Law and Policy of Public Health Information Sharing in Canada

CGP
Centre of Genomics and Policy
Centre de génomique et politiques

NOVEMBER 2021
Centre of Genomics and Policy

Contents
INTRODUCTION .................................................................................................................. 1

PART I: LEGAL FRAMEWORK .......................................................................................... 3
Section 1: The Structure of Canadian Data Protection Law ................................................. 3
  Defining Personal information ......................................................................................... 3
  Determining the Laws Applicable to a Health Institution ............................................. 5
Section 2: The Substance of Canadian Data Protection Law ........................................... 8
  Powers to Use, Collect, and Disclose Personal Information and Personal Health Information ................................................................. 8
  Provincial Public Health Laws ........................................................................................ 15
  Federal Powers to Collect Personal Information .......................................................... 16
Section 3: The Legal Limits of Personal Information Use ................................................. 17
  Limitations on information use ...................................................................................... 17
Section 4: Other Obligations to Respect in the Use of Personal Information ..................... 20
Section 5: Policy Barriers to Public Health Information Sharing ..................................... 23

PART II: Sharing Information for Public Health Purposes .............................................. 25
Potential Approaches to Sharing Information for Public Health Purposes ....................... 25

PART III: GOVERNANCE STRUCTURES AND TOOLS ............................................. 29
Section 1: Organizational Approaches to Information Governance ................................ 29
  Tool: Core consent elements ......................................................................................... 29
  Tool: Retrospective consent filter ............................................................................... 30
  Tool: Established Access Tiers .................................................................................... 30
  Tool: Data Access Agreement ..................................................................................... 32
  Tool: Policies to Incentivize Information Sharing ....................................................... 32
Section 2: Technological Approaches to Information Governance ................................ 33

CONCLUSION ................................................................................................................. 37
APPENDIX A: Provincial Health Sector Institution Powers to Use and Disclose Personal Information and Personal Health Information ................................................................. 40

APPENDIX B: Comparison of Provincial Public Health Acts ............................................ 61
APPENDIX C: Comparative Powers to Collect Personal Information – Federal and Provincial Public Sector Institutions ................................................................. 65
APPENDIX D: Using or Sharing Information and Research Participant Consent ................ 69

APPENDIX E: Security Safeguards .................................................................................... 73
APPENDIX F: Primer on Technological Approaches to Information Governance ......... 76
  Tool: Quantitative Assessments of Information Identifiability ........................................ 76
  Tool: Differential Privacy and Genomic Beacon Systems ............................................. 77
  Tool: Model-to-Data Approaches – Federated Learning and Swarm Learning ............ 78
  Tool: Homomorphic Encryption and Secure Multi-Party Computation ...................... 79

APPENDIX G: Sharing Anonymized Information .............................................................. 80
APPENDIX H: Opportunities From Virus Genomic Data: Summary ............................. 84
REFERENCES .................................................................................................................. 87
Law and Policy of Public Health Information Sharing in Canada

A Report to the Public Health Agency of Canada

Alexander Bernier, Hanshi Liu, Robyn McDougall, Yann Joly*

Abstract: In the face of the COVID-19 pandemic, Canadian researchers and public health agencies have struggled to assemble and disseminate the large quantities of information required to perform research that would promote evidence-based public health interventions. Barriers to information exchange include the decentralized information collection efforts of public health laboratories, researchers, and healthcare institutions, and a lack of incentives for such institutions to invest in the harmonization and centralization of information. Further, Canadian data protection legislation, public health law, and the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS-2) all create a complex landscape of rules applicable to such information exchanges.

Our legal analysis indicates that numerous lawful paths to the pan-Canadian dissemination of information exist. One approach is to anonymize information in reliance on a combination of de-identification methods and organizational controls. Invoking the broad information collection powers of governments and government agencies to obtain and transmit the necessary information is another potential approach. The statutory powers of public health agencies can also be relied on to mobilize information for reasons of public health surveillance or public health intervention. Last, access can be requested to the data of health information custodians, such as hospitals, for research purposes. To promote the implementation of a harmonized approach to health information exchange in Canada, the adoption of new laws or of regulations to existing laws is required. The applicable laws are unharmonized, inconsistent, and sometimes ambiguous. Moreover, these laws can impose undue restrictions or a significant administrative burden on the use of information. To ensure that Canada’s provincial and federal public health agencies are capable of responding to emergent public health crises in a coordinated manner, laws or regulations should be implemented to establish that data sharing is permitted for public health purposes, including research, all throughout Canada according to simple and uniform preconditions. If these changes are not implemented, Canada will struggle to match the efforts made by other members of the G20 to protect the health of its citizens and to address future epidemic and pandemic threats.

*The authors would like to thank Katherine Cheung and Sina Faraji of the Centre of Genomics and Policy at McGill University for editorial assistance. We would also like to acknowledge the support of Genome Canada, CanCOGeN ViruSeq and the Expert Advisory Group (EAG) to the Conference of Deputy Ministers of Health (CDMH).
EXECUTIVE SUMMARY

During the national SARS epidemic and the COVID-19 pandemic, Canada has struggled to bring together and disseminate public health information. Contributing factors include a policy environment that disfavors inter-institution information exchange, and unharmonized legal requirements. In this report, we propose potential paths to increased information sharing that draw on the existing legal powers of public health authorities, government bodies, and healthcare institutions. Healthcare institutions should operationalize these recommendations to ensure that public health research in Canada is rapid, responsive, and cost-effective.¹ Further legal reforms are proposed, to transition Canada from a restrictive model of information custodianship to a flexible model of ongoing information stewardship in the public interest.

Part I: General overview of Canadian data protection legislation

Canadian data protection legislation allows the collection, use, and disclosure of personal information (PI) and personal health information (PHI) if specified conditions are met. The law creates powers that enable federal and provincial public health institutions to collect, use, and disclose such information for purposes related to public health surveillance, intervention, and research. Moreover, federal and provincial government institutions also have general powers to collect, use, and disclose personal information for purposes related to their operating programs and activities. Further, the secondary use of such information for research purposes is often permissible, in compliance with applicable formalities, some enshrined in law and others in the Tri-Council Policy Statement (TCPS-2). Provincial health sector institutions that are subject to health sector data protection laws, such as clinics and laboratories, however, are often more circumscribed in their powers than are federal and provincial government institutions that are subject to federal and provincial public sector data protection laws.

Despite Canadian data protection law enabling the use of PI and PHI, there remain significant legal impediments to the flow of data between Canadian health sector institutions. The powers to use information and the associated formalities are distinct in each Canadian jurisdiction (i.e., in each province and at the federal level). Within each, different sector-specific laws may apply. Sometimes, multiple laws can apply to an institution at the same time. The fragmented structure of data protection legislation is suboptimal for information sharing between stakeholders located in different Canadian provinces and operating across distinct economic sectors (the health sector, the private sector, and the public sector). In the subsequent Parts, we summarize the rules applicable to information sharing in Canada, distinguishing them according to the nature of the entities using information and the anticipated purposes of use. We conclude with recommendations for the future.

Part II: Recommendations

This report articulates two categories of recommendations. The first are recommendations directed to Canadian institutions and organizations that intend to share information for public health purposes, including public health research, in accordance with the law as it currently exists. The second are recommendations directed to Canadian legislators and Canadian data protection regulators. These latter recommendations propose reforms to Canadian data protection legislation to facilitate the sharing of information for public health purposes and public health research purposes.

Recommendations for sharing information in compliance with data protection law

**Provincial and federal public health institutions should exercise their legal powers to collect, use, and disclose personal information for public health purposes to their full extent. Federal public health institutions should use their powers in the Privacy Act to their full extent.**

The powers of provincial health sector institutions, and of provincial public health institutions, to share personal health information differ considerably across provinces. In some provinces, the narrow powers of such institutions can inhibit their ability to share information.

In these cases, PI and PHI can still be used for secondary research purposes with the approval of the relevant information custodian and/or the approval of a competent Research Ethics Committee (REC). As each information custodian and REC can impose discretionary conditions on such information sharing, this approach is not streamlined enough to enable a harmonized national strategy to share PI and PHI for research.

Some institutions and organizations will not have sufficiently broad statutory powers to share personal information and personal health information as desired for public health purposes or public health research purposes.

Nonetheless, it is possible for these actors to share information in anonymized form. Information is considered anonymized if there is no ‘serious possibility’ that an individual could be re-identified through the use of that information, alone or in combination with other available information. A combination of de-identification methodologies and organizational governance measures can be used to anonymize information.

---

2 *Privacy Act*, R.S.C., 1985, c. P-21 at ss. 4, 7, 8. See also: *Canada (Syndicat des agents correctionnels) c. Canada (Procureur général)* 2019 FCA 212, 309 A.C.W.S. (3d) 78 at paras 8, 42-44.
Recommendations for Canadian data protection law reform

First, Canadian data protection legislation should be amended to stipulate in clear language that personal information and personal health information can be collected, used, and disclosed for public health purposes, including research, in combination with appropriate de-identification and good information stewardship practices. This could ideally be achieved through the adoption of special purpose federal legislation or through a legislative amendment, enabling by default the secondary use of personal information and personal health information for the purposes of public health surveillance, public health intervention, and public health research in the public interest.

These changes are intended to transition Canada from a model of information custodianship, which requires institutions and organizations to strictly limit their uses of personal information and personal health information to the minimum necessary, to a model of information stewardship. The information stewardship model would empower Canadian institutions and organizations to retain personal information and to use their judgment to authorize its secure use for future public health purposes. This transition is needed to ensure that public health authorities can deliver public health interventions to Canadians that attain the standard of other G7 economies, and to ensure a coordinated national response to future epidemic and pandemic threats.

Second, Canada should create a central institution responsible for public health information stewardship. This institution would be responsible for directing the use of health-related information for research purposes and other purposes in the public interest. The institution would be invested with the legal authorization, organizational structure, and technological and human resources necessary to fulfill its functions. It could also develop policies and standards enabling other institutions to achieve a high standard of technical and legal interoperability.

Third, legislation or research funding agreements should require public health institutions, both federal and provincial, to appoint a specialist staff member responsible for promoting and monitoring information sharing. These individuals would facilitate the transition from a closed and competitive public health research culture, towards a more open and transparent one. They would also be accountable representatives of their institutions that could be easily reached in case of unexpected problems and delays in information sharing.

Fourth, penal sanctions could be imposed for performing the illicit re-identification of individuals, and/or for failing to share information necessary for public health surveillance and public health intervention in a timely manner. The first of these penal sanctions could be modelled on Section 171 of the United Kingdom Data Protection Act 2018 (DPA 2018). The second one, while more challenging to formulate and implement, would nevertheless send a clear signal about the importance of information sharing for public health.

---

3 Ballantyne & Schaefer, “Public interest in health data research: laying out the conceptual groundwork” (2020) J Med Ethics. 6 (9):610-616.
INTRODUCTION

The SARS-CoV-2 (COVID-19) virus was first reported in Canada in January 2020; with subsequent community transmission being confirmed in mid-March. Since then, the virus has resulted in approximately 80,000 hospitalizations across the country. The scientific community was faced with the daunting task of advancing our knowledge and developing both tests and vaccines to address the ensuing pandemic as a matter of urgency.

Given the recent epidemic outbreaks of Ebola, Zika, and SARS, Canada had every reason to be well-prepared to conduct COVID-19 research. Yet on one key indicator of performance, that of information sharing for health research, Canada’s performance has been shamefully low. Information sharing for research between public health agencies, academic and private researchers, and the international community was slow, disparate, uncoordinated, and generally inadequate. This state of affairs has resulted in a suboptimal response to the pandemic and reflected poorly on Canada’s public image.

Emerging COVID-19 variants that can infect immunized individuals, especially if they can cause severe disease, must be rapidly identified and addressed as part of an efficient Canadian public health strategy. Detecting whether such variants are emerging is particularly challenging, in part because transmission is a group-level phenomenon, and because only a minority of COVID-19 infections cause severe disease. Furthermore, at the time of emergence, a new variant will necessarily occur in small numbers. These factors highlight the need to link multiple information sources together and to pool information across jurisdictions, in order to have the strongest possible statistical signal and the widest possible lens on the virus’ evolving phenotype. New COVID-19 variants can emerge anywhere, and Canadian public health researchers need to be in a much better position to detect emerging variants of public health concern in Canada. SARS-CoV-2 whole genome sequences are fundamental to this task, which requires not only sequence data but also information about transmissibility, severity, and immune escape.

This report addresses legal and policy challenges that may explain Canada’s poor performance as regards information sharing, and proposes policy options to facilitate information sharing in the future. Limitations arising from data protection legislation alone do not explain the present lack of information sharing. Information exchange is still not perceived to be a priority by most stakeholders in the Canadian health data ecosystem. Further, public health laboratories in Canada work under a veil of secrecy and demonstrate little interest in benefiting from the assistance of external collaborators to maximize the utility of their health datasets.

7 Ling, “Canada’s public health data meltdown” (7 April 2021), online: Macleans.ca.
8 See Appendix H for further details.
This report is divided into three Parts. The first describes the applicable legal and policy frameworks that govern data protection, public health, and research ethics at the provincial and national levels. To avoid imposing on non-expert readers, we have included more detailed legal information tables in Appendices A, B, C, and D of the report. Thus, the first Part provides an overview of the similarities, constraints and tools in the Canadian legal ecosystem. The first Part ends with a short reminder of further policy challenges that limit Canadian public health information sharing, other than those arising from the law. The second Part draws from this analysis to identify the most promising policy paths that could be used to share health information for research purposes, especially in future epidemics and pandemics. The third Part describes organizational and governance tools that can facilitate the adoption of these promising approaches. To enable the comprehension thereof, the technical aspects of select organizational and technological tools are described in Appendices D and F of the report. The report closes with some short remarks and recommendations for legislative reform that would facilitate data sharing in Canada. During both the COVID-19 pandemic and its precursor, the SARS outbreak of the early 2000s, Canada’s performance in coordinating public health data sharing has proven substandard relative to other developed economies. There is an urgent need to review priorities, policies, and practices to contribute to the global effort at a level commensurate with Canada’s high level of scientific and human development.

While these will not be detailed in the report, we note the recent efforts of Canada’s First Peoples, Inuit, and Métis communities to develop data infrastructures for the purpose of collecting and stewarding health-related information for research purposes. The First Nations Information Governance Centre (FNIGC) was created by First Nations leaders across Canada, and provided with funding in Canada’s 2018 Federal budget. The FNIGC was mandated to develop Canada’s First Nations Data Governance Strategy. FNIGC deposited the completed strategy in the Spring of 2020. Future efforts of the FNIGC are intended to create ten regional data governance centres dedicated to actualizing First Nations data stewardship and information sharing networks. Inuit Tapiriit Kanatami (ITK), the national representative organization for 65 000 Inuit in Canada, the majority of whom live in Inuit Nunangat, adopted a National Inuit Strategy on Research in 2018. The strategy identifies the need for coordinated action to “develop Inuit-specific guidelines on data accessibility, ownership, and control.”

---

PART I: LEGAL FRAMEWORK

Section 1: The Structure of Canadian Data Protection Law

Defining Personal information

Canada’s data protection laws use the criterion of ‘identifiable personal information’ to distinguish information that is regulated from that which is not.\textsuperscript{14} Non-identifiable information is not captured by Canadian data protection law.\textsuperscript{15}

Canadian data protection law establishes a double criterion for information to be considered regulated personal information, rather than being non-regulated anonymous or anonymized information. First, the information must be personal in nature. Second, the information must relate to an identifiable natural person. We will consider these elements in turn.

