracking, evaluation and research. The benefits of big data may be realized in the areas of disease prevention and treatment as well as health care delivery.

In disease treatment and prevention, for example, big data could allow the tracking, on a large scale, of how many patients receive a particular vaccine or how many people affected by a disease have their symptoms under control.[24] It could identify patterns

---

[19] http://www.fitbit.com/.
[20] http://www.nike.com/ca/en_ca/c/nikeplus-fuelband.
[21] https://jawbone.com/up.
[22] https://www.23andme.com/howitworks/.
[23] https://www.23andme.com/research/.
[24] http://medcitynews.com/2013/03/four-types-of-healthcare-analytics-that-providers-are-using-to-improve-population-health/.

and predict future outcomes, such as hospital re-admittance or medication compliance. Big data could also provide useful comparative information that enable health care providers to prioritize and focus their attention where it is needed or allow health care facilities to detect high level patterns and trends.[25]

Technological advances coupled with big data analytics allow for whole new realms of research. For example, a University of California San Francisco research study will use smartphones and mHealth devices and applications to engage one million people in a decade-long heart health study.[26] This study will be the first wide-ranging health study linking smartphone technology and health science to amass data and then develop models that predict and slow heart disease.[27]

Big data presents challenges in terms of privacy principles related to consent for collection and secondary use. These principles are discussed further below.

PART 2: BC'S CURRENT HEALTH INFORMATION PRIVACY LAWS

Given these rapid and wide-ranging changes in the health sector, how do BC's health information privacy laws address the privacy issues that they raise? As the following analysis clearly demonstrates, they do not, simply stated, meet the current and coming challenges.

☐ The patchwork of laws

Privacy laws of general application protect health privacy in the BC health care system. The *Freedom of Information and Protection of Privacy Act* ("FIPPA") applies to some 2900 public bodies in the public sector, including the Ministry of Health, health authorities, hospitals and professional regulatory bodies. The *Personal Information Protection Act* ("PIPA") applies to organizations operating in the private sector, including private labs as well as private health care providers or services, such as physicians, dentists, pharmacists, diagnostic imaging facilities and laboratory facilities.

These pieces of legislation do not always work well together in the integrated health sector. In some instances, they do not permit what most would regard as appropriate information flows among all of the players. We have seen this, for example, in relation to data flows through Excelleris, an organization governed by PIPA which distributes lab results to physicians' offices and health authorities. The consent requirements in PIPA make it problematic for health authorities to find clear legal authorities for every information flow.

---

[25] http://medcitynews.com/2013/03/four-types-of-healthcare-analytics-that-providers-are-using-to-improve-population-health/.
[26] https://www.health-eheartstudy.org.
[27] http://www.ucsf.edu/news/2013/03/13695/study-uses-mobile-technology-help-predict-and-prevent-heart-disease.

In addition to FIPPA and PIPA, there are health information privacy provisions scattered among other pieces of health legislation. These have been enacted in a piecemeal fashion. A list of key pieces of the patchwork is set out in Appendix A of this report. These include the *Pharmaceutical Services Act*, the *Public Health Act*, the *Ministry of Health Act* and the *Medicare Protection Act*. Not all of the information provisions in these statutes provide an adequate legal framework for the protection of the personal health information that is being collected under the authority of those statutes. Taken together, they represent a fragmented legislative framework for the protection of personal health information.

For example, the *Ministry of Health Act* was amended in 2010 to authorize the Minister of Health to collect personal information from any public body for a "stewardship purpose" and use or disclose personal information to any public body. A stewardship purpose is broadly defined to include program evaluation under a health enactment; health systems planning, maintenance or improvement; research into health issues; and monitoring or evaluating a health care body. It also includes a "prescribed purpose" which means that other purposes could be added by regulation.

Most British Columbians would be surprised to learn that the Minister of Health has such a broad discretion to collect, use and share their personal health information. This authority likely does not reflect the reasonable expectations of British Columbians when it comes to the privacy of the personal information they disclose in order to receive health services, even if they are publicly-funded services. They would also surely agree that their personal health information should not be subject to a lesser standard of privacy protection. Given the Minister's broad statutory authority, there are not adequate checks and balances in place to provide proper oversight to ensure the Minister is only collecting the minimum amount of personal health information that is necessary.

There is only one section in the *Medicare Protection Act* (s. 49) which protects the personal information collected for the purposes of the Medical Services Plan (MSP). Section 49 is a blunt tool at that. It merely creates a duty of confidentiality respecting information acquired in administering the Act, yet also creates a number of exceptions to that duty including disclosure for broad health-related purposes. Given the sensitivity of personal information related to medical services delivered to individuals, the lack of legal requirements for a robust privacy and security framework for MSP databases is troubling. It is also not something British Columbians would necessarily find acceptable moving forward into the era this report describes.

A more transparent privacy and security legal framework for designated databases of the Ministry of Health and health authorities has been set out in the *E-Health (Personal Health Information Access and Protection of Privacy) Act (*"E-Health Act"). This Office supported the E-Health Act when it was introduced in the Legislature. Since it came into force, however, the Act has been under-utilized. For no clear reason, it has only been applied to three of the numerous personal health information databases to which it

could, and should, apply, the Provincial Lab Information Solution (a repository of lab results in the provincial EHR), the Client Registry and the Provider Registry.

Other e-health databases, such as diagnostic imaging and Panorama, are governed by FIPPA and, in the case of Panorama, also by the *Public Health Act*. Yet another piece of legislation, the *Pharmaceutical Services Act*, governs PharmaNet. This Act repealed and replaced the *Pharmacy Operations and Drug Scheduling Act* in 2012. It has some privacy protective provisions in relation to PharmaNet but is not as comprehensive or robust as the E-Health Act.

Amendments were made to the E-Health Act in 2012 but none appear to relate to any issues that have arisen in the application of the Act. Recently, government decided to continue to govern PharmaNet in separate legislation rather than designate PharmaNet as a health information bank under the E-Health Act. Again, the policy reason for doing this is unclear.

Still other pieces of the legislative framework that relate to specific entities within the health sector could be characterized as antiquated and anomalous. For example, the *Health Act* authorizes the BC Cancer Agency to request prescribed information from any person for the purposes of medical research.[28] A person to whom a request is made must comply with the request in the manner and at the times requested. Information that may be requested includes records from labs, imaging services, hospitals and other health facilities and physicians, as well as mortality and morbidity data, including autopsy reports.[29] A person aggrieved by a request has to go to the Supreme Court of British Columbia for a review of the request, rather than to this Office which normally exercises oversight in relation to these matters. The BC Cancer Agency is also authorized to disclose information for the purpose of medical research. This authority is very broad and does not include any rules to protect privacy.

The BC Cancer Agency has voluntarily implemented a process designed to protect privacy, but it is not legally required. For reasons of certainty, transparency, consistency and even efficiency, the BC Cancer Agency should be required to comply with the same requirements as other public bodies involved in health care. The need for consistent, and expert, oversight is also clear, with this Office and not the Supreme Court as the regulatory body.

As a final example of many possible examples, the *Hospital Act* states that a record regarding a patient that is prepared in a hospital by an employee or by a practitioner is the property of the hospital. This notion of a record being property was once common and its persistence in this case, alongside the concepts of custody and control and information rights of individuals under FIPPA, is antiquated and unhelpful.

[28] *Health Act*, RSBC 1996, c. 179, s. 9.
[29] British Columbia Cancer Agency Research Information Regulation, Appendix 2.

To the extent that some of the holes in the patchwork are filled in with policies, procedures and information-sharing agreements, these are not statutorily-guaranteed, are changeable, confusing and lack transparency.

To summarize, the existing legislative patchwork contains inconsistent and incomplete standards, marking the BC approach to health privacy out as somewhat of an anomaly in Canada. It has been said that the complete picture is only understood by privacy and legal experts, leaving it opaque and confusing not only to the public but also to administrators and professionals working in the health sector. This is at odds with modern privacy protection expectations and approaches. Nor is it conducive to efficient administration of the health system or the vital public interest in health research.

British Columbia's complex, confusing, and inadequate health privacy framework needs to be replaced with a modern and effective privacy and security legislative framework that also supports the public interest in health care, research and sound fiscal management of the health system. The new framework needs to be comprehensive, consistent and transparent across the integrated health sector, both public and private components. It needs to be centred on the individual. It needs to be flexible and able to keep pace with technology. Last, it should be in harmony with health privacy laws in other provinces, given that there are flows of personal health information beyond BC's borders.[30]

RECOMMENDATION

Government should enact new comprehensive health information privacy law at the earliest opportunity.