The ‘about’ criterion

To be ‘personal’ in nature, information must be ‘about’ or be ‘related to’ a natural person.\textsuperscript{16} Information that relates to a natural person is usually considered to be ‘personal.’\textsuperscript{17} This means that there must be an appreciable relationship between the individual and the information that relates to them. Courts have often held that information that relates to something that is external to a person, such as a feature of the natural world, an object, or the person’s professional activities, might not be considered that individual’s ‘personal information’ even if there is a close relation between the concerned person and the external object to which the information relates.\textsuperscript{18}

In 2018, the Federal Court of Appeal in \textit{Husky Oil Operations Limited v Canada-Newfoundland and Labrador Offshore Petroleum Board} narrowly interpreted prior Supreme Court of Canada decisions that contemplated the definition of personal information.\textsuperscript{19} The court in \textit{Husky Oil} held that it was necessary to consider whether information “[relates] to the intimacy and the core identity of an individual, and [that the definition of personal information refers] to the type of information the dissemination of which a person would prefer to control.”\textsuperscript{20} The court further

\textsuperscript{15}This includes both anonymized information, information that was collected in identifiable form but is no longer identifiable, and anonymous information, which was originally collected in a non-identifiable format. These terms do not have defined legal meaning. The law considers information to be non-identifiable if there is no ‘serious possibility’ of the individual being re-identified, in reliance on the information alone or in combination with other available information. (See \textit{Gordon v Canada (Minister of Health)} 2008 FC 258 at paras. 34-35, \textit{infra} n. 24).
\textsuperscript{16}\textit{Dagg v. Canada (Minister of Finance)} [1997] 2 SCR 403 at para 69, [hereinafter \textit{Dagg}].
\textsuperscript{17}\textit{Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board)}, 2006 FCA 157, [2007] 1 FCR 203 at paras 52-53 [hereinafter \textit{Nav Canada}].
\textsuperscript{19}\textit{Husky Oil Operations Ltd. v Canada-Newfoundland and Labrador Offshore Petroleum Board} 2018 FCA 10 at paras 27-45 [hereinafter \textit{Husky Oil}].
\textsuperscript{20}\textit{Ibid} at para 38.
assessed whether information relates to individual “dignity or identity” and to the individual’s “reasonable expectation of privacy,” in characterising information as personal or non-personal.21

The effect of this determination is to narrow the ambit of ‘personal information’ in Canadian data protection law. This suggests that Canadian data protection legislation protects only information in which an individual has a reasonable expectation of privacy – similar to the approach adopted in Canadian constitutional and criminal law – rather than granting individuals broad rights in all information that relates to them, however remotely.22 This means that information that relates to individuals, but does not implicate their personal privacy, is not considered to be personal information according to Canadian law.23

The ‘identifiable’ criterion

The definitive test for determining if information relates to an identifiable natural person is established in the 2008 landmark decision Gordon v Canada.24 The court established that “information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.”25 Available information includes public information and other information that is reasonably considered to be available in the context of the concerned information’s use.26 This test has also been expressed as considering whether a ‘reasonable expectation’ of individual re-identification exists.27

In consideration of the above definitions, the following conclusions can be drawn:

a. Rich health information about a natural person could potentially constitute identifiable personal information even if all direct identifiers are removed, if there remains a ‘serious possibility’ of the concerned individual being re-identified using other available information. Direct identifiers are elements that include name, civic address, and social security number. These are appellations and unique characteristics that inherently allow an individual that has knowledge of them to single out the concerned individual from amongst the general population.28

21 Ibid at para. 39. This is consistent with the Federal Court of Appeal’s prior decision in Nav Canada, which stipulated that personal information must be ‘private’ in nature (the Supreme Court refused to grant leave to appeal this conclusion). See: Nav Canada, supra n. 17.
23 However, Supreme Court jurisprudence that predates Husky Oil and Nav Canada sometimes adopts a more expansive definition of personal information. Therefore, it may be prudent to consider information personal if it ‘relates to’ an identifiable person – regardless of whether the concerned individual has a reasonable expectation of privacy relative to such information. See e.g.: Dagg, supra n. 16. See also: Canada (Information Commissioner) v. Royal Canadian Mounted Police Commissioner 2003 SCC 8, [2003] 1 S.C.R. 66.
24 Gordon v Canada (Minister of Health) 2008 FC 258 at para 34.
25 Ibid at paras. 33-34.
27 Canada (Information Commissioner) v. Canada (Public Safety and Emergency Preparedness), 2019 FC 1279 (CanLII) at para 53.
b. Information that bears a low risk of causing individual re-identification, and aggregate information from multiple natural persons, is not identifiable personal information.

c. Information governance practices are relevant to determining whether information is considered to be identifiable or not, as confirmed in case law.\textsuperscript{29} Indeed, Canadian courts appear to presume that information that is indirectly identifiable\textsuperscript{30} will not be considered personal information when it is held in controlled access and not disclosed to the public.\textsuperscript{31} Therefore, information that might be identifiable if released to the public can often be considered anonymized\textsuperscript{32} if held in controlled access.\textsuperscript{33}

Some Canadian laws use different definitions of ‘personal information’ or ‘personal health information’\textsuperscript{34} that limit or nuance the categories of information that such laws capture. Nonetheless, case law and Canadian Privacy Commissioners’ guidance interpret these definitions of ‘personal information’ in a similar fashion.\textsuperscript{35}

\textbf{Determining the Laws Applicable to a Health Institution}

The structure of Canada’s data protection laws can create challenges in determining the laws that are applicable to different types of institutions and organizations.\textsuperscript{36} Canadian legislators have implemented three general categories of data protection law.

\textsuperscript{29} O’Grady v. Canada (Attorney General), 2017 FC 167 at paras 60-61.
\textsuperscript{30} Information that is indirectly identifiable can be or could potentially be associated to the concerned individual through the use of data elements that alone do not enable the re-identification of the underlying person, but could in combination with numerous such data elements. For example, personal attributes such as age, gender, nationality, and profession do not alone allow for the identification of the individual referred to, but a sufficient number thereof in combination could lead to individual re-identification.
\textsuperscript{31} O’Grady v. Canada (Attorney General), supra n. 29 at para 59.
\textsuperscript{32} Ontario IPC, supra n. 26 at pp. 13-17.
\textsuperscript{33} Controlled access refers to the practice of holding datasets according to stipulated conditions of governance that incorporate both organizational and technological access controls, as well as oversight bodies responsible for administering access requests to the datasets held.
\textsuperscript{34} Personal health information is personal information that health sector data protection legislation applies to. Functionally, personal health information is sufficiently similar to personal information that the two terms can be considered interchangeable, except that public sector and private sector data protection legislation refer to ‘personal information’ and health sector data protection legislation refers to ‘personal health information.’ Canadian legislation defines ‘personal health information’ to include enumerated categories of personal information concerning health status, healthcare provision, healthcare payment information, and “identifying information about an individual that is contained in a record that contains personal health information.” Personal information that is in a record that contains enumerated categories of PHI will, therefore, also be considered PHI.
\textsuperscript{35} Alberta’s Health Information Act is, however, a notable exception. Numerous provisions in the Alberta HIA only apply to information if the concerned individual’s identity can be ‘readily ascertained’ from the information. This means that most of Alberta’s HIA does not apply to some of the information to which other data protection laws in Canada would apply. The majority of its provisions are not applicable to information that is not identifiable without reliance on external datasets or complex re-identification methodologies. This law therefore creates a less onerous legal compliance burden than do other Canadian data protection laws. In Alberta, the use of information will not be regulated unless it is easy to identify the underlying person to whom that information relates. (External datasets are those that that are not directly available to the information custodian, but rather are available in other, public or controlled access data repositories or websites).
\textsuperscript{36} Attaran & Houston, supra n. 5.
Public sector legislation

The first are public sector data protection laws, applicable to both federal and provincial government institutions. Federal government institutions are bound by the Privacy Act and the Access to Information Act. Each Canadian province and territory has enacted similar statutes applicable to the government institutions of the concerned province or territory.

Private sector legislation

Second, private sector organizations in Canada are subject to specific data protection laws. The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to private sector uses of personal information across multiple provinces. For private sector uses of personal information that are internal to a single province, PIPEDA is applicable if the province has not implemented a domestic data protection law that the federal government has declared substantially similar. The ‘substantially similar’ designation means that the law has been designated as providing a similar standard of privacy as does the federal PIPEDA, and that PIPEDA will not apply to uses of data to which that law is applicable.

Alberta, British Columbia, and Quebec have adopted laws displacing PIPEDA in the private sector. PIPEDA is not applicable to province-internal information uses in Alberta, British Columbia, or Quebec. However, PIPEDA applies to information uses in Alberta, British Columbia, and Quebec that are cross-provincial or that cross international borders.

Health sector legislation

Third, health sector data protection law applies in addition to or instead of the relevant public sector or private sector law otherwise applicable. Health sector legislation applies to the use of personal health information by specified health information custodians. This term refers to enumerated categories of healthcare practitioners and health institutions, albeit the definition varies from statute to statute.

Health information custodians often include healthcare practitioners, hospitals, laboratories, and community health centres, amongst others. Ontario, New Brunswick, Newfoundland and

39 For PIPEDA to be applicable, organizations, including both for-profit and non-profit organizations, must use information in the “course of commercial activities.” The concept of commercial activities has received a broad interpretation from courts and Privacy Commissioners. Nonetheless, PIPEDA does not apply to universities and hospitals in most instances. The Office of the Privacy Commissioner of Canada considers the majority of the activities of public universities and public hospitals not to be subject to PIPEDA, even where these institutions charge fees for their services. This is principally because Canadian constitutional law establishes universities and hospitals to be a matter of provincial competence, and PIPEDA is a federal law.
41 Canada OPC, “Provincial laws that may apply instead of PIPEDA” (2020).
42 Ibid.
43 Personal Health Information Protection Act, S.O. 2004, c. 3, Sched. A.
44 Personal Health Information Privacy and Access Act, S.N.B. 2009, c. P-7.05.
Labrador,\textsuperscript{45} and Nova Scotia\textsuperscript{46} have implemented health information laws that are deemed substantially similar to PIPEDA, and therefore find application instead of PIPEDA if both would otherwise be applicable.\textsuperscript{47} Alberta,\textsuperscript{48} British Columbia,\textsuperscript{49} Manitoba,\textsuperscript{50} the Northwest Territories,\textsuperscript{51} Prince Edward Island,\textsuperscript{52} Quebec,\textsuperscript{53} Saskatchewan,\textsuperscript{54} and Yukon\textsuperscript{55} have implemented health information laws that are not deemed substantially similar to PIPEDA. If such institutions are engaged in the use of personal data in the “course of commercial activities,” PIPEDA would likely find application in addition to the health sector laws.\textsuperscript{56}

\textsuperscript{45} Personal Health Information Act, S.N.L. 2008, c. P-7.01.
\textsuperscript{46} Personal Health Information Act, S.N.S. 2010, c. 41.
\textsuperscript{48} Health Information Act, R.S.A. 2000, c. H-5.
\textsuperscript{49} E-Health (Personal Health Information Access and Protection of Privacy) Act, S.B.C. 2008, c. 38.
\textsuperscript{50} Personal Health Information Act, C.C.S.M., c. P33.5.
\textsuperscript{51} Health Information Act, S.N.W.T. 2014, c. 2.
\textsuperscript{52} Health Information Act, R.S.P.E.I. 1988, c. H-1.41.
\textsuperscript{53} Act respecting health services and social services, R.S.Q., c. s-4.2.
\textsuperscript{54} Health Information Protection Act, S.S. 1999, c. H-0.021.
\textsuperscript{55} Health Information Privacy and Management Act, S.Y. 2013, c. 16.
\textsuperscript{56} Canada OPC, “Provincial laws that may apply instead of PIPEDA,” supra n. 41.
Section 2: The Substance of Canadian Data Protection Law

Powers to Use, Collect, and Disclose Personal Information and Personal Health Information

Canadian data protection law authorizes the collection, use, and disclosure of personal information and personal health information in certain circumstances. The rules governing how information can be collected, used, and disclosed differ in each province. Such differences exist both across the laws of different provinces, and within different sector-specific statutes internal to a single province (i.e., health sector, private sector, public sector). There are however elements common to multiple Canadian statutes, which include the following:

Consent:

Personal information about an individual can be collected, used, or disclosed with that individual’s consent. Consent must respect certain legal formalities, which differ according to each law. For medical information and other sensitive categories of information, such consent must often be explicit. For less sensitive information, implied consent is sometimes sufficient. The form of consent must be aligned with the reasonable expectations of the individual.

Public sector institutions:

Public sector institutions have broad powers to collect, use, and disclose personal information and personal health information for the purpose of performing their functions (i.e., operating specific programs or activities) without the consent of concerned individuals.

---

58 Canadian law, unlike, for example, the principal data protection law of the European Union (the General Data Protection Regulation), does not distinguish between sensitive and less sensitive categories of information using enumerated categories of sensitive information. Instead, data is contextually assessed to determine if it is ‘highly sensitive.’ If information is considered to be highly sensitive, additional measures are often required to safeguard such information, and individuals must provide explicit consent rather than implied consent to the use thereof – provided, naturally, that consent is the legal justification for the collection, use, or disclosure of such information. Though there is no formal list of the categories of personal information that are considered sensitive, the following categories of information have often been considered sensitive: medical information, information about work performance, payroll information, and some forms of biometric information. (Canada OPC, “PIPEDA Interpretation Bulletin: Safeguards” (2015)).
60 Ibid at para. 27.
Though the definition used is variable in different federal and provincial statutes, public sector institutions often include bodies such as government ministries, government service providers, and hospitals.\textsuperscript{63}

Research:

Public sector institutions, private sector organizations, and health sector institutions can often disclose personal information and personal health information to allow authorized third parties to perform research.\textsuperscript{64}

Information custodians in the public sector or the health sector can, at their discretion, disclose personal information or personal health information for secondary research use if certain necessary formalities are met by the researcher requesting access. The discretion of health information custodians is not without its limits. Courts have established that health information custodians can exclusively consider the criteria that the law specifies in deciding to allow or to refuse researchers access to the personal information or personal health information requested.\textsuperscript{65}

The criteria established in law include, in most instances, the following: 1) The anticipated research purpose is not frivolous. 2) The research cannot be completed without personal information. 3) The research will be performed in a manner that preserves the confidentiality of the personal information used.\textsuperscript{66} Such permission can be granted to allow the secondary research use of information, even without the consent of the individuals to whom the information relates.

\begin{itemize}
\item Information and Protection of Privacy Act, S.N.W.T. (Nu) 1994, c. 20 at ss. 40 (c), 43 (a), 48 (a).
\item Ontario: Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 at ss. 38 (2), 41 (1) (b), 42 (1) (b).
\item Quebec: Act respecting Access to documents held by public bodies and the Protection of personal information, R.S.Q. c. A-2.1, at ss. 64, 65. 1, 68 (1).
\item Yukon: Access to Information and Protection of Privacy Act, S.Y. 2019, c.15 at ss. 15 (c), 21 (b) (i), 25 (a), 25 (c) (i).
\item Ontario Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 at s. 2 (1).
\item Consider e.g.: Ontario Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 at s. 2 (1).
\item Consider the following examples: Act respecting Access to documents held by public bodies and the Protection of personal information, R.S.Q., c. A-2.1 at art. 125. Act respecting health services and social services, R.S.Q., c. S-4.2 at art. 19.3. Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, at ss. 7 (2) (c), 7 (3) (f).
\end{itemize}
Applicable formalities often include the following:

- Deposit of a research plan.\(^{67}\)
- Approval by a competent Research Ethics Committee.\(^{68}\)
- Approval by a health information custodian or equivalent professional (at the custodian’s discretion, in consideration of the criteria established in the law).\(^{69}\)
- Contractual agreement to comply with conditions imposed by the ethics committee and/or the custodian.\(^{70}\)

In addition to these requirements, institutions or organizations that use personal information for research purposes can be required to respect further requirements. Such requirements are established both in the public sector data protection legislation, as well as in the Tri-Council Policy Statement (TCPS-2). The Tri-Council Policy Statement is Canada’s federal granting councils’ research ethics guidance.\(^{71}\) The TCPS-2 applies to all research that receives federal research funding or that is conducted in institutions that benefit from federal research funding.\(^{72}\)

Many other institutions, private or public, operating in Canada have also voluntarily bound themselves to the requirements of the TCPS-2.

\(^{67}\) **Provincial laws:** Alberta HIA at s. 49. Manitoba PHIPA at s. 24 (3). Nova Scotia PHIA at s. 59 (1), 59 (2). Ontario PHIPA at s. 44 (1) (a), 44 (2). Prince Edward Island HIA at s. 30. Prince Edward Island FIPPA at ss. 39, 40. Such a requirement is also implicit in a number of other statutes.

\(^{68}\) **Provincial laws:** Alberta HIA at s. 50 (1). NL ATIPPPHA at s. 44. Nova Scotia PHIA at ss. 57 (b), 59. Ontario PHIPA at ss. 44 (1) (a), 44 (3). NWT HIA at ss. 69-70. Prince Edward Island HIA at ss. 22 (5) (m), 30. Prince Edward Island FIPPA at ss. 39, 40. Saskatchewan: HIPA at s. 29 (1) (b). Yukon HIPMA at s. 68.

\(^{69}\) **Federal laws:** Privacy Act at s. 8 (2) (j), PIPEDA at s. 7 (3) (f) (must also inform the Privacy Commissioner). **Provincial laws:** Alberta FIPPA at s. 42 (c). Alberta HIA at s. 53 (1). British Columbia FIPPA at s. 35 (1) (c). British Columbia PIPA at s. 21 (1). Manitoba FIPPA at ss. 47 (1), 47 (4). Manitoba PHIPA at s. 24 (2). NB RIPPA at s. 47 (2) (b). NB (health sector) PHIPAA at s. 43 (1). NL (health sector) ATIPPPHA at s. 44. NL (public sector) ATIPPA at ss. 70, 70 (c). NWT HIA at ss. 76, 78. NWT ATIPPA at s. 49 (c) (also applies to Nunavut). Nova Scotia PHIA at s. 31 (h), 56. Nova Scotia FIPPA at s. 29 (c). Ontario FIPPA at s. 21 (1) (e). Ontario PHIPA at s. 44 (1). Prince Edward Island HIA at s. 32 (1). Prince Edward Island FIPPA at ss. 39, 40. Quebec AR-HSS (health sector): at s. 19.2. Quebec (public bodies) APPPI at s. 125 (the CAI is required to approve access to the data of public bodies for research purposes). Saskatchewan FIPPA at s. 29 (1) (k). Saskatchewan HIPA at s. 29 (1). Yukon ATTIPA at s. 38. Yukon HIPMA at s. 68 (1).

\(^{70}\) **Federal laws:** Privacy Act at s. 8 (2) (j). **Provincial laws:** Alberta FIPPA at s. 42 (c). Alberta HIA at s. 53 (2). 54. British Columbia FIPPA at s. 35 (1) (d). Manitoba FIPPA at ss. 47 (1), 47 (4). Manitoba PHIPA at s. 24 (4). NL (public sector) ATIPPA at s. 70 (d). NWT HIA at s. 80. NWT ATIPPA at s. 49 (d) (also applies to Nunavut). Nova Scotia PHIA at s. 60. Nova Scotia FIPPA at s. 29 (c). Ontario FIPPA at s. 21 (1) (e) (iii). Ontario PHIPA at s. 44 (1) (b), 44 (5). Prince Edward Island HIA at s. 32 (2). Prince Edward Island FIPPA at ss. 39, 40. Quebec AR-HSS (health sector) at s. 19.2. Quebec (public bodies) APPPI at s. 125 (the CAI is required to approve access to the data of public bodies for research purposes). Saskatchewan FIPPA at s. 29 (1) (k). Saskatchewan HIPA at s. 29 (1) (c). Yukon ATTIPA at s. 38. Yukon HIPMA at s. 69 (1).


The TCPS-2 requires researchers to demonstrate that the following conditions are met,\(^73\) to use identifiable personal information without consent for the purpose of their research:\(^74\)

a. “identifiable information is essential to the research;
b. the use of identifiable information without the participants’ consent is unlikely to adversely affect the welfare of individuals to whom the information relates;
c. the researchers will take appropriate measures to protect the privacy of individuals and to safeguard the identifiable information;
d. the researchers will comply with any known preferences previously expressed by individuals about any use of their information;
e. it is impossible or impracticable\(^75\) to seek consent from individuals to whom the information relates;”\(^76\)

The concerned Research Ethics Committee (REC) is responsible for assessing researchers’ compliance with the above criteria. The TCPS-2 also requires that researchers obtain REC approval to perform information linkage (i.e., to combine multiple independent sources of information about the same individuals).\(^77\) The TCPS-2, unlike Canadian data protection statutes, requires that researchers obtain REC approval prior to conducting research using anonymized information, that is, information that was collected in an identifiable format and subsequently rendered non-identifiable.\(^78\)

Health sector legislation stipulates that a Research Ethics Committee (REC) must perform the aforementioned review. In the public sector, the head of the institution or an equivalent executive is generally responsible for assessing compliance with the above criteria, instead of the Research Ethics Committee. Private sector organizations are subject to different and often less strict requirements in disclosing information for research purposes.\(^79\)

\(^73\) Canada Tri-Council. Tri-Council Policy Statement II (TCPS-2), supra n. 71. Chapter 5: Privacy and Confidentiality at art. 5.5 (B).

\(^74\) Ibid at s. 5.5. (A).

\(^75\) The TCPS-2 specifies that impracticable means more than “mere inconvenience,” and requires that the associated efforts would “[jeopardize] the conduct of the research.” (TCPS-2, 2018, at p. 196).


\(^77\) Ibid at s. 5.7.

\(^78\) Ibid at art. 5.5. (B).

\(^79\) Provincial private sector data protection laws each regulate the use or disclosure of personal information in a different manner. To reiterate, such laws have been implemented in Alberta, British Columbia, and Quebec. In Alberta, there is no general provision allowing private sector institutions to use or disclose personal information for research purposes. This creates a somewhat unusual scenario in which inter-provincial uses or extra-provincial disclosures of personal information appear to be permissible (because PIPEDA is applicable to these uses rather than the Alberta legislation) – but private sector research uses internal to Alberta are not permissible (because the Alberta legislation supersedes the application of PIPEDA as it is considered ‘substantially similar’ legislation). In British Columbia, for-profit and non-profit private sector organizations, regardless of their engagement in commercial activities, are subject to the B.C. Personal Information Protection Act. The Act establishes that
Health sector quality assurance and health system planning purposes:

Most health information laws create explicit powers to use and to disclose personal health information for healthcare planning and quality assurance purposes.80

Such powers bear certain limits:

- Healthcare institutions in Ontario and Quebec do not hold broad and general powers to disclose personal information or personal health information for healthcare planning purposes.81
- Disclosures made in British Columbia82 for such purposes require the disclosed information to remain within Canada (albeit this requirement has been relaxed to allow the health sector to better respond to the COVID-19 pandemic).83

organizations can disclose personal information for research purposes without individual consent, according to conditions similar to those established in the TCPS-2 and those that govern most health sector institutions.

In Quebec, private sector organizations, including both for-profit and non-profit organizations, can disclose personal information for research purposes with the approval of the Commission d’accès à l’information (CAI). The CAI must establish that the following conditions are met prior to disclosing the information:

“(1) the intended use is not frivolous and the ends contemplated cannot be achieved unless the information is communicated in a form allowing the persons to be identified;
(2) the information will be used in a manner that will ensure its confidentiality.”

The CAI can also impose the conditions it considers appropriate on the disclosure and on the use of the disclosed information. The Commission d’accès à l’information (CAI) is a body established in Quebec to administer requests for access to information, including those from the public and from requesting researchers. It occupies a similar role to the Information and Privacy Commissioner in other provinces, but is structured as an administrative tribunal rather than as an ombudsperson. See: https://www.cai.gouv.qc.ca/a-propos/organigramme/.

80 Alberta: Health Information Act, R.S.A. 2000, c. H-5 at ss. 27 (1) (g), 27 (2) (use, no disclosure). British Columbia: not applicable – British Columbia’s E-Health Act does not address the general collection, use, and disclosure of personal health information. Manitoba: Personal Health Information Act, C.C.S.M., c. P-33.5 at ss. 21 (d), 22 (2) (d) (use and disclosure). New Brunswick: Personal Health Information Privacy and Access Act, S.N.B. 1998, c. P-7.05 at ss. 34 (1) (e), (f), (o), 37 (6) (d), 38 (1), 31 (1) (d), (d.1.), (d.2.) (e) (use and disclosure). See also: Right to Information and Protection of Privacy Act, S.N.B. 2009, c. R-10.6 at s. 46 (1) (c.1.). Newfoundland and Labrador: Personal Health Information Act, S.N.L. 2008, c. P-7.01 ss. 34 (c), 34 (d), 34 (m), 39 (1) (e), 39 (1) (i) (use and disclosure to improve one’s own health system). Northwest Territories: Health Information Act, S.N.W.T. 2014, c.2 at ss. 35 (d), 35 (e), 35 (j), 37, 43 (use and disclosure). Nova Scotia: Personal Health Information Act, S.N.S. 2010, c. 41 at ss. 35 (1) (a), 35 (1) (c), 37 (f), 37 (g), 37 (i), 37 (k), 37 (t) (use and disclosure). Ontario: Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A at ss. 37 (c), 37 (d), 37 (e), 39 (1) (c), 45 (1), 47 (2) (use, or disclosure to prescribed entities or to the Minister). Prince Edward Island: Health Information Act, R.S.P.E.I. 1988, c. H-1.41 at ss. 22 (5) (e), 22 (5) (f), 22 (5) (q), 23 (13) (d), (e), (f) (use and disclosure to improve one’s own health system). Quebec: Quebec’s health sector legislation, the Act respecting health services and social services does not establish an explicit power to use or disclose health information for health system improvement purposes. However, such a power is presumably captured in Quebec’s Act respecting Access to documents held by public bodies and the protection of personal information, R.S.Q. c. A-2.1, at ss. 67, 67.1, 68, 68.1 (use, disclosure subject to CAI approval). Saskatchewan: Health Information Protection Act, c. H-0.021, ss. 26 (2) (a), 24 (1) (k) (ii) (use and disclosure to improve one’s own health system). Yukon: Health Information Privacy and Management Act, S.Y. 2013, c. 16, at ss. 56 (1) (c) (ii), 56 (1) (m), 56 (1) (p.0.1), 56 (1) (k), (l) (use and disclosure, though certain limitations are applicable regarding the recipients of information disclosures).

81 Ontario: In Ontario, such disclosures can be made only to Prescribed Entities that are approved in government regulations. See: Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A at s. 37 (1) (c), s. 45 (3). Quebec: The Minister can collect information that is provided for in regulation for purposes that are related to healthcare provision, health system improvement, quality assurance, and health care coordination, amongst others. See: Act respecting health services and social services, R.S.Q., c. S-4.2 at art. 431.

82 Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165 at s. 33. 1 (1).

83 British Columbia Minister of Citizens’ Services, Ministerial Order No. M085 (‘the Order’) on amendments to the Freedom of Information and Protection of Privacy Act 1996 (‘the Act’) in light of COVID-19 (‘Coronavirus’).
• Alberta law allows for broad information use for such purposes, but not its disclosure to other institutions for such purposes. 84
• Certain provinces allow health institutions to disclose health information for the purposes of improving their own health system, but do not explicitly allow for the disclosure of personal information to other institutions for the purpose of improving the health system of the recipient institution (e.g.: Newfoundland and Labrador, Prince Edward Island, Saskatchewan). 85
• Health information custodians in Newfoundland and Labrador are required to describe to the recipients of personal health information disclosures the potential limitations in the accuracy, completeness, and up-to-date character of the information disclosed. 86

Legal authorization or legal requirement:

There is a general power to collect, use, and disclose personal information or personal health information if a provincial or federal law allows or requires such disclosure. This could be the case if a law sets out that information can or must be shared for a specified purpose. For example, in some provinces, physicians and other healthcare practitioners are required to report identified cases of endemic communicable diseases to the medical officer of health. 87

Most, but not all, data protection laws also stipulate that a disclosure can be made if it is required to ensure compliance with the law. 88

84 Alberta: Health Information Act, R.S.A. 2000, c. H-5 at s. 27 (1) (e), 27 (2).
Saskatchewan: The Health Information Protection Act, S.S. 1999, c. H-0.021 at s. 27 (4) (k) (ii).
86 Newfoundland and Labrador. Personal Health Information Act, S.N.L. 2008, c. P-7.01 at s. 16 (b).
87 See, e.g.: British Columbia Health Act Communicable Disease Regulation, BC Reg 4/83.
Use for a consistent purpose:

Most provincial and federal public sector data protection laws enable regulated institutions to use, and sometimes also to disclose, personal information for a purpose that is compatible with the original purpose of information collection, use, or disclosure (without requiring individual consent).  

The law usually considers ‘consistent purpose’ to mean:

- Use or disclosure “has a reasonable and direct connection to [the original purpose],” and
- Use or disclosure “is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses the information or to which the information is disclosed.”

This definition is enshrined in the FIPPA of British Columbia and was applied in the case of Coast Mountain Bus Co. It is the consensus Canadian test for ‘consistent purpose.’ For this test, case law considers a reasonable and direct connection to exist if the new purpose is “logically, or rationally, connected to the original purpose.”

Some public sector laws that allow for the secondary use of personal information for a ‘consistent purpose’ also require that:

---


91 *Coast Mountain Bus Co. v C.O.P.E., Local* 378 2005 BCCA 604 para 59. This definition can be found in the legislation of some other provinces. Additionally, it has been applied in courts in other provinces as precedent to interpret the “consistent purpose exception” even where the applicable legislation does not adopt the same definition. See: *Saskatchewan Institute of Applied Science and Technology v SGEU* 2012 SKQB 102.

92 *Coast Mountain Bus Co. v C.O.P.E, Local, supra* n. 91. See also: BC IPC, Investigation Report 00-01; Use of Alumni Personal Information by Universities at para. 65.
The use or disclosure would have been reasonably expected\(^9\) by the concerned individual at the time of collection.\(^9\) There is legal precedent establishing that reusing information to perform health research, to inform health service development, and to establish health policy may constitute a 'consistent purpose.'\(^9\)

**Provincial Public Health Laws**

Provincial public health authorities have broad powers to collect, use, and sometimes also to disclose personal information for public health purposes. These powers are enshrined in provincial public health legislation. Therefore, the powers of provincial public health authorities differ to some extent in each province, as a different public health law applies in each.

The breadth and exact nature of such powers varies across provincial public health laws. Three general categories of laws exist. First, those that recognize a general power to access and use

---

\(^9\) The Supreme Court of Canada has interpreted this 'reasonable expectation' test to be applicable even in circumstances where legislation does not explicitly impose this requirement. Therefore, institutions using health information should generally consider whether the use of information falls within the reasonable expectations of the concerned individual in using the information for a consistent purpose without their consent. See: *Bernard v Canada (Attorney General)*, 2014 SCC 13 (CanLII), [2014] 1 SCR 227 at para 31. However, some case law suggests that it is not necessary to consider the reasonable expectations of individuals in determining if personal information can be used for a consistent purpose, if the information was not collected directly from the individual See: *Cash Converters Canada Inc. v Oshawa (City)*, 2007 CarswellOnt 4229, 2007 ONCA 502 at para. 40.

\(^9\) Courts have often considered a purpose not to be a consistent purpose if the use of the information leads to unanticipated and deleterious outcomes for the individual concerned. However, courts do consider a purpose to be a consistent purpose, even if such purpose is deleterious to the concerned individual, if there is a close conceptual connection between the initial purpose of use and the new purpose. Courts have, moreover, considered a purpose to be consistent if the disclosure relates to the use of information of an individual for the collective benefit of a group of which that individual forms part. For example, an employer’s disclosure of an employee’s information to a labor union of which that employee forms part has been considered a consistent purpose.

\(^9\) *O’Grady v Canada (Attorney General)*, supra n. 29. The court addressed the potential to re-use information that Statistics Canada collects as part of the census for the purpose of health research and policymaking, in accordance with the 'consistent purposes' rule enshrined in the *Privacy Act* (in a joint reading of the *Statistics Act* and the *Privacy Act*). The stated purpose of the census was “to develop programs and services such as education, health and other social and economic programs.” Therefore, the secondary use of such information for research purposes “to analyze and determine trends regarding perinatal health for usage in the development of social and health policies” or to support “policy development of governments and data users in the private sector” were considered to be consistent purposes. The court further held that it was unnecessary for the consistent purpose to be known or even possible to know, at the original time of information collection. The court came to the following conclusion regarding the potential to reuse government-held personal information for research in the public interest without first obtaining individual consent: “Parliament has built safeguards into the legislation to protect private information and for the use of census information for the public good.” The Court therefore interprets the concept of ‘consistent use’ liberally to allow for the secondary use of personal information and personal health information to act for the public good. This conclusion clarifies that the government re-use of personal information and personal health information for the purpose of performing actionable research in the public interest and to ensure appropriate health program delivery is compliant with Canadian privacy legislation. Despite this favorable development in Canadian jurisprudence, the Northwest Territories Information and Privacy Commissioner has previously articulated that ‘consistent purposes’ should not be interpreted in so broad a fashion as to enable the general reuse of personal health information for the purposes of healthcare provision or healthcare improvement. The Commissioner concluded that: “To assume, however, that that implied consent extends so as to allow a different practitioner to review the information for the purpose of dealing with a totally unrelated matter goes well beyond the scope of ‘consistent purpose’ as used in our current legislation.” See: *Northwest Territories Information and Privacy Commissioner. Yellowknife Health and Social Services Authority (Re)*, 2012 CanLII 94602 (NWT IPC). This report of findings holds less legal weight than the aforementioned judgment of the Superior Court, and it is therefore our position that this does not reflect the consensus position in Canadian law.
personal information for public health surveillance purposes. Second, those that establish a more limited power to access personal information for the purpose of responding to public health emergencies or to other potential threats to public health (e.g., the outbreak of an emergent disease). Third, those that establish only narrow powers to use personal information to combat known threats to individual health and safety, or to collect information about known cases for the purpose of combating infectious diseases. Further information regarding the public health powers available to provincial public health authorities is detailed in Appendix B.