The next part of this report describes what the major components of a new law should be and makes recommendations for legislative reform.

PART 3: HEALTH INFORMATION PRIVACY LAW REFORM

The policy objective of any reform of health privacy law in BC should be to ensure that privacy is protected and integrated in the delivery of health services. Although there may be widespread agreement in principle on this objective, the reality is that it takes work and resources to achieve properly. Privacy protection can sometimes be overlooked in the interests of facilitating health care delivery. There may be cost pressures involved in maintaining robust privacy protection in new systems and information flows. Further, some critics who claim to be privacy-supportive nonetheless argue that certain long-established privacy principles such as consent and secondary use are no longer relevant in the context of modern health care delivery. Such claims

[30] These flows of information stem from, to give only two examples, the mobility of individuals across Canada and the increasingly inter-jurisdictional nature of many larger-scale health research projects.

must be regarded with scepticism, not least because survey after survey shows that the public expect robust health privacy protections.

This said, it is becoming apparent that there are some privacy protection principles which could be re-visited and refined, while others may need to be enhanced or more broadly applied. For example, where consent requirements have been modified, or may continue to be, this must be offset with privacy protections that give individuals some other measure of control of their own personal health information. These include options to restrict disclosure (known as masking) and the right to know to whom their personal health information has been disclosed.

Fundamental privacy principles reflected in health information privacy law include the following:

- custodians should collect only the minimum amount of personal health information that is necessary to achieve the purpose for the collection;
- personal information should not be used for a purpose which is different from the original purpose for collection without consent or express authority;
- need to know and least privilege principles where users of a system can collect only the minimum amount of information that is required to perform their job functions;
- individuals have a right to exercise control over their personal health information and how it is collected, used and disclosed;
- individuals have a right to easily understandable and accessible information about the collection, use and disclosure of their personal information and privacy and security practices;
- the need for privacy impact assessments (PIAs) and security threat and risk assessments (STRAs) with respect to any new collection, use or disclosure of personal health information in order to identity privacy risks of new initiatives and strategies to mitigate them; and
- modern approaches to management of, and accountability for, personal health information practices should be required, with privacy management programs being at the core.

Comprehensive health information privacy laws generally have the following provisions:

- personal health information is a defined term;
- the law applies to both public and private sector health information custodians;
- specific rules are made around the collection, use and disclosure of personal information, with those rules hinging on the purpose for the collection, use or disclosure or on consent by the individual the information is about for an authorized purpose;
- a distinction is made between direct and indirect collection;

- the rules apply to those with custody or control of the personal health information;
- security standards to protect personal health information, including a duty of accuracy;
- penalties for unauthorized disclosures; and
- a right of access by individuals to their own personal health information and a right to request correction.

How these privacy concepts and requirements need to be adapted and mandated in new health information privacy law is now discussed in more detail.

☐ Definition of personal health information

The definition of personal health information needs to be broad enough to meaningfully protect privacy while enabling the data flows necessary to deliver quality care.

All stand-alone health information statutes in Canada define "personal health information". In BC, the term is only defined in the E-Health Act:

> "personal health information" means recorded information about an identifiable individual that is related to the individual's health or the provision of health services to the individual

This definition is too narrow except in one sense. The term "identifiable individual" in the E-Health Act is preferable to the term "identifying information" which is commonly used in other definitions. Information about an identifiable individual would include information that could be used to identify an individual.

In other ways definitions in other health privacy laws are broader. An example is the following definition from New Brunswick's 2009 *Personal Health Information Privacy and Access Act*:

> "personal health information" means identifying information about an individual in oral or recorded form if the information
>
> (a) relates to the individual's physical or mental health, family history or health care history, including genetic information about the individual,
> (b) is the individual's registration information, including the Medicare number of the individual,
> (c) relates to the provision of health care to the individual,
> (d) relates to information about payments or eligibility for health care in respect of the individual, or eligibility for coverage for health care in respect of the individual,

(e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any body part or bodily substance,
(f) identifies the individual's substitute decision-maker, or
(g) identifies an individual's health care provider.[31]

Other substantially similar definitions are found elsewhere in Canada. For example, the combined definitions of "health information" and "personal health information" in the new Yukon statute amount to the same meaning.[32] Recently-enacted health privacy laws in Nova Scotia and Newfoundland and Labrador also contain broad definitions of personal health information. It should be noted that all these definitions include information in both "recorded" and "unrecorded" form. This is appropriate in the modern electronic world because it addresses the many forms in which information exists in the health care field.

The need for a broad, purposive, definition is illustrated by the fact that, thanks to advances in technology, personal health information now includes such things as tissue samples in biobanks and the results of whole genome sequencing. These developments can raise the privacy stakes. Nothing is more inherently unique, and potentially stigmatizing, than an individual's genetic blueprint. Whole genome sequencing may be able to tell us who we are, where we came from, and the health challenges that may be in store for us. It also inadvertently conveys information about blood relatives. The disclosure of whole genome sequence information could affect the opportunities available to individuals, including eligibility for loans, employment and educational opportunities, or adoption. For this reason, there may be a need for government to consider the development of legislation prohibiting the use of genetic information in relation to employment and health insurance as exists in the US.[33]

When moving ahead with law reform in BC, therefore, questions should be asked as to how best to protect privacy in relation to biological materials and genetic information. It may be the case that certain types of personal information should be defined separately and treated differently in health information privacy law.

This said, the government should carefully consider the argument for genetic exceptionalism. Should the term 'genetic or genomic information' be defined separately? There is some debate in the field of genomics about whether consent requirements and limitations on use in relation to genetic information should be different from those for other types of personal health information. If the argument for genetic exceptionalism was accepted, the definition of personal health information would have to exclude genetic information to allow the law to provide for different requirements in relation to the collection, use and disclosure of genetic information. This regulatory approach is seen by some to be unnecessary and fragmented given that there are also many other types of personal health information that are particularly sensitive and

[31] *Personal Health Information Privacy and Access Act*, SNB 2009, c. P-7.05.
[32] Health Information Privacy and Management Act, S.Y. 2013, c. 16. Not yet in force.
[33] Genetic Information Nondiscrimination Act, Pub.L. 110-233, 122 Stat. 881

require robust privacy protection. For them, genetic information is not special and does not require special rules. This issue will need to be addressed in new health privacy law.

RECOMMENDATION

The law should define personal health information in a broad and comprehensive manner. Careful consideration should be given to developing a separate definition for genetic or genomic information because of its unique nature.

☐ Non-identifying information

Some health information privacy law also include provisions with respect to non-identifying information, that is, information that does not identify the individual. For example, the Alberta *Health Information Act* authorizes the collection of non-identifying health information for any purpose. It must be recognized, however, that with respect to de-identified information, there is always a risk that individuals may be re-identified. The determination of what is truly non-identifying information is a complex and vexing question and is a specialized area of expertise.[34] Any definition of non-identifying information must take into consideration the risk of re-identification.

RECOMMENDATION

The law should include a narrow definition of non-identifying information that takes into account the risk of re-identification.

☐ Legislative scope

To whom the health information privacy law should apply is a critical threshold issue. The health sector today presents significant challenges in terms of identifying all the entities that should be subject to health information privacy law. As discussed in Part 1, the health sector is expanding in many ways.

The scopes of practice of health professions are being enlarged, there are innovations in primary care and inter-disciplinary practice and there are new and emerging practitioners delivering tasks and services.

Increasing recognition of the social determinants of health and the desire to coordinate services delivered to the same individuals by different sectors are driving broader integrated service delivery models in government. For example, a team comprised of nurses, social workers, Crown counsel and probation offers may all have access to the

[34] See for example Khaled El Emam, *Guide to the De-Identification of Personal Health Information*, CRC Press, 2013.

personal health information of their clients. Does it make sense for only the Ministry of Health or a health authority to be subject to health information privacy law and not their partner ministries?

Technologies such as mHealth and tele-health monitoring by manufacturers are enabling new data flows. Should companies that monitor implants be subject to health information privacy law?

This question of who should be captured within the parameters of health information privacy law is a difficult issue which other provinces are also grappling with in the face of expanding health care sectors everywhere.

New health information privacy law should be forward-looking and applicable to all data flows of personal health information that raise privacy risks. At the same time, however, the obligations of custodians may be seen as too onerous or unenforceable in relation to certain entities. There needs to be a common sense approach in determining who's in and who's out. There also needs to be an ability to extend the reach of the law as health care evolves.