**Federal Powers to Collect Personal Information**

Both the Public Health Agency of Canada (PHAC) and the Department of Health dispose of broad federal powers to collect, use, and disclose personal information from natural persons and from other institutions in Canada. These powers are enshrined in the *Privacy Act*.

---

96 These provinces and territories include the following: British Columbia, Manitoba, Newfoundland and Labrador, Northwest Territories, Nova Scotia, Nunavut, Prince Edward Island, and Quebec.

97 These provinces and territories include the following: Alberta, Ontario, and Yukon. Alberta legislation creates broad powers for public health authorities to requisition and use personal information in relation to communicable diseases, including for purposes related to healthcare improvement, health research and public health. Information collected and used for these purposes cannot be disclosed, except for a narrow range of enumerated purposes (Alberta *Public Health Act* at s. 53 (2)).

98 These provinces and territories include the following: New Brunswick and Saskatchewan. Public health authorities in Saskatchewan do, however, have broad powers to collect and use information to respond to epidemics (Saskatchewan *Public Health Act* at s. 45 (2) (g)).


100 *Ibid.*
Section 3: The Legal Limits of Personal Information Use

The prior section established the circumstances in which personal information and personal health information could be used or disclosed. These powers are not unbounded. Certain limitations are applicable, which establish the conditions according to which uses and disclosures can be made. The following conditions often apply to the collection, use, and disclosure of personal information and personal health information.

Limitations on information use

Most of Canada’s data protection laws incorporate central principles that limit the powers of concerned institutions to use personal information. These principles are either integrated to the legislation directly in the form of explicit principles (e.g. PIPEDA), or through provisions that approximate the contents of such principles.

These principles are integrated in some form to most health sector and private sector laws that govern the use of information by health sector institutions, private sector institutions, and provincial public sector institutions. However, most of these principles are understood not to be integrated to the federal Privacy Act. Therefore, PHAC and the Department of Health, in exercising powers enshrined in the Privacy Act to collect, use, and disclose personal information, are not required to adhere to all such principles. Both the Federal Court and the Office of the Privacy Commissioner of Canada have concluded that government institutions acting according to the Privacy Act are not bound to demonstrate that their collection of information is ‘necessary’ for their activities – only that their collection of information is related thereto. These powers are therefore broader than the analogous powers in other health sector, public sector, and private sector legislation. Provincial public sector legislation imposes a greater number of limiting principles on how information can be used than does the Privacy Act, but less than health sector and private sector data protection laws.

The kinds of limiting principles enshrined in Canadian data protection laws are as follows:

Identifying Purposes / Purpose Limitation

Before collecting, using, or disclosing information, it is often necessary for the concerned institutions to identify the purpose for which the information is collected, used, or disclosed.¹⁰¹

---

Direct relation and necessity

Public sector institutions that collect, use, or disclose personal information are often required to demonstrate that the collection, use, or disclosure is directly related to and necessary for their activities. Certain provincial health sector laws also include this requirement.

Courts and Privacy Commissioners have interpreted the meaning of ‘necessity’ with flexibility and have held that information need not be literally “indispensable” to the concerned activity for its collection, use, or disclosure to meet the threshold of necessity. The necessity of information to an activity is assessed in a contextual manner.

Collection Limitation

The principle of collection limitation requires institutions that collect personal information to restrict their collection of personal information to the minimum information that is required to accomplish the established purposes.

Provincial health sector privacy laws almost invariably require health information custodians to limit their collection of personal health information to the minimum required to achieve the purpose of the collection.


104 Ibid.

Limiting Use, Disclosure, and Retention

Similarly, the principle of limiting information use, limiting information disclosure, and limiting information retention requires institutions that use personal information for an established purpose to restrict such use, disclosure, and retention to the minimum information that is required to accomplish their established purpose. Private sector data protection laws and provincial health sector data protection laws often require health information custodians to limit their use, disclosure, and retention of personal health information to the minimum amount of information required. Further, most provinces require health information custodians to adopt policies and procedures relating to the retention and timely disposal of PHI.

---


Section 4: Other Obligations to Respect in the Use of Personal Information

In collecting, using, and disclosing personal information or personal health information, institutions and organizations in Canada are required to ensure compliance with a number of distinct legal requirements. These obligations are variable from one statute to another, but often include some, or all, of the following requirements.

Security Safeguards

Institutions and organizations that collect, use, or disclose personal information are required to use security safeguards that are appropriate to the nature of the information and the context of its use. The measures adopted must include physical, technical, and organizational safeguards. Further, appropriate security measures must be adopted for the entire life cycle of the information, from the moment of its collection, on through the use, storage, disclosure, and destruction stages.

In addition to implementing appropriate security measures, it is necessary to ensure that staff members receive appropriate training regarding information privacy and information security. Specific security measures required differ according to the categories of personal information used, the technologies used to store or access such information, and the context of information use. Security measures must account for the sensitivity of the information, and must reflect the known risks associated with the technologies used rather than hypothetical future risks. The sensitivity of personal information is always assessed according to the specific nature of the information and the context of its use. Institutions and organizations using information thus have a measure of discretion in adopting the security measures that are the most relevant to their information use activities. However, medical information is generally deemed to be considerably more sensitive than other categories of information, and must therefore be handled with heightened care.

A non-exhaustive list of security safeguards that Canadian Privacy Commissioners have considered to be useful or necessary is provided in Appendix E.

---

112 Canada OPC, PIPEDA Case summary #2011-012: GMAT Test-taker Objects to Palm-Vein Scanning.
Privacy Management Programme

Institutions that collect, use, or disclose personal health information are often required to implement a privacy management programme. This is a binding requirement in most private sector privacy laws. It is also considered a best practice for health sector and public sector information custodians.

Privacy management programmes traditionally require specialized staff responsible for ensuring compliance with Canadian data protection legislation. Such individuals are also responsible for responding to queries addressed to the institution regarding information governance and information privacy, either from the public (e.g., access to information requests) or from individuals from whom the institution has collected information (e.g., exercises of individual rights of access to, or rectification of, information).

The privacy management programme also entails a general requirement to make available public documents including:

- Policies and practices relating to personal information management and information security.
- How to obtain access to information held by the organization.
- Categories of personal information held and the kinds of uses that are made of such information including copies of policies, standards, or practices relating to personal information use and information security.
- Details of the categories of personal information that are made available to subsidiaries, affiliates, or other related organizations.
- Details of anticipated information linkages.

This documentation should be made easily accessible to the public, and be drafted in lay language.

---

115 Ibid.
116 Ibid. See also: Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, Schedule I at s. 4.8.
117 Ibid.
The Privacy Impact Assessment

Federal public sector bodies enumerated in Schedule III of the *Privacy Act* are often also required to perform a privacy impact assessment (PIA), and certain laws also require provincial public sector or health sector institutions to perform such self-assessments. Schedule III of the *Privacy Act* includes the Public Health Agency of Canada and the Department of Health, suggesting that these entities are sometimes required to perform PIAs. Federal public sector bodies are required to perform a PIA in implementing a new programme or amending an existing programme according to the following circumstances. First, if such programme is anticipated to directly affect individuals through the use of personal information as part of a decision-making process. Second, if such programme is anticipated to indirectly affect individuals through the use of personal information for administrative purposes. The PIA must include information such as a description of the intended information collection, use, and/or disclosure and the program or initiative to which such actions are related. Other requisite information includes an assessment of the effects thereof on individual privacy, and its compliance with Canada’s data protection legislation. Last, a description of the measures intended to demonstrate compliance with data protection law and with associated guidance should be provided.

Individual Rights

Individuals hold certain rights in information that is collected from them to create a record, and in information about them that is otherwise included in a record. The structure and content of individual rights differ from one province to another. Most individual rights, however, are common across the majority of data protection laws in Canada. Such individual rights include: being notified of the existence of one’s information record, the right to access the contents thereof, and the right to request the correction of errors in the record. These rights also include the power to complain to a Privacy Commissioner, and an obligation for organizations and institutions to inform individuals of their data protection rights.

---

121 Saskatchewan IPC, supra n. 118 at pp. 14-15.
124 Bernier & Knoppers, “Health Data Sharing in Canada” *supra* n. 64.
Section 5: Policy Barriers to Public Health Information Sharing

It would be misleading to attribute the current underwhelming information sharing performance of Canada in the context of COVID-19 solely to impediments in the structure of data protection law. Arguably, some of the most significant impediments to data sharing in Canada may come from practices and policy obstacles other than the law. Below, we provide a summary overview of some of the common information sharing hurdles external to data protection law.

Canada’s decentralized data sharing landscape

Local institutions are responsible for the collection and custodianship of information related to health and to public health. Information sharing initiatives can therefore be difficult to implement in a centralized or harmonized fashion because of the many different stakeholders that must align their information-sharing activities. These different stakeholders may impose additional requirements because of a lack of trust or because they are less familiar with the importance of information sharing.

Lack of resources for capacity building

Limited access to technological and human resources has also been evoked as an explanation for the difficulties public health laboratories experience in sharing information for research. However, considerable public sector investment in developing the capacity of public health laboratories has been made since the beginning of the COVID-19 pandemic.

Need for more explicit incentives to share information

Information producers not familiar with open science benefits would require more explicit incentives for information sharing to become a priority for them. Educational materials on the health impact of information sharing and more explicit and harmonized rules on the acknowledgment of researchers who share information could promote information sharing.

---

125 Health Canada, A report of the National Advisory Committee on SARS and Public Health October 2003. Learning from SARS - Renewal of Public Health in Canada, supra n. 11 at p. 4.
126 Attaran & Houston, supra n. 5. Ling, supra n. 7.
127 Health Canada. A report of the National Advisory Committee on SARS and Public Health October 2003, supra n. 11 at p. 4.
128 van Panhuis et al. supra n. 9.
131 Kalia et al. supra n. 6. van Panhuis et al. supra n. 9.
Potential risks inherent in the use and dissemination of health information

Public health researchers are sometimes unwilling to share health information due to real or perceived legal, reputational, and societal risks associated with such sharing. These risks include the publication of inaccurate information or of information that could demonstrate their poor management of public health crises.\textsuperscript{133} There may also be concerns that unfavorable data (e.g. a high number of cases or the presence of more resistant variants in a province) may result in measures that would have negative economic impacts on affected Canadian provinces. Other risks include the unintended disclosure of personal information or personal health information that breaches data protection laws or that could lead to individual or group discrimination and stigmatization.\textsuperscript{134}

\textsuperscript{133} Chretien et al. \textit{supra} n. 129.
PART II: Sharing Information for Public Health Purposes

Potential Approaches to Sharing Information for Public Health Purposes

In this Part, we propose a comprehensive approach to sharing and using health information for public health purposes in Canada. The requirements applicable to the sharing of information differ from one intended use to another, and from one province to another. However, the following general principles describe the conditions according to which information can be shared for distinct purposes. Appendix A contains a full list of the conditions according to which provincial health sector institutions can use or disclose personal health information. Appendix B contains a comparative description of the conditions according to which provincial public health authorities in each Canadian province can use or disclose personal information.

Our proposed approach to sharing differs depending on the actors implicated. For federal public sector institutions such as the Public Health Agency of Canada (PHAC) and the Department of Health that can act according to the Privacy Act, both statute and case law provide unambiguous authority to collect, use, and disclose personal information for purposes directly related to the activities and operating programs thereof.

If institutions or organizations do not require the concerned information in a form that enables the identification of the concerned individuals, it is recommended to remove the direct identifiers associated to the information (e.g., name, civic address, social insurance number) and to use a combination of organizational and technological safeguards to ensure that the information is anonymized.

Information sharing scenarios:

The following information sharing scenarios are considered:

1) The collection and use of information by federal and provincial public health authorities from provincial health sector institutions for urgent public health purposes. 2) The collection of information by federal and provincial public health authorities from provincial health sector institutions for general public health purposes. 3) The disclosure of personal health information to provincial health sector institutions for numerous purposes established in statute. These purposes include health system planning, public health surveillance, healthcare delivery and management, risk management, and quality assurance. 4) The internal use of information by provincial public sector health institutions, including clinics, hospitals, and laboratories, among other health-sector institutions. 5) The secondary use and sharing of existing information for research purposes. This includes both research activities internal to the institution that holds the information, and the sharing of information with external researchers for their own research purposes. 6) Last, the sharing of information that has been anonymized in reliance on organizational governance controls and de-identification methods is discussed. Since the specific rules differ from one law to another and from one jurisdiction to another, it is helpful to also consult the attached appendices to determine which rules are applicable in a specified province.
Disclosure of identifiable personal information to respond to significant harms to individual health and safety, or public health and safety

The majority of Canadian data protection legislation explicitly allows for the collection, use, and disclosure of personal information to respond to significant harms to individual safety, public safety, individual health, or public health (See Appendix A). Jurisprudence and the investigation reports of Canadian Information and Privacy Commissioners have also afforded these provisions a liberal interpretation. Furthermore, the Public Health legislation enacted in most provinces also creates broad powers for provincial public health institutions to collect, use, and disclose personal information for the purposes of responding to risks to public health (See Appendix B).

Though the specific powers available to government institutions and public health authorities to collect personal information and personal health information differ from one jurisdiction to another and one law to another, these are broadly construed.

The Office of the Privacy Commissioner for British Columbia considers that the disclosure of identifiable personal information for the purpose of active response to a known disease outbreak is permissible according to B.C. public health legislation.135

Disclosure of identifiable personal information for the purpose of passive public health surveillance and for general health-related purposes

Most Canadian public health legislation enables public health authorities to collect identifiable personal information for numerous public health purposes. The provinces and territories of British Columbia, Manitoba, Newfoundland and Labrador, the Northwest Territories, Nova Scotia, Prince Edward Island, and Quebec recognize broad powers for local public health authorities to collect, use, and disclose personal information for ongoing public health surveillance, and in some instances for more general population health or public health purposes (See Appendix B). Conversely, the powers of public health authorities in Alberta, Ontario, Yukon are more limited, and those public health authorities in New Brunswick and Nunavut more limited still.

As previously discussed, the Public Health Agency of Canada (PHAC) and Canada’s Department of Health hold broad powers to collect, use, and disclose personal information that are included in the Privacy Act, where such collection, use, or disclosure “relates directly to an operating program or activity of the institution.”136 Canada’s provincial government institutions have analogous powers to collect personal information that are established in the applicable provincial public sector data protection legislation.

In addition to the aforementioned government powers to collect personal information for ongoing public health surveillance purposes and for purposes related to government programmes, provincial health institutions have certain powers to disclose personal health

---

136 Privacy Act, R.S.C., 1985, c. P-21 at ss. 4, 7, 8 (2) (a).
information for purposes related to healthcare delivery, healthcare planning and management, public health surveillance, quality assurance, and risk management, amongst others (See Appendix A).

It is therefore possible for provincial healthcare institutions to exercise their discretion to disclose personal health information to third parties for these enumerated purposes. Because the nature and ambit of such powers differs in each jurisdiction, it is recommended for healthcare institutions to determine which of their available powers enable the sharing of information for ongoing public health surveillance or related purposes.

**Disclosure of information for secondary research use**

Researchers can gain access to identifiable personal information for the purposes of performing health research, as described in the previous sections. To do so, it is necessary to obtain the authorization of the information custodian responsible for safeguarding the concerned information, and often also to obtain the approval of a competent Research Ethics Committee, if such approval is necessary for the intended research.

This approach could create greater challenges for the liberal sharing and reuse of information than the approaches discussed prior, because each instance of information sharing and intended research could require independent approvals from each local information custodian concerned, and from the competent Research Ethics Committees (RECs). Because RECs and information custodians can impose distinct conditions of information use on researchers at their discretion, this approach to information sharing could lead to different research endeavors being subject to disparate and non-harmonized conditions of governance.\(^{137}\)

**Data anonymization**

Canadian data protection law does not apply to information that has been anonymized.\(^{138}\) Information is anonymized if there is no “serious possibility”\(^{139}\) of the concerned individual being identified through the use of that information, alone or in combination with other available information. Anonymized information can be shared liberally in anonymized form, without infringing data protection law.

Because the legal test for data identifiability is contextual – that is, the law considers if a “serious possibility” of identification exists, in the specific context of the information’s use – a combination of data de-identification methods and ongoing data governance practices can be used to sufficiently reduce the risk of individual re-identification.\(^{140}\)

---


\(^{139}\) Gordon v Canada (Minister of Health), supra n. 24 at paras. 34-35.