The difficulty and complexity of this endeavour raises the question of whether a single stand-alone health information privacy law can ever be comprehensive enough. There may be a need to develop separate specific provisions that apply to distinct types or data flows of personal health information. Consideration should also perhaps be given to having different kinds of custodians with obligations tailored to the type and nature of the personal health information they collect.

For example, the E-Health Act in BC establishes a separate privacy and security framework for databases of the Ministry of Health and health authorities. Quebec has also chosen to have specific legislation for electronic health records. Recent legislation passed in Quebec (Bill 59) included a privacy and security framework for the Quebec Electronic Health Record. The Electronic Personal Health Information Protection Act, 2013 (Bill 78), was recently introduced in Ontario which would enact a separate part of its stand-alone statute for electronic heath records. It may be that a one-size fits all approach is not appropriate given all the data flows in the expanding health sector.

RECOMMENDATION

The law should define custodian in such a way that the application of the law can be extended as new entities and practitioners collect personal health information. There should also be consideration of distinct provisions for certain data flows.

COLLECTION

➢ Minimum collection

Only the minimum amount of personal information that is necessary to achieve the purpose for the collection is authorized under privacy law. Given that where there is a collection there is a corresponding disclosure, only the minimum amount of personal information should also be disclosed.

This principle should be reflected in new health information privacy law. There should be a provision such as in the Nova Scotia *Personal Health Information Act* which states that the collection, use and disclosure of personal health information must be limited to the minimum amount of personal health information necessary to achieve the purpose for which it is collected, used and disclosed.[35] There is a similar requirement in the Ontario *Personal Health Information Protection Act, 2004*.[36]

➢ Indirect collection

In privacy law, collection is indirect when the personal information is collected from a source other than the individual the information is about. Under BC's privacy laws of general application, indirect collection is only authorized in certain circumstances. Limits on indirect collection present challenges for EHR systems because users indirectly collect personal health information from the system. It is questionable whether the distinction between direct and indirect collection is still relevant in the context of EHR systems.

➢ Multiple purposes for collection

In privacy law, the ability to collect personal information must be specifically authorized. Privacy law tends to authorize collection, use and disclosure for a particular purpose, although it sometimes may also be authorized for a consistent purpose (as defined).

In relation to the health sector, collection is often for multiple purposes. Initially, the purpose is for the delivery of health services to an individual. However, by necessity, that information may also be collected for purposes related to the administration of our publicly-funded health care system. These purposes include billing the Medical Services Plan as well as for quality assurance and improvement, to ensure that services are being delivered in a safe, efficacious and cost-effective manner. The same personal information may also be collected for the purpose of conducting health research.

---

[35] *Personal Health Information Act*, SNS 2010, c. 41 as amended, s. 25.
[36] *Personal Health Information Protection Act, 2004*, s. 30(2).

Multiple purposes for collection in relation to electronic databases are authorized in relation to electronic databases under the E-Health Act and in other health information privacy legislation such as the New Brunswick[37] and Nova Scotia laws.[38]

RECOMMENDATION

The law should authorize only minimum collection; permit indirect collection; and allow multiple purposes for collection.

CONSENT

From a privacy perspective, individuals should have the ability to control the collection, use and disclosure of their own personal information to the greatest extent possible. This is generally recognized in health information privacy law through requirements of express or implied consent.[39] Provisions authorizing the collection, use and disclosure of personal health information with express or implied consent need to be a fundamental part of new health information privacy law in British Columbia.

In relation to EHRs, however, consent requirements are said to be impractical. It is argued that EHR systems support clinical workflow and patient safety, and the difficulties and delays that would be involved in obtaining an individual's consent make a consent-based model simply not feasible or desirable.

This has already been accepted in BC in that the E-Health Act is a no-consent model which authorizes the collection, use and disclosure of personal health information through a health information bank without consent. Similarly, new health privacy legislation in Quebec (Bill 59) presumes that individuals have consented to the release of their health information through the Quebec Health Record. Other provincial laws contain provisions that produce the same result. For example, Alberta's *Health Information Act* does not require consent for making health information accessible in the EHR. Newfoundland and Labrador's *Personal Health Information Act* makes disclosure to the provincial electronic health record mandatory,[40] as does the New Brunswick *Personal Health Information Privacy and Access Act*.[41] These policy approaches may make sense from the perspective of an electronic health record system for it to function as intended. However, if this is the policy choice made by government, in the absence of consent, it is critical that individuals are able to exercise control in relation to their electronic health record through other mechanisms.

---

[37] *Personal Health Information Privacy and Access Act*, SNB, c. P-7.05.
[38] *Personal Health Information Act*, s. 31.
[39] See, for example, s. 33 of the Yukon Health Information Privacy and Management Act which provides that implied consent is sufficient unless the Act requires express consent.
[40] *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 39(4)(c).
[41] *Personal Health Information Privacy and Access Act*, SNB 2009 c P-7.05, s. 37(6)(c)(iii).

These elements of control are discussed below.

➢ Accuracy

Custodians should have a duty to ensure that the information that they collect is accurate. For example, the new Yukon law includes a requirement that a custodian use every reasonable effort to ensure that the personal health information the custodian collects is accurate at the time the custodian collects it.[42] The Newfoundland and Labrador law imposes a duty on custodians to ensure information is as accurate as necessary for the purpose for which it is used or disclosed.[43]

RECOMMENDATION

The law should require custodians to ensure the accuracy of personal health information.

Use

➢ Secondary use

Health care administrators today are generally of the view that personal information collected for the delivery of health services should be available for other health-related purposes, including billing, quality assurance and improvement, planning and research. This is often reflected in health information privacy legislation.[44] There is currently an effort by deputy ministers of health across Canada to articulate a national vision for making information in EHR systems available for health system use.

In the privacy context, the notion of health system use is characterized as a secondary use. A secondary use arises where personal information is being used for a purpose that is different from the original purpose for which it was collected. Traditionally, secondary uses are not permitted unless the individual has consented first or they are statutorily authorized.

There is some question whether secondary use is an outdated concept in the context of Canada's increasingly electronic health sector. If collection can be seen as being in relation to multiple purposes, its use for multiple purposes flows from that broader set of collection purposes. The use is no longer secondary since it was an original purpose for collection. This makes it vitally important to ensure that the scope of collection purposes is reasonable, to avoid the problem of use beyond the health sector. Given the expanding health sector and the changes in models of health care delivery, there is

[42] Health Information Privacy and Management Act, S.Y. 2013, c. 16, s. 52.
[43] *Personal Health Information Act*, SNL 2008, c P-7.01, s. 16.
[44] See for example, ss. 35, 46 and 47 of the Alberta *Health Information Act*, RSA 2000, c. H-5 and the E-Health Act, s. 4.

danger that health system use will be defined so broadly that there will be over collection of personal health information from individuals. This greater amount of personal health information could also be shared beyond what individuals would reasonably expect.

British Columbians expect their personal health information to be treated as confidential unless they otherwise consent. The purposes for collection in the new law therefore need to be as specific and limited as possible, and established in law, in order to both maintain public trust and confidence in the health care system and meet privacy expectations.

Broad health system use was authorized in the E-Health Act through the recognition of multiple purposes for the initial collection of personal health information. They are also authorized under the *Public Health Act* in relation to the reporting of disease or health hazards.[45] The *Pharmaceutical Services Act* has different purposes that include a prescribed purpose.[46] The potential for government to prescribe purposes that are not health-related is troubling. This same concern arises in relation to the *Ministry of Health Act* where the Minister of Health is authorized to collect personal information from any public body for a broadly-defined "stewardship purpose".[47] The Minister has used this legislation to collect personal information from the surgical patient registry of the Provincial Health Services Authority.

The E-Health Act and the *Public Health Act* authorize the use of personal health information for the same health-related purposes as they authorize for collection. The specificity of enumerating them in that manner is desirable. This is not the case in the *Pharmaceutical Services Act* where use is authorized for the same health-related enumerated purposes but also for additional purposes, including a prescribed purpose. The latter is too vague and overly broad given the sensitivity of PharmaNet data. This concern was previously raised by this Office publicly when the Bill was introduced in the Legislature in 2012.

RECOMMENDATION

The law should permit secondary use but expressly limit it to specific health-related purposes only.

[45] *Public Health Act*, SBC 2008, c 28, s. 9.
[46] *Pharmaceutical Services Act*, SBC 2012 c 22, s. 22(1).
[47] *Ministry of Health Act*, RSBC 1996, c 301, s. 9.

DISCLOSURE

➢ Multiple purposes for disclosure

Health information privacy law tends to authorize multiple purposes for disclosure, including in relation to payments, quality assurance and research. Examples of such authorities are found in the E-Health Act as well as in stand-alone health privacy statutes in other provinces.[48]

➢ Role-based access

The need to know and least privilege concepts are key privacy principles that are reflected in privacy law, even though they are not always stated explicitly. These principles become particularly important in relation to large databases containing personal health information, notably when they form part of an EHR system. Users of the system should only be able to access the minimum amount of personal health information of individuals that they require in order to provide care to those individuals. The mechanism for restricting access in this way is typically a "role-based access model" whereby users only have access to the personal health information that is necessary for them to perform their job functions. A role-based access model is key to a privacy protective system.

A role-based access model forms part of the designation order approved by the Minister of Health under the E-Health Act for the Provincial Laboratory Information Solution. This level of specificity and transparency within a legal instrument is desirable. It also means that the offence provision in the Act is triggered if a user fails to adhere to the role-based access model as set out in the designation order.

Role-based access models also exist in relation to other electronic health record systems within health authorities at a policy level. Our Office previously reviewed such a model at Vancouver Coastal Health Authority, for its Primary Access Regional Information System (PARIS) in Investigation Report F10-02.[49]

Role-based access models are a key enabler of EHR systems. They must be described in enough detail to accurately reflect the need to know and least privilege principles. Roles should be assigned by a central authority so that they are assigned on an objective and consistent basis. Other important aspects of such models are beyond the scope of this report, but these should also be reflected in or under the law.

Another aspect of a role-based access model is the need to monitor it by auditing disclosures of personal information to users of the system. Different types of audits should be mandated in legislation. For example, Bill 78 in Ontario has a requirement to audit and monitor every instance where a user collects personal health information that

[48] See, for example, AB *Health Information Act*, RSA 2000, c H-5, Part 5.
[49] Available at http://www.oipc.bc.ca/investigation-reports/1241.

has been masked.[50] There should also be requirements to conduct proactive audits on a regular basis.

RECOMMENDATION

The law should entrench role-based access models (based on need to know and least privilege privacy principles) with as much granularity as possible and attach penalties for users who violate their conditions of access. Audits should be required.

➢ Disclosure for research purposes

There is a widely held view in BC, notably amongst the research community, that researchers cannot access the personal health information they need to conduct important health research. Some have suggested that privacy is a barrier and the root cause of the problem.

In response to this concern, this Office convened a roundtable discussion in June 2012 involving representatives of the research community, the Ministry of Health, health authorities and the public to consider whether privacy is in fact a barrier negatively impacting researchers' access.

The roundtable concluded that that privacy laws themselves are not a barrier. There was agreement, however, that delays in research access approval processes and the lack of understanding of the process and the criteria for approval are serious challenges.

This Office and the Ministry of Health convened a second roundtable in December 2013 to identify solutions that would address health data access issues and develop an implementation plan. At the roundtable, stakeholders recommended harmonized and consistent criteria and approval processes. There was also support for a single gateway for health researchers to access data.

We agree that a clear and consistent approval process for all data stewards in the health sector would help resolve current delays and confusion. That approval process should be set out in detail in legislation and in an over-arching policy framework.

BC's privacy laws of general application permit a public body or an organization to release personal information for a research purpose without consent if certain conditions are met.[51] In the health sector, data stewards impose additional requirements, by policy, beyond the minimum conditions set out in current legislation. As a result, FIPPA and PIPA do not reflect current practice in the health sector and lack specifics regarding the level of privacy protection and transparency that is required. We

[50] Electronic Personal Health Information Protection Act, 2013 (Bill 78), s. 55.6(5).
[51] FIPPA, s. 35; PIPA, s. 21.

believe that a detailed framework for approvals should be set out in legislation and regulations to provide transparency and certainty to the public and to the research community.

The Ministry of Health and health authorities require researchers to obtain approval from a research ethics board before they will disclose data to researchers. This helps, among other things, to ensure that identifiable data is necessary to conduct the research. Research ethics boards generally apply the *Tri-Council Policy Statement of Ethical Conduct for Research Involving Humans* by the Medical Research Council of Canada, the Natural Sciences and Engineering Research Council of Canada and the Social Sciences and Humanities Research Council of Canada.[52] The Canadian Institutes of Health Research have also developed best practices which must be adhered to for funding.[53]

Unlike other provinces in Canada, however, this is not a legal requirement and the roles and responsibilities of research ethics boards have not been set out in law in BC.

The *Health Information Act* in Alberta mandates review by a designated research ethics board before the health researcher can request personal information from a custodian. The research ethics board must consider whether consent should be required, conduct a proportionality assessment and consider whether adequate safeguards are in place to protect privacy. The research ethics board must send a copy of its response to the Information and Privacy Commissioner who may publish it.[54]

Pursuant to the Newfoundland *Health Research Ethics Authority Act*, a corporation, the Health Research Ethics Authority for Newfoundland and Labrador, appoints members of a health research ethics board following consultation with the Minister of Health, the President of Memorial University and the CEO of the Eastern Regional Health Authority. The Authority may also approve other research ethics bodies if it is established in conformity with the principles of the *Tri-Council Policy Statement*.[55]

The legislation provides that the health research ethics board or a research ethics body must apply one or both of the *Tri-Council Policy Statement*, the International Conference on Harmonization of Technical Requirements for the Registration of Pharmaceuticals for Human Use Guidance E6: Good Clinical Practice: Consolidated Guideline; and other guidelines or standards it approves.[56]

The Ontario *Personal Health Information Protection Act* requires researchers to submit the research plan that has been approved by the research ethics board to the custodian and prescribes what the plan must contain, including the affiliation of each person

---

[52] http://www.pre.ethics.gc.ca/pdf/eng/tcps2/TCPS_2_FINAL_Web.pdf.
[53] CIHR Best Practices for Protecting Privacy in Health Research, September 2005, http://www.cihr-irsc.gc.ca/e/29072.html.
[54] *Health Information Act*, RSA 2000, c. H-5, ss. 50, 51 and 50.1.
[55] *Health Research Ethics Authority Act*, SNL 2006, c. H-1.2, ss. 3, 7, 8, 9.
[56] Ibid., s. 9(5).

involved in the research; the nature and objectives of the research and the public or scientific benefit of it. The criteria that the research ethics board must apply in its decision whether to approve a research plan are also prescribed as are the contents of its decision.[57]

We are of the view that BC should consider following the Newfoundland approach and establish one research ethics board for the entire province in legislation. Having a single board would help to address the problems of consistency and transparency about the data access approval process that have been identified in BC. It may also help streamline reviews.

Moreover, the criteria it must apply in assessing requests for data should be set out in legislation. Having the mandate of a research ethics board explicitly stated in legislation would improve public understanding and awareness about both the approval process for the conduct of health research and the responsibilities of a research ethics board.

RECOMMENDATION

The law should establish a single research ethics board for the province and mandate its role and the criteria the board applies, including the *Tri-Council Policy Statement*.

Data stewards of personal health information have the responsibility for determining whether a health researcher making a data access request requires identifiable data for their research studies or whether de-identified or anonymized data would be sufficient to accomplish the research purpose. Data stewards also have an important responsibility to meet public expectations in the timely disclosure of data to support public interest research.

In Manitoba, approval of a data access request is required not only by a research ethics board but also from a separate health information privacy committee that is established in the *Personal Health Information Act*. This committee is responsible for applying a privacy lens to research requests. It is comprised of representatives from the health authorities, the College of Physicians and Surgeons, the College of Registered Nurses, the Manitoba Pharmaceutical Association, the Manitoba Health Records Association and the University of Manitoba.[58]

There is a similar body in BC but it has a very limited mandate. A data stewardship committee appointed by the Minister of Health approves requests from health researchers for data that is contained only in either a health information bank or in PharmaNet.[59] The role of the data stewardship committee should be expanded to

[57] *Personal Health Information Protection Act, 2004*, SO 2004, c. 3, s. 44.
[58] *The Personal Health Information Act*, SM 1997, c. 51, s. 24; Personal Health Information Regulation, s. 8.3
[59] E-Health Act, s. 11; *Pharmaceutical Services Act*, SBC 2012, c 22, s. 26.

broaden its current scope to other personal health data holdings along the lines of the Manitoba model. This will help ensure data access requests are appropriately scrutinized from a privacy perspective and to ensure consistency in the decision-making process. In the event government decides to develop one robust data platform with multiple dataset from various sectors, including health, the mandate of the data stewardship committee should be broadened even further so that it establishes policies or processes for a consistent approach to vetting requests for access to data.