\(^{140}\) Ontario IPC, supra n. 26 at pp. 13-19. O’Grady v Canada (Attorney General), supra n. 29 at paras 60-61.
Institutions and organizations can thus use a combination of data de-identification methods and ongoing governance controls to render information anonymized.

This approach to information sharing should be considered if information users will not later need to ascertain the identities of the individuals concerned by the information. This approach to information sharing should also be considered if the legal powers available to the concerned institutions or organizations are too restrictive to enable their intended use of personal information (PI) or personal health information (PHI). Further details regarding data de-identification and data anonymization are available in Appendix G.

In consideration of the difficulties that the custodial and REC models generate in establishing information sharing according to harmonized or interoperable conditions, a model of information governance based on ongoing information stewardship could be preferable to the law’s present approach, which centralizes the interpretation and application of predetermined rules that are established in the law to each intended use of information. This would entail the modification of data protection laws, or the implementation of new special purpose legislation, to allow data stewards to exercise their judgment to re-use and to share personal information and personal health information according to secure data governance practices.
PART III: GOVERNANCE STRUCTURES AND TOOLS

Governance structures formalize the organizational approaches and practices according to which institutions and organizations collect, use, and disclose information.141 These structures and associated tools incorporate institutional structures, policies, and practices that can help translate the legal and ethical requirements applicable to public health researchers into actionable procedures.142

In this Part, we will consider the following categories of tools for information governance:

- First, organizational approaches to information governance.
- Second, technological approaches to information governance.

These organizational and technological tools can be used to ensure that public health information sharing is systematically performed in compliance with the legal and ethical obligations of the participating institutions.143

Section 1: Organizational Approaches to Information Governance

Tool: Core consent elements

The use of information for research purposes often requires the concerned individuals to provide their informed consent to participation in such research. This consent is recorded in an informed consent form, which establishes the circumstances according to which the information can be used in the future. If public health researchers intend to obtain consent to use information for research and share that information amongst themselves, it is important that the conditions described in the informed consent materials used are compatible. This can require collaborating institutions to coordinate the common elements of their consent materials amongst themselves, for instance through the use of core consent elements.

Core consent elements

Institutions that intend to collect information based on individual consent and to subsequently share it with each other should agree to common core consent elements, so that their information can be used for compatible purposes.144

---

142 Ibid.
Sharing information for secondary research use without obtaining informed consent to all of the core consent elements:

If informed consent to research participation has not been obtained, it is also possible to share information for secondary research use if certain legal preconditions are met. This can require obtaining an ethics waiver of informed consent from a Research Ethics Committee, recontacting the research participants to obtain a fresh consent, or anonymizing information prior to its secondary research use. The Research Ethics Committee is responsible for determining which of these options is appropriate in the circumstances.\textsuperscript{145}

Further details regarding research consent and exceptions thereto are available in Appendix D.

**Tool: Retrospective consent filter**

Legacy datasets are pre-existing datasets that are created prior to an intended information sharing initiative. Ethical and legal restrictions are often applicable to the use of such information. Therefore, it can be helpful to determine if the use restrictions applicable to an existing legacy dataset are compatible with a new intended purpose of use.\textsuperscript{146}

To determine if the ethical and legal permissions applicable to legacy datasets are sufficient to allow for a new intended use or a new intended information sharing exercise, a retrospective consent filter can be used.\textsuperscript{147}

Examples of retrospective consent filters are available in Appendix D.

**Tool: Established Access Tiers**

The second critical element of a functional health information governance programme is the use of distinct access tiers to maximize open access to information that is low-sensitivity or low-risk, and using more restrictive access protocols for high-sensitivity or high-risk information.

Distinct tiers of information access are established according to the relative sensitivity of the different categories of information.

\textsuperscript{145} Canada Tri-Council. Tri-Council Policy Statement II (TCPS-2), supra n. 71. Chapter 5: Privacy and Confidentiality at article 5.5.A.


Open-access information

Open-access information is among the least sensitive categories of information. Open access information elements often include anonymized individual-level information or aggregated information that present a minimal risk or no risk of leading to the re-identification of the individuals comprised in the concerned datasets. Sufficiently rich genetic information, however, could be difficult or impossible to anonymize.

Controlled-access information

Controlled-access or managed-access information access models are used to safeguard more sensitive information types. Such an approach requires external applicants to submit an application and to obtain approval prior to being able to access the specific controlled-access datasets requested, for research purposes or for other permitted purposes.

Controlled access is often used to hold datasets that contain coded individual-level information that is considered identifiable or potentially identifiable alone or in combination with other available information. This precaution still needs to be taken despite the removal of direct identifiers such as name and civic address. Controlled-access governance of information often includes the following components.

First, the information is held according to the stewardship of a specified research institution or other established body (e.g., a corporation, international organization, or non-profit). Second, the information is held according to established governance rules and policies that determine which individuals can have access to the information held, and the conditions according to which such access can be made. Third, a committee, individual, or group of individuals is required to accord or refuse information access to external applicants.

152 Central oversight bodies are often structured as ‘data access committees’ that are independent from the custodian and composed of relevant experts from numerous disciplines (often including bioethics, law, and a relevant biomedical science). The principal advantage of this approach is that it ensures that the same body is responsible for administering access to all of the different datasets of a health information repository, ensuring that the process is transparent, fair, and expedient for all users. Reliance on an independent body composed of interdisciplinary experts further helps recognize and mitigate potential legal risks and privacy risks that could arise from inappropriate or high-risk disclosure of information. Assessing these risks often requires an understanding of both the applicable bioethics or legal principles, and a deep understanding of the risks inherent in the scientific research proposed.
Tool: Data Access Agreement

Information custodians that host information that third parties can access and use for the purposes of research should consider subjecting such information to a uniform ‘data access agreement’ or ‘data sharing agreement.’ These agreements help to communicate expectations to researchers and other information users regarding the informed consent of research participants and the governance conditions that must be respected in the use of the information.

For controlled-access information, this is often devised in the form of an agreement between data users, their institution, and a data repository. Such agreement is often made available online through an information sharing portal. For open-access datasets, a click-wrap agreement or browse-wrap terms of use could be used to inform information users of their respective obligations. Click-wrap agreements enable users to consult the agreement upon opening a webpage and to bind themselves to the agreement in checking a box on an electronic prompt through their browser. Browse-wrap terms of use are made available on a webpage for user consultation, but are not drawn to the attention of the user and are not signed or otherwise explicitly agreed to by the user.

Tool: Policies to Incentivize Information Sharing

Attribution policies are documents that guide and dictate how researchers making secondary use of information are to provide recognition to the original information producers that generated the research information used. These policies often require that information contributors be accredited through an acknowledgment statement at the beginning or at the end of research manuscripts published from information that makes secondary use of the existing research information.

---

154 Saulnier et al. supra n. 132.
155 Courts might not always hold ‘browse-wrap’ terms of use or ‘click-wrap’ agreements to be legally binding, in contrast to more traditional contracts that the parties are required to read, acknowledge, and sign. The Supreme Court of Canada (SCC) has previously held that a browse-wrap terms-of-use is a binding contract only if a link thereto is made sufficiently prominent, for example through its inclusion on each of the pages of a web-site (according to Quebec law). Canadian and U.S. courts have in the past held that browse-wrap or click-wrap agreements are binding if it can be determined that the parties intended to bind themselves to the conditions thereof. See: Joly, “Propriété intellectuelle et modèles de collaboration ouverte” In : JurisClasseur Québec. I. Droits intellectuels : spécificité et spécialité (p. 3/17) (2017). Canino, “The Electronic Sign-in-Wrap Contract: Issues of Notice and Assent, the Average Internet User Standard, and Unconscionability” (2016) *UCD L Rev* 50:1 535.
Section 2: Technological Approaches to Information Governance

Technological approaches to information governance can also be adopted to help minimize risks to individual privacy while still enabling the use of the information for purposes of scientific analysis. Other technological approaches to information governance can help to ensure compliance with privacy legislation in performing or facilitating certain actions that the law requires, in an automated fashion.

These technologies can also serve to anonymize information either through the removal of identifiers (i.e., technologies for de-identification) or through the use of technological measures to enable the use of information whilst reducing or eliminating the risk of individuals being re-identified as a result of the information being accessed or analyzed.

While organizational information governance tools are well-developed and have been implemented in a number of practical circumstances to govern the sharing and the centralization of information, technological information governance tools are still in a state of development and have received less widespread adoption. Select technological approaches to information governance are described below. These methods have been endorsed by regulators, by sectoral organizations such as the Global Alliance for Genomics and Health (GA4GH), and in academic literature on biomedical information governance. More extensive details are provided in Appendix F.

Quantitative Approaches to Assessing Information Identifiability

Computer scientists and statisticians have developed quantitative metrics for assessing the re-identification risk associated to information that has been subjected to de-identification techniques. These metrics are often used to determine if the risk of individual re-identification is sufficiently high for the information to be considered ‘identifiable personal information,’ or if the information should instead be considered anonymized.

One principal metric used to assess information’s identifiability is ‘k-anonymization.’ K-anonymization is a method used to assess how unique combinations of potential identifiers are, within a concerned dataset. First, one must determine which attributes in a dataset are potential identifiers. These could include, for example, age, gender, and profession.

Once the potential identifiers in the dataset are determined, the identifiability of the information can be calculated in assessing how many records share the same combination of potential identifiers. This is performed for each combination of potential identifiers in the dataset (e.g., each combination of age, gender, and profession). If a sufficient number of individual records (often eleven) in a dataset share the same combination of potential identifiers, it can be presumed

---

that those records are anonymized. This is the case because each of the records could refer to any one of the concerned individuals, even in combination with other information.

**Differential Privacy**

Differential privacy is a method used to ensure that aggregate or summary-level information cannot be used to identify the individuals that contributed information to the dataset. This potential for re-identification exists because computational methods could be used to compare slightly different versions of an aggregate dataset to the known information of target individuals for the purpose of determining if the records of the target individuals were used to generate the concerned aggregate information.\(^{157}\)

Differential privacy safeguards against this risk by adding noise to the results of the aggregation process, to prevent the aggregated output information from being compared to the individual-level input records for the purpose of performing individual re-identification.

**Beacon Systems**

Genomic Beacon Systems are used to safeguard the privacy of individuals that have contributed their genomic information to research databases. The privacy challenge is the following. External researchers must determine if a controlled-access genomic database contains genetic variants that are of research interest before performing the labor-intensive process of applying for access to data for a specified research project. However, publishing lists of available genetic variants in open access creates privacy risks, because often genetic variants or combinations thereof can be sufficiently rare as to create risks of individual re-identification through the comparison of a database’s available variants to the known genetic variants of a real-world individual.

Beacon Systems safeguard against this re-identification risk. Beacons function in allowing individuals to search a database of aggregate genomic records for variants that are of research interest. Privacy is preserved using a number of techniques, such as returning false results to queries that target a large number of genetic variants belonging to the same individual.\(^{158}\)


Model-To-Data Approaches: Federated Learning and Swarm Learning

The advent of cloud computing has allowed researchers and healthcare providers to leverage increasingly large amounts of information. Despite the many advantages of cloud computing, the transfer of information between different entities creates privacy risks. Federated computing and federated machine learning techniques can alleviate major privacy concerns.  

In federated computing, various local information storage solutions can run similar analysis procedures on their local information and then exchange the parameters and results of this analysis without transferring the potentially sensitive information on which the analysis is performed. The local and central entities are constantly communicating with each other to refine and regenerate their analysis. This allows for an analysis to be performed that aggregates or utilizes multiple datasets from different institutions or research cohorts, without the input information being shared between the collaborators.  

“Swarm Learning” is a machine learning technique that shares many features with federated learning. Both techniques entail local entities exchanging the results of analysis instead of the underlying information. Swarm Learning does not employ a central entity responsible for aggregating the results of local analyses. Each local network constantly communicates its findings with several other networks, rather than only one central network. This system is advantageous in that it is less affected by any central network failures.

---


Homomorphic Encryption and Secure Multi-Party Computation

Homomorphic encryption is a form of encryption that allows users to use and perform computations on encrypted information without first decrypting it. Subsequently, when decrypted, the results of the computations can be viewed. This technique can be combined with cloud computing strategies to maximize the preservation of privacy. Full homomorphic encryption is challenging to implement. Some procedures benefit significantly from “somewhat” homomorphic encryption, wherein only a limited set of operations are performed using homomorphic encryption. Emergent technological developments are making homomorphic encryption increasingly practicable. This technique has been applied to the storage of medical records and in the financial industry, and its utilization is likely to increase as such technologies improve.

Secure multi-party computation is a cryptographic method that allows computation efforts to be distributed across numerous parties in a secure manner that involves no information exposure. This method is used to perform the combine analysis of information from multiple parties, yet there is a desire to hold each collaborator’s information confidential. Overall, such methods are highly secure and precise. However, these processes generally result in increased computational costs.

---

CONCLUSION

The COVID-19 pandemic has revealed the limitations of Canada’s public health information sharing networks. These limitations arise from the decentralized and independent organizational structure of Canada’s provincial public health bodies. Other contributing factors include a lack of incentives to share information. Neither the funding structure nor the reward mechanisms of institutions producing information encourage them to work towards the rapid and efficient exchange of available information. Last, and most importantly, the unharmonized nature of Canadian data protection legislation acts as a disincentive to information sharing or is invoked as a justification to avoid information exchange. Having acknowledged these barriers, we articulate a number of proposals. The first category of proposals emphasize that institutions and organizations can and should already share information in many instances using their existing legal powers. The second category of proposals detail how Canadian data protection law should be amended to enable more liberal, yet secure, information sharing for public health research, and advance general policy proposals to incentivize information sharing.

Public sector institutions, and private sector organizations can share PI and PHI for numerous purposes. These include public health, health system planning, and government purposes, amongst others. Provincial health sector institutions, and public health authorities in select provinces with more restrictive public health legislation, can share PI and PHI, but their powers to do so are more limited. For those institutions that have insufficient powers to access and transfer the needed information in identifiable form, data anonymization can be performed by removing direct identifiers, and using a combination of organizational technological measures to share information in anonymized form. Third parties can access PI and PHI for a specified research project. This requires REC approval, custodian approval, or both.

Canada’s federal and provincial legislatures should implement laws or regulations that enable or require the sharing of public health information that is personal in nature. Creating a coordinated Canadian public health strategy requires information flows to occur by default, rather than as an ad hoc exercise of exceptional statutory powers. In past epidemics, Canada’s decentralized public health landscape has limited the country’s ability to remain competitive with other developed economies in research activities and disease containment efforts.

The lack of harmonization in Canadian data protection legislation causes institutions and organizations to adopt individuated and incompatible practices and policies for information sharing. This inhibits attempts to create pan-Canadian information sharing initiatives according to common standards. Harmonising the applicable legal requirements would hold all Canadian health institutions and organizations accountable to a same standard of data protection, and curtail the discretion of information custodians in deciding whether and how to share information. Common pan-Canadian rules would facilitate the development of cohesive, national public health research efforts, and entitle Canadians to uniform guarantees of privacy protection and information governance nation-wide. Last, doing so would enable all Canadians to benefit more equitably from scientific research.
Law could further be reformed to grant clear discretion to central public health authorities, local public health authorities, and other health institutions to share information for public health purposes. Contemporary data protection legislation emphasizes compliance with principles established in law, many of which require the limitation of information use as a default proposition. This fosters conservatism in the use of information. Transitioning to a model of ‘data stewardship’ that enables secondary use by default, according to ongoing expert governance, is recommended. The stewardship approach enables flexibility in the use of information that Canada’s present ombudsperson model of data protection legislation cannot guarantee. The implementation of data sharing rules that reflect the data stewardship approach could therefore save lives, avert the misallocation of government resources, and ensure the justified and proportionate implementation of public health measures in reliance information that is updated in real time.