RECOMMENDATION

The law should expand the role of the data stewardship committee, so that a privacy lens is applied consistently in the data access approval process.

Another aspect of disclosure for research purposes which should be specifically authorized is the disclosure of data by the Ministry of Health to the Canadian Institute for Health Information and to Population Data BC. The Ministry discloses most of its data to these entities so that they can make it available to health researchers. Given the significant amount of data, and the nature of it, there needs to be transparency and particular rigour as to how it is being protected.

The *Personal Health Information Act* in Manitoba permits the disclosure of personal information to prescribed health research organizations under certain conditions.[60] The Manitoba Centre for Health Policy at the University of Manitoba and the Canadian Institute for Health Information have been prescribed.[61]

Pursuant to the *Personal Health Information Protection Act, 2004*, the Information and Privacy Commissioner of Ontario is responsible for reviewing the practices and procedures implemented by the Institute for Clinical Evaluative Sciences to protect privacy.[62]

Should BC move towards a single gateway for data access, that secure research platform should have a legal mandate. Its practices and procedures should require review by this Office.

RECOMMENDATION

The law should specifically authorize all disclosures for research purposes to the Canadian Institute for Health Information, organizations like Population Data BC or any other secure research platform and require practices and procedures to be reviewed by the Commissioner on a periodic basis.

[60] *The Personal Health Information Act*, SM 1997, c. 51, s. 24.1.
[61] Personal Health Information Regulation, s. 8.5(1).
[62] *Personal Health Information Protection Act, 2004*, SO 2004, c 3, Schedule A, s. 45(4).

➢ Disclosure of genetic information

The potential of biomedical research today is exciting. Through the use of biobanks and genetic information, health researchers are studying the interactions between genes, genome variation, and the environment to determine individuals' propensity to certain diseases and are enabling personalized medicine. Biobanks are repositories of human biological material that contains at least traces of DNA or RNA that would allow for genetic analysis.

In Canada, large longitudinal research projects (such as the Canadian Partnership for Tomorrow Project and the Canadian Longitudinal Study on Aging) involve the collection, storage and long-term analysis of human tissue linked with health and demographic information. These large-scale biobanks have great potential for understanding genomic variation and the distribution of health and disease.

There are also large-scale health research projects in many countries that involve the collection of whole genome sequencing data. Whole genome sequencing reveals an individual's DNA, that is, his or her unique genetic blueprint. The information is useful in the delivery of health services to the individual and in health research where it will improve understanding of the changes in DNA that underlie disease. However, the benefits to society from health research using whole genome sequencing data are tempered by the risks to individual privacy.

Biobanks and genetic information raise distinct privacy issues. A person's genome is a unique identifier. It is also a network identifier. This type of personal information requires a high level of privacy protection because of its predictive potential and relevance not only for the individual, but for his or her family members. Unauthorized disclosure of genetic information can place individuals at risk of discrimination and stigmatization.

It may be the case that the standard authority for disclosure for research purposes is not appropriate in relation to genetic information and consideration should be given to enacting specific rules. Such rules would require individuals to give consent and give individuals the right to revoke their consent to participate in the biobank at any time.

Formerly, the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* required informed consent in the context of genetic research and, especially, in the banking of genetic material. It also required specific consent for each research project involving tissue collection. This latter requirement was seen as problematic in the context of biobanks given the long-term nature of many biobank projects where all possible future research projects are not yet known. Recently, amendments were made to the *Tri-Council Policy Statement* that would permit researchers to use previously collected specimens without consent in specified circumstances. New provisions also refer to "research directives" where individuals who volunteer for long-term research studies can set out their preferences for future uses of their samples.

At this point in time, it is challenging to determine the appropriate consent requirements for genetic information given how rapidly the science of genomics and personalized medicine is evolving. In order to make that determination, there needs to be a multi-stakeholder conversation involving, among others, genome scientists, clinicians and the public.

➢ Disclosure of genetic information without consent

Other specific issues have emerged with respect to the disclosure of genetic information. One of the most difficult is whether genetic information should be disclosed to family members in certain circumstances without consent. The American Society of Human Genetics maintains that physicians have a duty to warn the third-party relatives of patients with disease-causing mutations without the consent of the patients under certain circumstances.

In Australia, amendments to the *Privacy Act* made in 2006 implemented recommendations of the Australian Law Reform Commission and the Australian Health Ethics Committee to allow health practitioners to use or disclose patients' genetic information, whether or not they give consent, in circumstances where there is reasonable belief that doing so is necessary to lessen or prevent a serious threat to the life, health or safety of their genetic relatives. The amendments also required guidelines to be issued by the National Health and Medical Research Council with the approval of the Australian Privacy Commissioner. These guidelines were finalized in 2009 and apply to private sector organizations that have obtained genetic information in the course of providing health services to individuals.

The issue of "duty to warn" is a difficult one because scientists do not agree with a high level of certainty what genome variations mean or what should be done with the information. There is a continuum of professional opinions about which variations should be disclosed and in what circumstances. We recommend that health privacy law provide for a duty to warn and require guidelines that are developed in consultation with genome scientists, clinicians, research ethics boards, Privacy Commissioners and the public.

CUSTODY AND CONTROL

➢ Governance and accountability

Privacy laws generally contemplate a single custodian of personal information. The person who would head such a body is responsible and accountable for compliance with the privacy-related obligations set out in policy and legislation.

In the world of EHR systems, where the same personal health information is accessed at different points of service throughout the system, there may be different custodians at

each point of service and the responsibilities are therefore arguably shared, at least in a practical sense. When EMRs are integrated with EHR systems, responsibilities for custody and control are even more diffuse. The concept of integration of systems or interoperability across systems also raises challenging governance and accountability issues.

As a result, we are seeing multiple custodianship models. In such a model, each custodian at each point of service becomes accountable for the personal health information in their custody or control. There must also be an overall governance structure which clearly sets out where accountability resides for the EHR system as a whole, so that decisions can be made with respect to system-wide issues such as secondary use limitations and security. Responsibility for responding to access requests, requests for correction and privacy complaints must also be clearly identified. Governance models may either be centralized in a designated data steward of the Ministry or health authority or decentralized, even federated, through committees, councils and data stewards of the various custodians.

Among other things, the governing body must ensure all custodians have robust privacy management programs (discussed below). Other responsibilities of a governing body include:

- entering into information-sharing agreements;
- coordinating investigations of privacy breaches where the source of a breach is unclear or involves multiple sources;
- updating standards and jurisdictional practices for privacy and security, including information technology;
- responding to data access requests from researchers;
- responding to access requests and complaints from individuals that cannot be dealt with by a single data steward; and
- external communication regarding the EHR.

The E-Health Act provides that the Chief Data Steward of the Ministry of Health is the administrator of a Ministry database.[63] It establishes a clear and transparent governance model where ultimate accountability resides with an identifiable person.

The Ministry of Health has advised that having the Chief Data Steward as the sole administrator does not work in relation to a large and complex system where there is collection, use and disclosure from multiple points of service. We are concerned, however, that accountability in a multiple custodianship model becomes unclear and

[63] E-Health Act, s. 1.

responsibilities are so diffused that they can become uncoordinated and inconsistent. There may also be gaps or confusing areas of overlap in terms of who is responsible for what. We prefer a model where it is clear who is ultimately accountable and the need to delegate certain responsibilities to others is dealt with in information sharing agreements. In that case, there is clear and unmistakeable governance and accountability and, at the same time, the need for other custodians to handle certain functions at various points of service is enabled in a legal instrument. The contents of those information sharing agreements could be prescribed in legislation.

There may also be agreements between custodians and information managers (such as agents, registries and special entities) and guidance related to those agreements could also be set out in legislation so as to establish clear roles and responsibilities in the interoperable EHR context.

Canada Health Infoway is funding EHR systems across Canada with a long-term vision for an interoperable EHR where EHR systems in different provinces and territories will have the ability to communicate with one another to facilitate patient care and treatment of a mobile population. Representatives of health ministries across Canada have been working together as a Pan-Canadian Health Information Privacy Group to develop common understandings related to the trans-jurisdictional nature of the interoperable EHR. The hope is that these common understandings would be adopted consistently across jurisdictions to support trans-jurisdictional disclosures of personal information.

In terms of accountability and trans-jurisdictional disclosures of personal health information, the common understanding of the Health Information Privacy Group is that accountability for the privacy of personal health information held in EHR systems will continue to rest with the jurisdictions, and a pan-Canadian coordinating group is needed to discuss, address and coordinate common information governance issues.[64] This illustrates the need for a clear governance and pan-Canadian approach in health information privacy law.