Though a full discussion of the details of such an information governance paradigm is outside of the scope of this report, it is anticipated that such a model would define the organizational and technical preconditions to information sharing and information use in a rigorous and specific manner, and permit such information uses as a default position. This would reduce the administrative burden that the custodianship model imposes on health information custodians and Research Ethics Committees. It also guarantees all Canadians an equitable right to benefit from best-of-class information protection according to a standardized model, and from efficient and effective public health interventions. This approach reflects contemporary policy perspectives on health information governance, which recognizes such information to be a shared resource and a knowledge commons to be used for future healthcare purposes in the public interest. The anticipated governance controls include the removal of direct identifiers, and the use of considerable organizational safeguards and technological safeguards to ensure that such information is not misused. This would enable the liberal use of data for public health purposes. Other proposed legal amendments and policy initiatives to incentivize the ongoing governance and appropriate use of Canadian PI and PHI for public health purposes include the following:

First, it is recommended that a central institution, equipped with appropriate technological infrastructure, be created to store and steward health-related information for public interest purposes, including public interest research purposes. The institution would be invested with the legal authorization, organizational structure, and technological and human resources necessary to fulfill its functions. It could also develop policies and standards enabling other institutions to achieve a high standard of technical and legal interoperability. Second, legislation or research funding agreements could require health institutions to appoint a specialist staff member responsible for facilitating and performing information sharing. Third, Federal law could create a penal sanction applicable to persons who intentionally re-identify individuals, such as the one present in the United Kingdom Data Protection Act 2018 (DPA 2018). This could incentivize institutions to share information more liberally, as legal rules would exist to deter third parties from attempting the re-identification of the shared information. The changes needed in Canada’s

164 Kalia et al. supra n. 6. Moher & Cobey, supra n. 10.
information policy ecosystem can be characterized as follows. Canada’s national strategies and public statements regarding information strategy all reflect a commitment to maximizing the nation’s benefit from its considerable information holdings. However, the structure of its data protection laws creates considerable compliance risks in using and sharing information, and creates no countervailing incentives to maximize the benefits from information.

Other policy instruments could be used to achieve a better balance between the imperative to safeguard individual privacy and the societal need to obtain heightened benefits from the use of available information. These include laws explicitly allowing or requiring the sharing of information, to counteract the law’s present bias toward precluding information exchange. Other available policy tools include subsidies, tax advantages, and financial incentives to enable institutions and organizations to finance information infrastructure, or to reward high-performers in information sharing initiatives. The public sector could also delineate more concrete standards regarding the categories of information that can or must be disclosed for public health purposes, or that should be considered anonymized. This could be achieved in reliance on soft-law instruments, for example regulatory guidance on the part of Canadian public health agencies and Canadian Privacy Commissioners. The principal advantage of these non-binding approaches is that these could be implemented and modified faster than binding national legislation, to respond to a changing understanding of information security and privacy risks.

Last, enforcement policies or liability rules related to data protection and privacy could explicitly be made less strict in adjudicating information uses that are made for public health purposes, research purposes, or for other purposes in the public interest. Limiting strict enforcement of data protection laws to bad faith actors or to incidents of gross negligence could incentivize good-faith attempts to use information according to sound judgment and in reliance on good data governance practices. This is similar to the approach of the United Kingdom Information and Privacy Commissioner, which acknowledged the need for greater nuance in the application of information governance standards due to the turmoil that the global pandemic imposed on organizations responsible for managing the use of data. The critical policy conclusion that can be drawn from these recommendations is that Canada’s health information policy paradigms must shift away from privileging privacy and information non-utilization in imposing ambiguous and onerous legal compliance risks on institutions and organizations that hold health data. Multiple policy tools should be leveraged together to create incentives to perform pro-social information use, and create countervailing disincentives to the misuse of information. Canada’s information laws impose high compliance costs on information use, and especially on inter-provincial or inter-sectoral information use. Canadian institutions and organizations have responded accordingly, strictly limiting their use of information. Canadian policymakers should therefore use a combination of policy tools to proactively incentivize enhanced information sharing and ongoing information stewardship.

---

APPENDIX A: Provincial Health Sector Institution Powers to Use and Disclose Personal Information and Personal Health Information

The Powers of Provincial Health Sector Institutions:

<table>
<thead>
<tr>
<th>Province or territory</th>
<th>Powers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alberta</td>
<td>Use: All health information custodians in Alberta can use personal health information for the purpose of: &quot;providing health services,&quot;&quot;providing for health service provider information,&quot; and for &quot;internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management.&quot; Provincial health boards, regional health authorities, and the Health Quality Council of Alberta, the Minister of Health and Wellness, and the Department of Alberta Health and Wellness can also use personal health information for the following purposes: &quot;(a) planning and resource allocation. (b) health system management. (c) public health surveillance. (d) health policy development.&quot;</td>
</tr>
</tbody>
</table>

Disclosure: Health information custodians in Alberta can disclose “diagnostic, treatment, and care information” to other health information custodians in Alberta for the aforementioned purposes. Health information custodians can also disclose such information to the “Government of Canada or of another province or territory of Canada for that government’s use for health system planning and management and health policy development” if "(i) the individual is a resident of that other province or territory, or (ii) that government is otherwise responsible for payment for health services provided to the individual". |

| British Columbia | British Columbia does not have specific legislation establishing the powers of health sector institutions to collect, use, and disclose information. Therefore, it is necessary to consider if the |

---

169 *Ibid* at s. 27 (1) (e).
170 *Ibid* at s. 27 (1) (g).
171 *Ibid* at s. 1 (1) (f).
172 *Ibid* at s. 27 (2).
173 *Ibid* at s. 35 (1) (a).
174 *Ibid* at s. 35 (1) (a.1.).
concerned institution is subject to public sector or private sector (which in B.C. captures non-profits)\textsuperscript{175} data protection laws.

**Private sector health organizations:**

British Columbia’s private sector data protection law contains only limited powers enabling organizations to collect, use, and disclose personal information without individual consent.

However, such information can be used\textsuperscript{176} as is “necessary to respond to an emergency that threatens the life, health or security of an individual.”

Despite the narrow powers of B.C. private sector health organizations to use and disclose personal information without consent, such organizations will be able to disclose personal health information to other organizations and institutions where such organizations have the legal power to collect such information for their own use.

**Public sector health institutions:**

British Columbia public sector health institutions can use\textsuperscript{177} or disclose personal information within Canada for the following purposes:

“for the purpose for which it was obtained or compiled or for a use consistent with that purpose.”\textsuperscript{178}

or

“to an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of the officer, employee or minister,”\textsuperscript{179}

or if the

“information is necessary for the delivery of a common or integrated program or activity and for the performance of the duties, respecting the common or integrated program or activity, of the officer, employee or minister to whom the information is disclosed,”\textsuperscript{180}

or

“to an officer or employee of a public body or to a minister, if the information is necessary for the purposes of planning or evaluating a program or activity of a public body.”\textsuperscript{181}

<table>
<thead>
<tr>
<th>Manitoba</th>
<th>Use:</th>
</tr>
</thead>
</table>

\textsuperscript{175} B.C. *Personal Information Protection Act*, S.B.C. 2003, c. 63 at s. 1 “organization.”

\textsuperscript{176} Ibid at s. 15 (1) (l).

\textsuperscript{177} British Columbia: *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, at s. 32 (c).

\textsuperscript{178} Ibid at s. 33.2 (a).

\textsuperscript{179} Ibid at s. 33.2 (c).

\textsuperscript{180} Ibid at s. 33.2 (d).

\textsuperscript{181} Ibid at s. 33.2 (l).
Health information custodians can use personal health information for a purpose that “is directly related to the purpose for which the personal health information was collected or received,”182 to “prevent or lessen a serious and immediate threat to health or safety of the individual the information is about or another individual, [or to] … public health or public safety.”183

[Public bodies or health information custodians] can use personal health information to “deliver, monitor or evaluate an [internal] program that relates to the provision of health care or payment for health care”184 or “for [internal] research and planning that relates to the provision of health care or payment for health care.”185

**Disclosure:**

Health information custodians can disclose personal health information “to prevent or lessen a risk of harm to the health or safety of a minor, or … a risk of serious harm to the health or safety of the individual the information is about or another individual, or to public health or public safety.”186

For select risk management and performance review purposes, including:

For a “risk management assessment,” or to “a body with statutory responsibility for the discipline of health professionals or for the quality or standards of professional services provided by health professionals” or for the “purpose of peer review by health professionals,” or for the “purpose of review by a standards committee established to study or evaluate health care practice in a health care facility or health services agency.”187

For the purpose of delivering, monitoring, or evaluating the healthcare the disclosing custodian provides,188 or to another healthcare information custodian for the purposes of evaluating its own healthcare provision.189

Disclosures can also be made to a “computerized health information network”190 that is established by one or many Canadian governments or government agencies. Such disclosures can be made for the purpose of:

“(i) providing health care,

(ii) facilitating the evaluation or monitoring of a program that relates to the provision of health care or payment for health care, or

(iii) facilitating research and planning that relates to the provision of health care or payment for health care.”191

---

182 Manitoba *Personal Health Information Act*, C.C.S.M., c. P33.5 at s. 21 (a).
183 *Ibid* at s. 21 (c) (i), (c) (ii).
184 *Ibid* at s. 21 (d) (i).
185 *Ibid* at s. 21 (d) (ii).
186 *Ibid* at s. 22 (2) (b).
187 *Ibid* at s. 22 (2) (c).
188 *Ibid* at s. 22 (2) (g).
189 *Ibid* at s. 22 (2) (g.1).
190 *Ibid* at s. 22 (2.1).
191 *Ibid* at s. 22 (2) (h).
### Use:

Health information custodians can use personal health information without individual consent for the following purposes:

#### Public health:

“To prevent or reduce a risk of significant harm to the health or safety of the public or a group of people, the disclosure of which is clearly in the public interest.”

#### Health system planning and healthcare delivery:

“If the custodian is a public body, for planning or delivering programs or services that the custodian provides or that the custodian funds in whole or in part, allocating resources to any of those programs or services, evaluating or monitoring any of them or detecting, monitoring or preventing fraud or any unauthorized receipt of services or benefits related to any of them.”

“If the custodian is a public body, for planning or delivering common or integrated services, programs or activities”

“If the custodian is a health care provider, for delivering common or integrated services, programs or activities”

#### Risk management and quality assurance activities:

“For the purpose of risk management, error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the custodian.”

#### Education and training:

“For educating agents of the custodian to provide health care.”

#### Regional health authorities:

“If the custodian is a regional health authority, the board of directors or management personnel of a regional health authority or any member of any administrative or advisory committee established in accordance with the by-laws of a regional health authority for the following functions within the geographic area in which the custodian has jurisdiction:

---

192 *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05 at s. 34 (1) (d).
193 *Ibid* at s. 34 (1) (c).
194 *Ibid* at s. 34 (1) (c.1).
195 *Ibid* at s. 34 (1) (c.2).
196 *Ibid* at s. 34 (1) (f).
197 *Ibid* at s. 34 (1) (g).
(i) planning and resource allocation;
(ii) health system management;
(iii) public health surveillance; and
(iv) health policy development”\(^{198}\)

Custodians who are Ministers of the Crown can also use data for these latter purposes.\(^{199}\)

**Disclosure:**

**Public health and individual or public safety:**

“(a) to the chief medical officer of health or other medical officers of health if the disclosure is required by another Act of the Legislature or the Parliament of Canada, or

(b) to a public health authority established under an Act of the Parliament of Canada, an Act of another province or territory or an Act of another jurisdiction if the disclosure is made for a public health purpose.”\(^{200}\)

“(a) [T]o prevent or reduce a risk of serious harm to the mental or physical health or safety of the individual to whom the information relates or another individual, or

(b) to prevent or reduce a risk of significant harm to the health or safety of the public or a group of people, the disclosure of which is clearly in the public interest.”\(^{201}\)

**Health system planning and healthcare delivery:**

“[F]or the purpose of delivering, evaluating or monitoring a program of the custodian that relates to the provision of health care or the payment for health care”\(^{202}\)

“[I]f the custodian is a public body, for the purpose of planning or delivering a common or integrated service, program or activity.”\(^{203}\)

“[I]f the custodian is a health care provider, for the purpose delivering a common or integrated service, program or activity.”\(^{204}\)

“[F]or the purpose of review and planning necessary for the provision of health care by another custodian.”\(^{205}\)

**Risk management and quality assurance activities:**

\(^{198}\) *Ibid* at s. 34 (1) (o).
\(^{199}\) *Ibid* at s. 34 (1) (p).
\(^{200}\) *Ibid* at s. 37 (5.1).
\(^{201}\) *Ibid* at s. 39 (1).
\(^{202}\) *Ibid* at s. 38 (d).
\(^{203}\) *Ibid* at s. 38 (1) (d.1.).
\(^{204}\) *Ibid* at s. 38 (1) (d.2.).
\(^{205}\) *Ibid* at s. 38 (1) (e).
“[T]o a person who requires the personal health information to carry out an audit for, or to provide legal services, error management services or risk management services to, the custodian”\textsuperscript{206}

**Statistical compilation:**

“[T]o the Canadian Institute for Health Information, the New Brunswick Health Council or another entity prescribed by regulation for the purpose of compiling and analyzing statistical information to assist in the management, evaluation and monitoring of the allocation of resources, health system planning and delivery of health care services in accordance with the terms of an agreement between the Province and the Canadian Institute for Health Information, the New Brunswick Health Council or the other entity, as the case may be.”\textsuperscript{207}

<table>
<thead>
<tr>
<th>Newfoundland and Labrador</th>
<th>Use:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Health information custodians can use personal health information without individual consent for the following purposes:</td>
</tr>
</tbody>
</table>

**Healthcare planning or delivery:**

“[F]or planning or delivering health care programs or services provided or funded by the custodian, in whole or in part, allocating resources to those programs or services, evaluating or monitoring those programs or services or preventing fraud or an unauthorized receipt of services or benefits related to those programs or services.”\textsuperscript{208}

**Risk management and quality assurance activities:**

“[F]or the purpose of risk management or error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of related programs or services of the custodian.”\textsuperscript{209}

**Individual or public risk prevention:**

“[To] prevent or reduce a risk of serious harm to

(i) the mental or physical health or safety of the individual the information is about or another individual, or

(ii) public health or public safety”\textsuperscript{210}

**Health system planning:**

\textsuperscript{206} *Ibid* at s. 38 (1) (g).
\textsuperscript{207} *Ibid* at s. 38 (1) (g.1.).
\textsuperscript{208} *An Act to Provide for the Protection of Personal Health Information*, S.N.L. 2008, c. P-7.01 at s. 34 (c).
\textsuperscript{209} *Ibid* at s. 34 (d).
\textsuperscript{210} *Ibid* at s. 34 (l).
Certain health information custodians\(^{211}\) can use personal health information for the purpose of:\(^{212}\)

- (i) Planning and resource allocation,
- (ii) health system management,
- (iii) public health surveillance, and
- (iv) health policy development.”

**Disclosure:**

Health information custodians can disclose personal health information without individual consent for the following purposes:

**Healthcare planning or delivery:**

- “[F]or the purpose of delivering, evaluating or monitoring a program of the custodian that relates to the provision of health care or payment for health care,”\(^{213}\)

- “[F]or the purpose of review and planning that relates to the provision of health care by the custodian,”\(^{214}\)

**Risk management and quality assurance activities:**

- “[T]o a person who requires the personal health information to carry out an audit for, or provide legal services, error management services or risk management services to, the custodian,”\(^{215}\)

- “[T]o the Canadian Institute for Health Information or other entity prescribed in the regulations for the purpose of compiling and analyzing statistical information to assist in the management, evaluation and monitoring of the allocation of resources, health system planning and delivery of health care services in accordance with the terms of an agreement between the Canadian Institute for Health Information or other entity and the province.”\(^{216}\)

Personal health information can also be disclosed to a health information manager for the purposes of creating an integrated electronic health record shared across multiple health information custodians.\(^{217}\)

**For purposes related to individual health or public health:**

“to prevent or reduce a risk of serious harm to the mental or physical health or safety of the individual the information is about or another individual; or

---

\(^{211}\) The following categories hold this power: Authorities, the Minister, branches of the executive government, or boards, councils, committees, corporations or agencies of the executive government.

\(^{212}\) *An Act to Provide for the Protection of Personal Health Information*, S.N.L. 2008, c. P-7.01 at s. 34 (m).

\(^{213}\) *Ibid* at s. 39 (1) (d).

\(^{214}\) *Ibid* at s. 39 (1) (e).

\(^{215}\) *Ibid* at s. 39 (1) (g).

\(^{216}\) *Ibid* at s. 39 (1) (h).

\(^{217}\) *Ibid* at ss. 22, 39 (1) (f).
for public health or public safety”

**Extra-provincial disclosures for health care and health planning in other provinces:**

“(i) the disclosure is for the purpose of health planning or health administration,

(ii) the information relates to health care provided in the province to a person who is a resident of another province or territory of Canada, and

(iii) the disclosure is made to the government of that other province or territory of Canada.”

**Northwest Territories Use**

Health information custodians can use information for the following purposes:

**Healthcare planning, risk management, and other internal use purposes:**

“[F]or internal management purposes, including:

(i) planning and resource allocation,
(ii) development of policies, procedures and protocols,
(iii) monitoring, audits, evaluations and reporting,
(iv) development of measures for the improvement of the quality of administration, health services and practices and procedures carried out in health facilities,
(v) obtaining or processing payment for health services,
(vi) legal services, error management services and risk management services, and
(vii) training health information custodians and agents;”

**Education and training:**

“[T]o educate health service providers”

**Health system management and public health surveillance:**

---

218 *Ibid* at s. 40 (1).
219 *Ibid* at s. 47 (1) (d).
220 *Health Information Act*, S.N.W.T. 2014, c.2 at s. 35 (d).
221 *Ibid* at s. 35 (j).
Health information custodians that are public institutions can also use personal health information for the following purposes:

“Health system management, including (i) the development and management of health services, and (ii) planning, program development, resource allocation, monitoring and evaluation in respect of health services and related matters; (b) public health surveillance and health promotion; and (c) the administration and enforcement of this Act and the regulations.”

Disclosure:

General purposes of disclosure:

Health information custodians can disclose personal health information to other health information custodians for the purposes of Healthcare planning, risk management, and other internal use purposes, and education and training purposes, described above. Health information custodians that are public institutions can also disclose personal health information to other health information custodians that are public institutions for the purposes of health system management and public health surveillance, as described above.

These disclosures cannot be performed if the concerned individuals have expressly opted-out of such disclosures.

Disclosure to government health programs and services:

“Subject to the regulations, the Department may disclose personal health information about an individual for the purpose of the development of health programs or services, or for the management, monitoring or evaluation of the health system or health programs or services, to:

(a) the Government of Canada, a government of a province or territory, or an Aboriginal government; or

(b) a department or other organization of a government referred to in paragraph (a).”

---

222 Ibid at s. 37.
223 Ibid at s. 43 (1).
224 Ibid at s. 43 (2).
225 Ibid at s. 43 (3).
226 Ibid at s. 60.
Disclosure for error management or risk management purposes:

Health information custodians can disclose personal health information for the purposes of enabling third parties to:

“(a) [C]arry out an audit for the custodian or in respect of health services provided by the custodian; or

(b) provide legal services, error management services or risk management services to the custodian.”

Disclosures for the prevention of harm and for public health purposes:

“A health information custodian may disclose personal health information about an individual if the custodian has reasonable grounds to believe that the disclosure is required to prevent or reduce:

(a) an imminent threat to the health or safety of the individual or another individual;

(b) a risk of serious harm to the health or safety of the individual or another individual; or

(c) an imminent or serious threat to public safety.”

“Subject to the regulations, a health information custodian shall disclose personal health information about an individual to a public health authority established under an Act, or under the legislation of Canada, a province or another territory, if the disclosure is required for a public health purpose.”

Nova Scotia Use

“[F]or planning or delivering programs or services that the custodian provides or that the custodian funds in whole or in part, allocating resources to any of them and evaluating or monitoring any of them”

---

227 Ibid at s. 53.
228 Ibid at s. 58 (1).
229 Ibid at s. 66.
230 Personal Health Information Act, S.N.S. 2010, c. 41, at s. 35 (1) (a).
“[F]or the purpose of ensuring quality or standards of care within a quality review program within the custodian's organization”\textsuperscript{231}

“[F]or the purpose of risk management or patient safety within the custodian's organization”\textsuperscript{232}

**Disclosure**

“to any person if the custodian believes, on reasonable grounds, that the disclosure will avert or minimize an imminent and significant danger to the health or safety of any person or class of persons”\textsuperscript{233}

“to another custodian for the purpose of ensuring quality or standards of care within a quality review program within the custodian's organization.”\textsuperscript{234}

“[T]o the Minister and the Minister of Health Promotion and Protection for the purpose of planning and management of the health system.”\textsuperscript{235}

“[F]rom the Province to another provincial or territorial government or the Government of Canada to assist in the planning and management of the health system.”\textsuperscript{236}

“[T]o the Canadian Institute for Health Information to assist in the planning and management of the health system in accordance with the terms of an agreement between the Canadian Institute for Health Information and the Province.”\textsuperscript{237}

“[F]or the purpose of risk management or patient safety within the custodian's organization.”\textsuperscript{238}

**Nunavut**

Nunavut has not implemented health sector specific data protection legislation. Therefore, health sector activities in Nunavut may be regulated by the federal PIPEDA (uses of information by private sector organizations in the course of commercial activities).\textsuperscript{239} The Access to Information and Protection of Privacy Act (S.N.W.T. 1994, c.20) applies to health sector uses of personal data performed by public sector institutions.\textsuperscript{240} This is the same act as applies to public sector institutions in the Northwest Territories.

If neither of these laws applies to an organization or an institution in its use of personal information, no data protection law will be applicable to such use.

**Access to Information and Protection of Privacy Act:**

Information can be collected and subsequently used:

\textsuperscript{231} *Ibid* at s. 35 (1) (c).
\textsuperscript{232} *Ibid* at s. 35 (1) (j).
\textsuperscript{233} *Ibid* at s. 38 (1) (d).
\textsuperscript{234} *Ibid* at s. 38 (1) (f).
\textsuperscript{235} *Ibid* at s. 38 (1) (h).
\textsuperscript{236} *Ibid* at s. 38 (1) (k).
\textsuperscript{237} *Ibid* at s. 38 (1) (i).
\textsuperscript{238} *Ibid* at s. 38 (1) (t).
\textsuperscript{239} *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 at s. 4. See also: Canada OPC, “PIPEDA legislation and related regulations.” (2018).
\textsuperscript{240} OPC, “Provincial laws that may apply instead of PIPEDA,” *supra* n. 41 (2020).
If the information “relates directly to and is necessary for

(i) an existing program or activity of
the public body, or

(ii) a proposed program or activity where collection of the information has been authorized by the
head with the approval of the Executive Council.”

Consistent purpose:

Information can be used or disclosed:

“[F]or the purpose for which the information was collected or compiled, or for a use consistent with that purpose.”

“[T]o or [by] an officer or employee of a public body, if the disclosure is necessary for
the delivery of a common or integrated
program or service and for the
performance of the duties of the officer
or employee to whom the information is
disclosed.”

Individual or public safety:

As is “necessary to protect the mental or physical health or safety of any individual”

Disclosure or use for any purpose:

“[F]or any purpose when, in the opinion of the head,

(i) the public interest in disclosure
clearly outweighs any invasion of
privacy that could result from the
disclosure, or

(ii) disclosure would clearly benefit the
individual to whom the information
relates,”

Ontario Use:

Healthcare planning or delivery:

---

241 Access to Information and Protection of Privacy Act, S.N.W.T. 1994, c.20 at s. 40 (c).
242 Ibid at s. 43 (b).
243 Ibid at ss. 43 (a), 48 (a).
244 Ibid at s. 48 (q.1).
245 Ibid at s. 48 (q).
246 Ibid at s. 48 (s).
“[F]or planning or delivering programs or services that the custodian provides or that the
custodian funds in whole or in part, allocating resources to any of them, evaluating or monitoring
any of them or detecting, monitoring or preventing fraud or any unauthorized receipt of services
or benefits related to any of them.” 247

Risk management and quality assurance:

“[F]or the purpose of risk management, error management or for the purpose of activities to
improve or maintain the quality of care or to improve or maintain the quality of any related
programs or services of the custodian.” 248

Education and training:

“[F]or educating agents to provide health care.” 249

Disclosure

Public health purposes:

“A health information custodian may disclose personal health information about an individual,” 250

“To the Chief Medical Officer of Health or a medical officer of health within the meaning of the
Health Protection and Promotion Act if the disclosure is made for a purpose of that Act or the
Immunization of School Pupils Act;” 251

“To a public health authority that is similar to the persons described in clause (a) and that is
established under the laws of Canada, another province or a territory of Canada or other
jurisdiction, if the disclosure is made for a purpose that is substantially similar to a purpose of the
Health Protection and Promotion Act or the Immunization of School Pupils Act.” 252

Public safety purpose:

“A health information custodian may disclose personal health information about an individual if
the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of
eliminating or reducing a significant risk of serious bodily harm to a person or group of
persons.” 253

Healthcare planning or delivery (on conditions approved by the Information and Privacy
Commissioner):

---

248 Ibid at s. 37 (1) (d).
249 Ibid at s. 37 (1) (c).
250 Ibid at s. 39 (2).
251 Ibid at s. 39 (2) (a).
252 Ibid at s. 39 (2) (a.1.).
253 Ibid at s. 40 (1).
A “health information custodian may disclose to a prescribed entity personal health information for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services, if the entity … has in place practices and procedures to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of the information; and … the Commissioner has approved the practices and procedures, if the custodian makes the disclosure on or after the first anniversary of the day this section comes into force.”

This provision does not allow for the disclosure of information collected in counselling sessions.

Healthcare planning or delivery (for individual receiving healthcare from multiple health information custodians):

Such a disclosure can be made if:

“the disclosure is to another custodian described in paragraph 1, 2 or 4 of the definition of “health information custodian” in subsection 3.”

“the individual to whom the information relates is one to whom both the disclosing custodian and recipient custodian provide health care or assist in the provision of health care or have previously provided health care or assisted in the provision of health care, and”

“the disclosure is for the purpose of activities to improve or maintain the quality of care provided by the receiving custodian to the individual to whom the information relates or individuals provided with similar health care”

Health system management (on the request of the Minister):

“Subject to the restrictions, if any, that are prescribed, a health information custodian shall, upon the request of the Minister, disclose personal health information to a health data institute that the Minister approves under subsection (9) for analysis with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services, if the requirements of this section are met.”

Prince Edward Island

Use:

Public health or public safety:

“[T]o prevents or reduce a risk of significant harm to the health or safety of the public or a group of people.”

Healthcare planning or delivery:

“[I]f the custodian is a public body, for planning or delivering programs or services that the custodian provides or that the custodian funds in whole or in part, allocating resources to any of

---

254 Ibid at s. 45 (3).
255 Ibid at s. 45 (3) (2).
256 Ibid at s. 39 (1) (d) (i).
257 Ibid at s. 39 (1) (d) (ii).
258 Ibid at s. 39 (1) (d) (iii).
259 Ibid at s. 47 (2).
260 Prince Edward Island Health Information Act, R.S.P.E.I. 1988, c. H-1.41. at s. 5 (d).
those programs or services, evaluating or monitoring any of them or detecting, monitoring or preventing fraud or any unauthorized receipt of services or benefits related to any of them.”

Risk management and quality assurance:

“[F]or the purpose of risk management or error management or for the purpose of activities to improve or maintain the quality of health care or to improve or maintain the quality of any related programs or services of the custodian.”

Education and training:

“[F]or educating agents of the custodian to provide health care.”

Data matching:

“For the purpose of performing data matching.”

The Act includes considerable powers for custodians to perform data matching (i.e. data linkage) for their own internal use purposes. No additional formalities need be met if this is done.

These powers also enable custodians to perform the data matching their own data with the data of other health information custodians or non-custodians. These powers further enable custodians to allow researchers to perform data matching once certain formalities have been met.

In the latter instances (i.e., external disclosure and research), health information custodians must perform a Privacy Impact Assessment and submit it to the Commissioner for comment prior to engaging in such data matching.

Health system management and public health surveillance:

“[F]or the purpose of the custodian’s:

(i) planning and resource allocation,
(ii) health system management,
(iii) public health surveillance,
(iv) health policy development, or
(v) delivery or administration of health care.”

Disclosure:

Disclosure for public health, individual safety or public safety purposes:

---

261 *Ibid* at s. 5 (e).
262 *Ibid* at s. 5 (f).
263 *Ibid* at s. 5 (g).
264 *Ibid* at s. 5 (o).
265 *Ibid* at s. 26 (1).
266 *Ibid* at ss. 27 (1), 28 (1).
267 *Ibid* at ss. 26 (2), 29, 31 (c) 32 (3).
268 *Ibid* at ss. 27 (2, 28 (2), 29.
269 *Ibid* at s. 5 (q).
“A custodian may disclose personal health information without the consent of the individual to whom it relates if the custodian reasonably believes that disclosure is required

(a) to prevent or reduce a risk of serious harm to the health or safety of the individual to whom it relates or another individual; or

(b) to prevent or reduce a risk of significant harm to the health or safety of the public or a group of people.”  

**Healthcare planning or delivery (internal):**

“[F]or the purpose of delivering, evaluating or monitoring a program of the custodian that relates to the provision of health care or the payment for health care”

**Healthcare planning or delivery (other custodian providing healthcare to the concerned individual):**

“[F]or the purpose of review and planning necessary for the provision of health care to the individual to whom the personal health information relates by another custodian.”

**For risk management or quality assurance purposes:**

“[T]o a person who requires the personal health information to carry out an audit for, or to provide legal services, error management services, risk management services, peer reviews or quality improvement services to, the custodian.”

The Minister has additional powers to unilaterally require the communication of health data for numerous healthcare planning, management, and monitoring purposes.

**Quebec**

In Quebec, the powers and obligations of health institutions concerning the collection, use, and disclosure of health information differs across public sector health institutions and private sector health organizations.

Further obligations and powers related to the use and disclosure of health information are also enshrined in the *Act Respecting Health and Social Services*, as described below.

**Public sector institutions** can use or disclose personal information for the following purposes:

**Use:**

Collection and use of information necessary to the exercise of its powers or the performance of its functions:

---

270 *Ibid* at s. 24 (1).
271 *Ibid* at s. 13 (d).
272 *Ibid* at s. 13 (e).
273 *Ibid* at s. 13 (1) (g).
274 *Ibid* at s. 16.
“Collect [and subsequently use] personal information if it is necessary for the exercise of the rights and powers or for the implementation of a program of a public body with which it cooperates to provide services or to pursue a common mission.

The information referred to in the second paragraph is collected under a written agreement that is sent to the Commission. The agreement comes into force 30 days after it is received by the Commission.”

**Use for a consistent purpose:**

“If the information is used for purposes consistent with the purposes for which it was collected.”

**Disclosure:**

**Disclosure to public bodies:**

“A public body may, without the consent of the person concerned, release personal information:

(1) to a public body or an agency of another government if it is necessary for the exercise of the rights and powers of the receiving body or the implementation of a program under its management.”

Such a disclosure must be subject to an agreement, the conditions of which are described in the footnote below.

The Commission d’accès à l’information (CAI) must approve the agreement prior to the disclosure being performed. The CAI must issue its decision within a time limit of sixty days of receiving the proposed agreement, subject to extension in certain circumstances.

**Disclosure according to exceptional circumstances:**

“To a person or a body where exceptional circumstances justify doing so.”

Such a disclosure must also be subject to an agreement, the conditions of which are described in this footnote.

---

276 *Ibid* at s. 65.1.
277 *Ibid* at s. 64.
278 *Ibid* at s. 65.1 (1).
279 *Ibid* at s. 68 (1).
280 *Ibid* at s. 70.
281 *Ibid* at s. 68 (2).
282 The information is released under a written agreement that indicates:
(1) the identity of the public body releasing the information and of the person or body collecting it;
(2) the purposes for which the information is released;
(3) the nature of the information released;
(4) the method of transmitting the information;
(5) the security measures necessary to ensure the protection of the information;
(6) the intervals at which the information is released; and
(7) the duration of the agreement.
The Commission d’accès à l’information (CAI) must approve the agreement prior to the disclosure being performed. The CAI must issue its decision within a time limit of sixty days of receiving the proposed agreement, subject to extension in certain circumstances.\textsuperscript{283}

**Private sector organizations** can use or disclose personal information for the following purposes:

Disclosure to public bodies in the exercise of their functions:

“[T]o a public body within the meaning of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1) which, through a representative, collects such information in the exercise of its functions or the implementation of a program under its management.”\textsuperscript{284}

Disclosure to other bodies in the exercise of their functions:

“to a person or body having the power to compel communication of the information if he or it requires it in the exercise of his or its duties or functions.”\textsuperscript{285}

**Health institutions** can further disclose personal information for the following purposes:

**Public health purposes:**

“[F]or the purposes of the Public Health Act.”\textsuperscript{286}

**Disclosure of information to the Minister:**

“In performing his duties under section 431, the Minister may require an institution to furnish to him, at the time and in the form he determines, the information, whether personal or not, prescribed by regulation under subparagraph 26 of the first paragraph of section 505 concerning needs for and utilization of services.”\textsuperscript{287}

The duties established at s. 431 include a broad range of functions related to healthcare provision, health system improvement, quality assurance, and health care coordination, amongst others.\textsuperscript{288}

**Saskatchewan**

**Use and disclosure:**

Health information custodians can use\textsuperscript{289} or disclose personal health information as follows:

“[F]or the purpose for which the information was collected by the trustee or for a purpose that is consistent with that purpose”\textsuperscript{290}

\textsuperscript{283} *Ibid* at s. 70.