RECOMMENDATION

The law should require clear governance models and reflect a pan-Canadian approach.

[64] Privacy and EHR Information Flows in Canada, Common understandings of the Pan-Canadian Health Information Privacy Group, Canada Health Infoway, July 31, 2012. https://www.infoway-inforoute.ca/index.php/resources/reports/privacy/doc_download/626-privacy-and-ehr-information-flows-in-canada-version-2-0.

➢ Privacy management programs

In a system where there are multiple custodians of personal health information, it is essential that each of them have a robust privacy management program in place. A privacy management program is necessary to ensure compliance with privacy obligations under FIPPA and PIPA.

This Office has provided comprehensive guidance to both private sector organizations and public bodies sector regarding privacy management programs. The guidance tool for organizations, *Getting Accountability Right with a Privacy Management Program,*[65] and the one for public bodies, *Accountable Privacy Management in BC's Public Sector*[66] are the basis for the conduct of compliance audits by this Office. They serve as a baseline for how organizations and public bodies can demonstrate compliance to the public and to our Office.

In the health care sector, a privacy management program at each point of service helps to ensure that the personal health information in the custody or control of that public body or organization is adequately protected. This privacy management program should include staff resources dedicated to privacy, an inventory of data holdings, policies, breach protocols, risk assessment tools and privacy training and education for users. We made recommendations to the Ministry of Health to implement such components of a privacy management program following our investigation of the 2012 privacy breach at the Ministry.[67]

Custodians need to be able to demonstrate compliance with their privacy obligations under applicable privacy law. Requirements for privacy management programs should be part of the agreements required by the Ministry of Health and health authorities with entities who are being given access to their systems. It should also be in funding agreements with physicians for EMRs.

Privacy management programs will vary depending on the size of the entity and the amount and sensitivity of the personal health information that it has in its custody and/or control. Given that privacy risks, and mitigation strategies, evolve over time, privacy management programs need to be monitored and assessed on a regular and frequent basis. Privacy breaches or complaints may also prompt ad hoc reviews.

All of the building blocks of a privacy management program do not necessarily have to be prescribed in law, although consideration should be given to entrenching some of them. These include requirements to complete privacy impact assessments (PIAs) and security threat and risk assessments (STRAs).

---

[65] http://www.oipc.bc.ca/guidance-documents/1435.
[66] http://www.oipc.bc.ca/guidance-documents/1545.
[67] Investigation Report F13-02, *Ministry of Health (Re),* 2013 BCIPC 14 (CanLII).

It should be mandatory for PIAs to be completed by custodians so that there can be some assurance that all privacy risks have been identified and addressed through appropriate mitigation strategies. A PIA is a self-education tool that facilitates knowledge of privacy obligations and proactive compliance. The *Health Information Act* in Alberta imposes a duty on custodians to prepare PIAs describing how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual the information is about.[68] Given the nature and amount of personal information in electronic record systems in particular, it behooves custodians to complete PIAs and STRAs for each new system at the conceptual, design and implementation phases of the initiative.

There should also be a statutory requirement for custodians to establish policies and procedures as exist, for example, in the Alberta law[69] and in *The Health Information Protection Act* in Saskatchewan.[70]

At the very least, all of the building blocks of a privacy management program should either be a legislative or a policy requirement and be embedded in information-sharing or data access agreements that the Ministry or health authorities enter into with other entities accessing electronic health record systems.

RECOMMENDATION

The law should prescribe essential elements of a privacy management program.

INDIVIDUAL CONTROL

➢ Notification

In the absence of consent, notification requirements become extremely important. Individuals should be made aware of how their personal health information is being stored, used, disclosed and protected. For example, individuals should know that their personal health information is being collected into electronic health record systems and is accessed by users in accordance with a role-based access model.

There are no notification requirements in BC health information legislation. It is our view that, in the absence of consent, notification requirements should be entrenched in law.

---

[68] *Health Information Act,* RSA 2000, c H-5, s. 64(1).
[69] *Health Information Act,* s. 63(1).
[70] *The Health Information Protection Act*, SS 1999, c H-0.021, s. 16.

Quebec's Bill 59 has a novel provision that requires the Minister to inform the public of:

- the aims and operational procedures of the Quebec Health Record;
- the use, release and conservation of information in health information banks in clinical domains; and
- the rights of individuals regarding access, correction and refusal.[71]

No other province seems to specifically place an obligation on the Minister to communicate with the public at large.

Other provinces require custodians (or "trustees") of personal health information to notify the public regarding collection, use and disclosure of their personal information or of their rights under the legislation. For example, *The Health Information Protection Act* in Saskatchewan states an individual has the right to be informed about the anticipated uses and disclosures of the individual's personal health information and a trustee must take reasonable steps to inform the individual of the anticipated use and disclosure of the information by the trustee.[72] The Yukon Health Information Privacy and Management Act requires custodians to make statement of information practices public.[73]

RECOMMENDATION

The law should include notification provisions, with obligations placed on the Minister with respect to the provincial EHR system and also on other custodians.

➢ Masking

Masking options are another important way for individuals to exercise control of their personal health information in electronic health records. Masking permits individuals to restrict access to their own personal health information. In BC, individuals have a legal right to exercise a masking option in relation to two different repositories, the Provincial Laboratory Information Solution and PharmaNet. With respect to the former, individuals may make a disclosure directive. This disclosure directive can only be overridden in the event of an emergency, when the individual is incapable.[74] With respect to PharmaNet, an individual may ask a pharmacist to attach a protective word to their personal health

[71] An Act respecting the sharing of certain health information (2012, c. 23).
[72] The *Health Information Protection Act*, s. 9.
[73] *Health Information Privacy and Management Act*, s. 21.
[74] E-Health Act, ss. 8 to 10.

information contained in PharmaNet so that their personal health information can only be accessed with consent or in other limited circumstances.[75]

In the electronic health record systems of health authorities, masking options vary and are at the discretion of the health authority. As part of our investigation of the PARIS system at Vancouver Coastal Health Authority, noted above, we reviewed the option for individuals to have their record flagged as an Enhanced Information Security Client.

To date, there has been very low uptake on these masking options. This is likely due in large part to the fact that British Columbians are largely unaware that these options are available to them. The Ministry of Health has made little effort to communicate the options of making a disclosure directive or attaching a protective word.

A right such as the right to make a disclosure directive or attach a protective word to PharmaNet records should exist for all other EHR systems used for clinical care, including systems within health authorities.

It should be noted that other provinces also have requirements for masking options. In Quebec, Bill 59 permits information to be collected for the purposes of the Quebec Health Record without consent but gives individuals the right to refuse to allow the release of their health information through the Quebec Health Record.[76] Under the new Yukon statute, the ability of individuals to make consent directives in relation to the Yukon Health Information Network may be established by regulation.[77] Bill 78 in Ontario requires certain processes in relation to consent directives and references a degree of granularity that is desirable.[78]

In conjunction with statutory requirements for masking options, investments must be made in public awareness campaigns so individuals know they have the right to mask their personal health information. Furthermore, the process for doing so should not be burdensome for individuals.

RECOMMENDATION

The law should give individuals the ability to exercise masking options in relation to the provincial EHR and other electronic record systems.

➢ Audit logs

It is important that individuals have the ability to find out who has accessed their records. With electronic health records, this means that individuals must have the right

[75] *Pharmaceutical Services Act*, ss. 28 and 29.
[76] An Act respecting the sharing of certain health information (2012, c. 23).
[77] *Health Information Privacy and Management Act*, s. 79.
[78] Electronic Personal Health Information Protection Act, 2013 (Bill 78), s. 55.5.

to see the audit logs that contain information about who has accessed their record and when.

The E-Health Act requires the administrator of a health information bank to make available to an individual information respecting who has collected, used or disclosed that individual's personal health information.[79] Because only three databases have been designated as health information banks, this requirement currently has limited application.

There are no specific legal requirements for any other electronic health record systems although, on a policy basis, health authorities normally make audit logs available to individuals upon request.

RECOMMENDATION

The law should establish the right of individuals to know to whom their personal health information has been disclosed from databases that contain clinical information.

➢ Access request

Another way for individuals to control their own personal information is to be able to make an access request so that they can determine what personal information about them has been collected. Privacy law also generally requires that individuals have the ability to request a correction of their personal information.

The existing rights of individuals under FIPPA and PIPA to request access to their own personal information, and make corrections to it, therefore should be included in health information privacy law. There must be an ability to make a complaint to the Commissioner if the individual is not satisfied with the custodian's response to an access request. Such provisions are contained in all provincial stand-alone health information statutes.[80]

RECOMMENDATION

The law should provide individuals with the right to have access to, and request correction of, their own personal health information.

[79] E-Health Act, s. 17.
[80] See, for example, Parts 2 and 6 of the New Brunswick *Personal Health Information Privacy and Access Act*.

➢ Patient portals

To the maximum extent possible, custodians should implement "patient portals" in their electronic record systems so that individuals can have routine and timely access to their own personal health information. There is a provision in the E-Health Act that actually establishes a right of access. An administrator of a health information bank must make available, without request, to an individual that individual's personal health information that is contained in the health information bank. This right of access also applies to records of disclosure directives and audit logs.[81] Although this provision has not been brought into force, it is a good precedent in terms of patient portals.

Portals raise issues related to identification management and authentication. The use of portals also raise difficult issues related to the rights of substitute decision makers and the rights of minors and others to access personal health information. Substitute decision makers and mature minors are recognized in law as having rights and responsibilities in the delivery of health services. Access to portals should reflect those rights and responsibilities.

RECOMMENDATION

The law should recognize the right of individuals to have routine and timely access to their own personal health information through portals; issues raised in relation to substitute decision-makers and mature minors must also be addressed.

➢ Transparency

Individuals have a right to know how their personal health information is being collected, used, disclosed and protected throughout the health sector. Because legislation is published and easily accessible, transparency is best achieved by having as much detail as possible in legislation and regulations rather than in policies. In addition to transparency, a legislative solution can also create important privacy rights and add an increased level of certainty. While a statute is generally higher-level and in many ways enabling, regulations and ministerial orders give the detail, with ease of amendment over statutes offering needed responsiveness to technological and other changes.

The E-Health Act is a good example of legislation that is designed to promote transparency of data flows of personal health information. Under the Act, ministerial orders designating databases as health information banks set out the data elements those databases contain and authorize specific persons to collect, use and disclose

[81] E-Health Act, s. 17.

personal information through them. The purposes for the collection, use and disclosure are also identified and the limits or conditions on collection, use, storage or disclosure are described in detail.

However, the promise of the E-Health Act has not been realized because the Minister of Health has exercised his discretion to designate databases infrequently. To date, just three databases have been designated. Even then, despite repeated requests by our Office, the ministerial orders have not been posted on the Ministry website. This is an inexplicable state of affairs, one that should not be a hallmark of modern health information privacy laws.

Despite the experience to date with the E-Health Act, however, this type of legislation is one way to enhance the transparency of data flows through electronic databases. Should the E-Health Act be applied as originally intended there would be a significant measure of transparency in relation to the provincial EHR system.

Another important facet of transparency that is achieved in comprehensive health privacy law is notification requirements. These raise public awareness of how their personal health information is being collected, used and disclosed.

A properly documented privacy management program goes a long way in terms of transparency. For example, by having written policies and procedures and completing privacy impact assessments, custodians are able to demonstrate to the public how they are protecting personal health information. A description of the privacy management program implemented by custodians to protect personal health information should be made publicly available on a proactive basis.

Transparency is also achieved by the right of individuals to access their own personal health information.

RECOMMENDATION

The law should enhance transparency in relation to data flows of personal health information and privacy and security frameworks.

➢ Flexible rather than prescriptive security standards

Any new legislation to address privacy concerns in the health sector needs to be agile so that it can be applied to changing technologies. That is, flexibility needs to be built in so that the legal requirements keep up with technology.

A good example is s. 30 of FIPPA, which requires public bodies to protect personal information by making *reasonable* security arrangements. This standard of

reasonableness is not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect personal information vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, security. A specific security standard cannot be mandated when technology is changing so rapidly.

This said, consideration should be given to requiring that personal health information not be stored in portable storage devices, including laptops, unless it is absolutely necessary to do so and then only when it is protected by the strongest encryption solution available.

RECOMMENDATION

The law should establish security requirements that are based on a standard of reasonableness so that they can be adjusted to new technologies and changing practices.

➢ Penalties for non-compliance

The potential magnitude and harm of privacy and security breaches is staggering given the nature and amount of personal health information in large EHR systems. It also needs to be kept in mind that the risks of privacy and security breaches are heightened by a number of factors, including the number of users and the costs and challenges of maintaining technical security.

Penalties for failing to adequately protect personal health information should be commensurate with this reality. They should be significant and they should be strictly enforced. The E-Health Act provides for a maximum fine of $200,000 for an unauthorized disclosure. The new Electronic Personal Health Information Protection Act, 2013 in Ontario (Bill 78) provides for a maximum fine of $500,000. In our view, this increased amount is appropriate for EHR systems given the scope of potential breaches.

The Ontario legislation also provides that the standard six month limitation period for provincial offences does not apply. This is because privacy breaches are often not discovered immediately. The typical time period for an audit is two years.

Consideration must be given to an appropriate limitation period for the prosecution of offences in the context of EHR systems.

Recommendation

The law should impose significant penalties for non-compliance, including a maximum fine of $500,000 with an appropriate limitation period.

➢ Oversight by the Commissioner

It is essential that an independent agency monitor implementation of new health information privacy law. Effective oversight and strong enforcement powers are essential because it will help to maintain public trust and confidence in the health care system and help to ensure compliance.

As a regulator, this Office is well placed to assume responsibility for oversight. Commissioners across Canada play this role under health privacy laws in all but one province. At a minimum, the existing mandate of the Commissioner under FIPPA should be replicated in relation to new health information legislation. This would include the ability to:

- review a custodian's response to an access request;
- conduct investigations and audits to ensure compliance;
- make an order;
- inform the public about the legislation and receive comments from the public about its administration;
- engage in or commission research into anything affecting the achievement of the purposes of the legislation;
- review and comment on privacy impact assessments;
- comment on the implications for the protection of privacy of proposed legislation and policies; and
- comment on the implications for access to information or for protection of privacy of automated systems for the collection, storage, analysis or transfer of information.

➢ Mandatory review of privacy impact assessments

It should be mandatory for PIAs regarding proposed administrative practices and information systems and data-linking initiatives in the health sector to be submitted to the Commissioner for review and comment. There is such a requirement in Alberta's

Health Information Act. PIAs must be submitted to the Information and Privacy Commissioner of Alberta for review and comment.[82] Mandatory review by the Commissioner enables relationship-building within the health sector so that there is effective oversight. It allows the Office of the Commissioner to develop a deep and holistic level of understanding of systems and initiatives so that it is in a position to assist custodians with risk assessments, mitigation strategies and high quality breach reporting. Review of PIAs also help to drive compliance with legal obligations and facilitates investigations. Consideration should also be given to requiring STRAs to be submitted to the Commissioner.

Currently in BC, the Commissioner has the responsibility under FIPPA to review mandatory PIAs for common or integrated programs or activities and data-linking initiatives.[83]

➢ Mandatory breach notification

In practice, public bodies and organizations notify this Office when a significant privacy breach has occurred. This occurred, for example, with respect to the three breaches at the Ministry of Health in 2012. In that case, those breaches warranted investigation by this Office to ensure that appropriate steps were taken to remedy the harm and prevent such incidents in future.

However, in BC, it is not a legal requirement to advise our Office of a privacy breach. A legal requirement would help to ensure that this Office is advised of a privacy breach on a consistent basis so that this Office can monitor and provide advice on such issues as the appropriate notice that should be given to individuals. Given the amount and nature of personal health information that could be disclosed in a privacy breach involving EHRs, it should be a requirement in health information privacy law that this Office be notified. The law should also provide for notification of affected individuals, and the public, if there is a risk of significant harm. Precedents exist for this under, for example, Alberta's *Personal Information Protection Act.*[84]

In relation to an investigation of a potential privacy breach involving an interoperable EHR, this Office should have the ability to collaborate on investigations with oversight bodies in other jurisdictions.

➢ Approval of EHR policies and procedures

The Commissioner could play a valuable role in ensuring that the privacy management programs of custodians are up to date and protect privacy adequately. Recent legislation introduced in Ontario requires that the policies and procedures of a prescribed organization such as eHealth Ontario have to be approved by the

[82] *Health Information Act*, RSA 2000, c. H-5, s. 64.
[83] FIPPA, ss. 69(5.2) and (5.4).
[84] *Personal Information Protection Act*, SA 2003, c P-6.5

Commissioner every three years.[85] This requirement warrants serious consideration in this province.

➢ Approval of practices and procedures of a secure research platform

Similarly, in relation to a secure research platform, the Ontario *Personal Health Information Protection Act, 2004* requires the Commissioner to review the practices and procedures of the Institute for Clinical Evaluative Sciences every three years. This is a good model and also warrants serious consideration. Such oversight reinforces public trust and confidence in the conduct of health research.

➢ Data-linking initiatives

Data linking inherently raises risks to privacy because it repurposes information and creates new information. Recent amendments to FIPPA included requirements for public bodies to submit early notice and privacy impact assessments to the Commissioner.[86] However, these requirements do not apply to the integrated health sector.[87] New health information privacy law should give the Commissioner oversight of major data linking initiatives involving linkages of larger repositories or databases of both personal health information and non-identifying health information. This oversight would be similar to that currently exercised by the Information and Privacy Commissioner of Alberta pursuant to the Alberta *Health Information Act*.[88]

➢ Public education

Consistent with the Commissioner's public education role under FIPPA, the law should give the Commissioner the authority to engage in public education about privacy issues in the health sector and the steps individuals can take to protect their personal health information. Because individuals are increasingly becoming responsible for their own personal health information, the importance of public education in this area cannot be overstated. The user-beware message must be understood and individuals need to be empowered to take the necessary steps to protect their privacy. Not only this Office but the Ministry of Health, health authorities, health professionals and organizations all need

[85] Electronic Personal Health Information Protection Act, 2013 (Bill 78), s. 4 (adding new s. 55.3(2) para. 14) to the *Personal Health Information Protection Act, 2004*.
[86] FIPPA, s. 69(5.2), (5.4) and (5.5).
[87] FIPPA, s. 69(5.6).
[88] *Health Information Act*, ss. 32(2) and 70(2).

to devote time, effort and resources into raising awareness of individuals' responsibilities to protect their own personal health information.

RECOMMENDATION

The law should provide the Commissioner with oversight of its administration, including the existing oversight responsibilities of the Commissioner under FIPPA and authorities in relation to the following: mandatory privacy impact assessments, mandatory breach notification, approval of EHR policies and procedures, approval of practices and procedures of a secure research platform, notice and review of data linking initiatives and public education.

CONCLUSION

No one would argue with the need to protect personal health information. It is the most sensitive type of personal information because it is information about our body, our state of mind and our behaviour. As Information and Privacy Commissioner, I am concerned about how this sensitive personal health information is protected in privacy law and policy. I am convinced that new health information privacy law is needed in BC.

Reform of the current complex and fragmented legislative framework is long overdue. The current legislation is inadequate in comparison to legislation in place in other provinces and is out of step with today's dynamic health sector.

This report recommends new tailor-made legislation and policy that will protect the privacy of personal health information in a way that is comprehensive, consistent and forward-looking. It also needs to authorize data flows that are necessary for the efficient and cost-effective delivery of health services in BC and permit appropriate secondary use.

While it is desirable for privacy and security frameworks to have legal force and effect, at the same time, they need to be agile. That is, flexibility needs to be built in so that the legislation is adaptable to new technologies and models of health service delivery.

New health information privacy law needs to properly protect privacy and with the specificity, certainty and transparency that the public deserves. Given current legislative approaches to health information privacy elsewhere in Canada, and abroad, it would not be at all surprising if the government here in British Columbia decided to move forward with new health information privacy legislation. I urge government to move forward on such an initiative consistent with this Special Report and as a matter of high priority.

It is important for British Columbians to enjoy the protection of a comprehensive 21st Century health information privacy law. That law will position BC as a leader in protecting health privacy in Canada in the new dynamics of the health sector. I hope that my prescription for legislative reform will inform that work and that government will fill this prescription at the earliest possible opportunity.

ACKNOWLEDGEMENTS

I would like to thank Helen Morrison, Senior Policy Analyst, who assisted in the preparation of this report.

April 30, 2014

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

SUMMARY OF RECOMMENDATIONS

Government should enact new detailed and comprehensive health information privacy law at the earliest opportunity.

The law should:

1. **define personal health information in a broad and comprehensive manner. Careful consideration should be given to developing a separate definition for genetic or genomic information because of its unique nature;**

2. **include a narrow definition of non-identifying information that takes into account the risk of re-identification;**

3. **define custodian in such a way that the application of the law can be extended as new entities and practitioners collect personal health information. There should also be consideration of distinct provisions for certain data flows;**

4. **authorize only minimum collection; permit indirect collection; and allow multiple purposes for collection;**

5. **require custodians to ensure the accuracy of personal health information;**

6. **permit secondary use but expressly limit it to specific health-related purposes only;**

7. **entrench role-based access models (based on need to know and least privilege privacy principles) with as much granularity as possible and attach penalties for users who violate their conditions of access. Audits should be required;**

8. **establish a single research ethics board for the province and mandate its role and the criteria the board applies, including the *Tri-Council Policy Statement*;**

9. **expand the role of the data stewardship committee, so that a privacy lens is applied consistently in the data access approval process;**

10. **specifically authorize all disclosures for research purposes to the Canadian Institute for Health Information, organizations like Population Data BC or any other secure research platform and require practices and procedures to be reviewed by the Commissioner on a periodic basis;**

11. **require clear governance models and reflect a pan-Canadian approach;**

12. **prescribe essential elements of a privacy management program;**

13. **include notification provisions, with obligations placed on the Minister with respect to the provincial EHR system and also on other custodians;**

14. **give individuals the ability to exercise masking options in relation to the provincial EHR and other electronic record systems;**

15. **establish the right of individuals to know to whom their personal health information has been disclosed from databases that contain clinical information;**

16. **provide individuals with the right to have access to, and request correction of, their own personal health information;**

17. **recognize the right of individuals to have routine and timely access to their own personal health information through portals; issues raised in relation to substitute decision-makers and mature minors must also be addressed;**

18. **enhance transparency in relation to data flows of personal health information and privacy and security frameworks;**

19. **establish security requirements that are based on a standard of reasonableness so that they can be adjusted to new technologies and changing practices;**

20. **impose significant penalties for non-compliance, including a maximum fine of $500,000 with an appropriate limitation period; and**

21. **provide the Commissioner with oversight of its administration, including the existing oversight responsibilities of the Commissioner under FIPPA and authorities in relation to the following: mandatory privacy impact assessments, mandatory breach notification, approval of EHR policies and procedures, approval of practices and procedures of a secure research platform, notice and review of data linking initiatives and public education.**

APPENDIX A

KEY PIECES OF THE "PATCHWORK"OF HEALTH INFORMATION LAWS IN BC

Continuing Care Act**,** s. 5

Authorizes the Ministry and a health authority to require a person to provide information respecting the person or the members of the person's family thought necessary for the proper administration of the Act.

E-Health (Personal Health Information Access and Protection of Privacy) Act

Governs the collection, use and disclosure of personal health information through electronic databases of the Ministry and health authorities that have been designated by the Minister as "health information banks". To date, only applied to a repository of lab data that is part of the provincial EHR system.

Freedom of Information and Protection of Privacy Act

Applies to personal information that is in the custody or control of the Ministry, health authorities, agencies, boards and commissions in the health sector (including the Medical Services Commission) and professional regulatory bodies.

Health Act, ss. 9 and 10

The BC Cancer Agency is authorized to collect, use and disclose information for the purpose of medical research.

The health status registry may request that a person provide it with information concerning congenital anomalies, genetic conditions or chronic handicapping conditions of individuals.

Hospital Insurance Act, s. 7

Authorizes the Ministry or a hospital to require a person to provide information respecting the person or the members of the person's family thought necessary for the proper administration of the Act.

Laboratory Services Act (not in force)

Governs the collection, use and disclosure of personal information by the Ministry in relation to the payment of benefits for laboratory services.

Medicare Protection Act, s. 49

Section 49 provides that individuals must keep matters about beneficiaries and practitioners that come to their knowledge in the course of administering the Act confidential subject to certain exceptions.

Ministry of Health Act*,* Part 2

Authorizes the collection, use and disclosure of personal information by the Ministry from a public body for a stewardship purpose.

Personal Information Protection Act

Applies to personal information that is in the custody or control of organizations, including private practices of health professionals and private labs.

Pharmaceutical Services Act

Governs the collection, use and disclosure of personal information by the Ministry in relation to the payment of benefits for pharmaceutical services. Additionally, it governs access to and recording of information in prescribed information management technology.

Public Health Act

Part 1, Division 3 sets our purposes for collection, use and disclosure of personal information related to reporting of reporting disease, health hazards and other matters.

Health Act Communicable Disease Regulation

Governs the collection, use and disclosure of personal information related to public health matters, including mandatory reporting of infectious diseases or health hazards.