\textsuperscript{284} *Act respecting the protection of personal information in the private sector* at s. 18 (5).

\textsuperscript{285} *Ibid* at s. 18 (6).

\textsuperscript{286} *Act Respecting Health Services and Social Services* R.S.Q. c. S-4.2, at s. 19 (9).

\textsuperscript{287} *Act Respecting Health Services and Social Services* R.S.Q. c. S-4.2, at s. 433.

\textsuperscript{288} *Ibid* at s. 431.

\textsuperscript{289} *The Health Information Protection Act*, Chapter H-0.021 of the Statutes of Saskatchewan, 1999 at s. 26 (2) (a).

\textsuperscript{290} *Ibid* at s. 27 (2) (a).
To “avoid or minimize a danger to the health or safety of any person.”$^{291}$

For the purpose of “planning, delivering, evaluating or monitoring a program of the trustee.”$^{292}$

“[W]here the disclosure is being made to a standards or quality of care committee established by one or more trustees to study or evaluate health services practice in a health services facility, health region or other health service area that is the responsibility of the trustee, if the committee:

(i) uses the information only for the purpose for which it was disclosed;
(ii) does not make a further disclosure of the information; and
(iii) takes reasonable steps to preserve the confidentiality of the information.”$^{293}$

**Yukon**

**Use:**

**Risks to health or safety:**

“(i) [P]reventing or reducing a risk of serious harm that the custodian reasonably believes exists to the health or safety of any other individual, or

(ii) assessing whether such a risk exists.”$^{294}$

**Family or genetic history:**

“(F)or the purpose of assembling a family or genetic history for the individual.”$^{295}$

“(F)or the purpose of educating agents of the custodian in respect of the provision of health care.”$^{296}$

**Healthcare management and healthcare audit:**

“(F)or the purpose of managing or auditing the health care activities of the custodian”$^{297}$

“(F)or the purpose of carrying out quality improvement”$^{298}$

**Management of healthcare programs (Minister or Department of Health)**

---

$^{291}$ *Ibid* at s. 27 (4) (a).
$^{292}$ *Ibid* at s. 27 (4) (k) (ii).
$^{293}$ *Ibid* at s. 27 (4) (g).
$^{294}$ *Health Information Privacy and Management Act, SY 2013, c.16* at s. 56 (1) (c).
$^{295}$ *Ibid* at s. 56 (1) (d).
$^{296}$ *Ibid* at s. 56 (1) (g).
$^{297}$ *Ibid* at s. 56 (1) (l).
$^{298}$ *Ibid* at s. 56 (1) (m).
“[U]se an individual’s personal health information and, where the custodian is the Minister or the Department, an individual’s personal information, for the purpose of carrying out, otherwise than by providing health care to the individual, a statutory duty, function or power of the custodian or any of its programs or activities.”

**Health System Planning (as prescribed):**

“The Minister, the Department, the Yukon Hospital Corporation or a prescribed branch, operation or program of a public body may, without an individual’s consent, use the individual’s personal health information for the purpose of the planning and management of the health system.”

**Disclosure:**

**Risks to health or safety:**

“for any purpose other than providing health care to the individual, if the custodian reasonably believes that the disclosure will prevent or reduce a risk of serious harm to the health or safety of any other individual, or will enable the assessment of whether such a risk exists.”

**For risk management or quality assurance purposes:**

“[F]or the purpose of carrying out quality improvement for or on behalf of the custodian.”

“to the Minister, the Department, the Yukon Hospital Corporation or a prescribed branch, operation or program of a public body, for the purpose of the planning and management of the health system”

---

299 *Ibid* at s. 56 (3) (a).
300 *Ibid* at s. 54.
301 *Ibid* at s. 58 (h).
302 *Ibid* at s. 58 (k).
303 *Ibid* at s. 58 (l).
“[T]o a custodian that is a branch, operation or program of a Yukon First Nation for planning and management of that Yukon First Nation’s health system”\textsuperscript{304}

“[T]o the Canadian Institute for Health Information, or to a prescribed health data institute in Canada that has entered into a written agreement with the Minister governing its collection, use and disclosure of the personal health information.”\textsuperscript{305}

\textbf{For public health purposes:}

“[T]o the chief medical officer of health under the Public Health and Safety Act, or to a public health authority that is established under the laws of another jurisdiction, if the disclosure is made to permit the chief medical officer or the authority to discharge a duty, function or power under that Act or a substantially similar duty, function or power.”\textsuperscript{306}
APPENDIX B: Comparison of Provincial Public Health Acts

General power to access and use personal information for public health surveillance

British Columbia
BC’s Public Health Act places significant emphasis on health protection and promotion. Information can be collected and disclosed as long as it is necessary for any purpose listed in Division 3: Reporting Disease, Health Hazards and Other Matters. The purposes include, but are not limited to, identifying an individual who is receiving health services, preventing chronic conditions at the individual or population level, health services development, public health surveillance, addressing threats to public health, and conducting research into health issues.

Manitoba
Information is reportable in Manitoba if there is a threat to public health even if the information is personal and confidential. However, there is a necessity standard, as is the case in many other provinces. In dealing with threats to public health, information can be disclosed to ministers or to government bodies in charge of public health. Personal information is only to be used if non-identifying information does not accomplish the purpose.

Newfoundland and Labrador
Newfoundland and Labrador collect information for public health surveillance, managing diseases, and conducting or facilitating research among other uses. The Public Health Act explicitly states that the “minimum” amount of information necessary should be collected or disclosed to accomplish the purpose.

Northwest Territories
Similar to the other Public Health Acts in this section, the Northwest Territories allows for collection of personal health information without consent for development of public health policies, public health surveillance, and health promotion. The information must be necessary for the purpose it is collected and the Act instructs the public health officer to make security arrangements against risks such as “unauthorized access, collection, use, disclosure, or disposal.” Personal health information may be disclosed for purposes related to examination or treatment of an individual, to prevent or control the spread of disease, to regulatory bodies requesting the information, and for potential investigation into the conduct of a health care professional. Non-identifying information may be disclosed for a “use consistent with the purpose for which personal health information may be collected.”

308 Ibid at s 9(1).
309 Manitoba, The Public Health Act, C.C.S.M. c. P210 at s 78(1).
310 Ibid at s 80.
311 Ibid at s 103(3).
313 Ibid at s 15(2) and s 16(2).
315 Ibid at s 35(2).
316 Ibid at s 38(1).
317 Ibid at s 40.
Nova Scotia
Nova Scotia allows collection and disclosure of information for ongoing surveillance as well as medical officers carrying out their functions and duties. Hospitals must also make full disclosure of medical records upon request. A unique component in Nova Scotia’s Public Health Act is that medical officers may enter any premises at a reasonable time and may require a person to provide personal health information or confidential business information when it is reasonably required to investigate a potential health hazard or disease. This applies notwithstanding FIPPA.

Nunavut
Collection of health information in Nunavut by the Chief Public Health Officer can be done for the purpose of public health surveillance, which places it in the broad power category. Health information collected under the Nunavut Public Health Act can only be disclosed in two forms: “(a) aggregate health information that relates only to groups of individuals in the form of statistical information or aggregated, general or anonymous data; or (b) anonymous health information that relates to an unidentifiable individual.” There is a duty to warn and protect present in the Act, however the Chief Public health officer is not required to disclose information if they believe that disclosure would result in a “clear and overriding adverse effect”. This would include violating privacy rights, stigmatising groups, causing behaviour that would result in an increased risk to public health.

Quebec
Ongoing surveillance of the health status of the population in Quebec is an exclusive function of the Minister and public health directors. However, they can confer the mandate of surveillance on the Institut National de Santé Publique. The Minister has more power compared to public health directors/authorities. In cases where the public health director believes on reasonable grounds that the health of the public is threatened, they may authorize communication or disclosure of information. The information may also be disclosed to any health authority outside of Quebec if it is necessary to protect the health of that authority’s population or is part of a prior agreement.

Prince Edward Island
This Public Health Act stipulates that one may collect any information necessary to assess a threat to public health as well as evaluating and monitoring the health and safety of the general public. This ongoing surveillance is characteristic of all the provinces in this category.

---

318 Nova Scotia Health Protection Act, S.N.S. 2004, c. 4, at s 14(1).
319 Ibid at s 16(2).
320 Ibid at s 58(1).
321 Ibid at s 107.
322 Nunavut Public Health Act, SNu 2016, c. 13, at s. 17 (1).
323 Ibid at s. 18.
324 Ibid at s 50.
325 Quebec Public Health Act R.S.Q., c. S-2.2 at s. 34.
326 Ibid at s 34.
327 Ibid at s 133.
328 Ibid.
More limited powers to access personal info for the purpose of responding to public health emergencies or to other potential threats to public health

**Alberta**

Alberta’s Public Health Act is actually quite similar to the provinces in the section above, but does not extend its power to ongoing surveillance. Information can be collected during a public health emergency or in the event of a threat to public health. The Act contains a “diseases under surveillance section” which states where a disease is not a notifiable disease and where the chief medical officer considers it advisable to keep that disease under surveillance, the chief medical officer may require medical officers, physicians or lab directors to provide any information related to the disease. In addition, as specified above, Alberta public health legislation creates broad powers for public health authorities to requisition and use personal information in relation to communicable diseases, including for purposes related to healthcare improvement, health research and public health. Information collected and used for these purposes cannot be disclosed, except for a narrow range of enumerated purposes.

**Ontario**

Ontario allows the chief medical officer of health to make an order if they are of the opinion (reasonable and probable grounds) that the information is necessary to “investigate, eliminate or reduce the immediate and serious risk to the health of any persons” and the quantity of information is no more than reasonably necessary for that purpose. Information may only be disclosed or used for the purposes of investigation, eliminating or reducing the risk to the health of persons in Ontario.

**Yukon**

The Yukon Public Health Act specifies that the Minister and chief medical officers of health may indirectly collection personal information. This Act specific that the Access to Information and Protection of Privacy Act does not apply to the information is it is collected during and in relation to a health emergency.

---

331 *Ibid* at s 16 (1).
332 *Ibid* at s 53 (2).
333 Ontario *Health Protection and Promotion Act*, R.S.O. 1990, c. H.7 at s 77.6 (2).
334 *Ibid* at 77.6 (3).
336 *Ibid* at s 2.1(2).
Narrow powers to combat known threats or collect information about known cases for the purposes of combatting infectious diseases

**New Brunswick**
In New Brunswick, a medical officer of health may collect and use personal health information without the consent of the individual if it is required to contain and prevent the spread of a notifiable disease or to mitigate risks of a health hazard. 337 This is more specific than the other provinces and territories and gives this legislation a narrower ambit.

**Saskatchewan**
Pursuant to the public health act, the minister may make the necessary orders and regulations that are necessary to protect the public health for the following purposes: “1) the control, notification, prevention and treatment of all communicable disease and 2) the reporting to a medical officer by every medical practitioner of persons under his treatment suffering from a communicable disease”. 338 This is slightly more broad than the powers in New Brunswick since it specifies all communicable diseases as opposed to notifiable diseases.

---

## APPENDIX C: Comparative Powers to Collect Personal Information – Federal and Provincial Public Sector Institutions

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Canada</td>
<td><em>Privacy Act</em> R.S.C., 1985, c. P-21</td>
</tr>
<tr>
<td></td>
<td>4: No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.</td>
</tr>
<tr>
<td></td>
<td>Collection:</td>
</tr>
<tr>
<td></td>
<td>33 (c): No personal information may be collected by or for a public body unless (…) that information relates directly to and is necessary for an operating program or activity of the public body.</td>
</tr>
<tr>
<td></td>
<td>Collection:</td>
</tr>
<tr>
<td></td>
<td>26 (c): the information relates directly to and is necessary for a program or activity of the public body.</td>
</tr>
<tr>
<td>Manitoba</td>
<td><em>Freedom of Information and Protection of Privacy Act</em> C.C.S.M. c. F175.</td>
</tr>
<tr>
<td></td>
<td>Collection:</td>
</tr>
<tr>
<td></td>
<td>26 (1) (b): the information relates directly to and is necessary for an existing service, program or activity of the public body.</td>
</tr>
<tr>
<td></td>
<td>Collection:</td>
</tr>
<tr>
<td></td>
<td>37 (2):</td>
</tr>
<tr>
<td></td>
<td>[P]ersonal information may also be collected by or for a public body [if] …</td>
</tr>
<tr>
<td></td>
<td>(a) the information relates directly to and is necessary for:</td>
</tr>
<tr>
<td></td>
<td>(i) a service, program or activity of the public body, or</td>
</tr>
<tr>
<td></td>
<td>(ii) a common or integrated service, program or activity.</td>
</tr>
<tr>
<td>Newfoundland and Labrador</td>
<td><em>Access to Information and Protection of Privacy Act</em> SNL2015 Chapter A-1.2</td>
</tr>
<tr>
<td></td>
<td>Collection:</td>
</tr>
<tr>
<td>Northwest Territories</td>
<td>Access to Information and Protection of Privacy Act, SNWT 1994, c.20</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Collection:</strong></td>
<td></td>
</tr>
<tr>
<td>40 (c):</td>
<td><strong>[T]he information relates directly to and is necessary for:</strong></td>
</tr>
<tr>
<td></td>
<td>(i) an existing program or activity of the public body, or</td>
</tr>
<tr>
<td></td>
<td>(ii) a proposed program or activity where collection of the information has been authorized by the head with the approval of the Executive Council.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collection:</strong></td>
<td></td>
</tr>
<tr>
<td>24 (1) (c):</td>
<td>Personal information shall not be collected by or for a public body unless … that information relates directly to and is necessary for an operating program or activity of the public body.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nunavut</th>
<th>Access to Information and Protection of Privacy Act, SNWT 1994, c.20</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collection:</strong></td>
<td></td>
</tr>
<tr>
<td>40 (c):</td>
<td><strong>[T]he information relates directly to and is necessary for:</strong></td>
</tr>
<tr>
<td></td>
<td>(i) an existing program or activity of the public body, or</td>
</tr>
<tr>
<td></td>
<td>a proposed program or activity where collection of the information has been authorized by the head with the approval of the Executive Council.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collection:</strong></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Act/Statute Description</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| Prince Edward Island | P.E.I *Freedom of Information and Protection of Privacy Act*  
Collection:  
31 (c): No personal information may be collected by or for a public body unless … that information relates directly to and is necessary for an operating program or activity of the public body. |
| Quebec | *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* chapter A-2.1  
Collection:  
64: No person may, on behalf of a public body, collect personal information if it is not necessary for the exercise of the rights and powers of the body or the implementation of a program under its management.  
A public body may, however, collect personal information if it is necessary for the exercise of the rights and powers or for the implementation of a program of a public body with which it cooperates to provide services or to pursue a common mission.  
The information referred to in the second paragraph is collected under a written agreement that is sent to the Commission. The agreement comes into force 30 days after it is received by the Commission. |
| Saskatchewan | *Freedom of Information and Protection of Privacy Act* Chapter F-22.01 of the Statutes of Saskatchewan, 1990-91  
25: No government institution shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the government institution. |
| Yukon | *Access to Information and Protection of Privacy Act* SY 2018, c.9; amended by SY 2019, c.15  
Collection:  
15 (c):  
A public body may collect the personal |
information of an individual only if …

The collection relates to, and is directly necessary for the purposes of:

(i) carrying out or evaluating a program or activity of the public body, or a data-linking activity in respect of which the public body is a partner

(ii) providing or evaluating a specialized service in respect of which the public body is the personal identity manager or a partner, or

(iii) planning:

(A) a proposed program or activity of the public body

(B) a proposed specialized service in respect of which the public body is the personal identity manager or a partner, or

(C) a proposed data-linking activity in respect of which the public body is a partner.
APPENDIX D: Using or Sharing Information and Research Participant Consent

Research institutions should consider what permissions in information are necessary to intended research, and integrate such permissions to their core consent elements. These core consent elements should guide the creation of their informed consent materials. Contributors to an inter-institutional research collaboration should agree to common core consent elements for the overall collaboration.

Despite the need to tailor core consent elements to the circumstances of each intended research collaboration, the following core consent elements should always be used as a mandatory minimum set of permissions, to maximize the future compatible use of the information (cited from Bernier and Knoppers, below):

Permission to use information for:

1. Further biomedical research.
2. Open-access sharing of aggregated or anonymized [information].
3. Controlled-access sharing of individual-level identifiable (coded) [information].
4. International sharing of research [information].
5. Commercial and non-commercial research purposes.
6. The storage of [information] on a cloud platform.
7. In combination with other sources of research or health [information].

If information is not subject to an informed consent to research participation that captures the intended secondary use thereof, it can be necessary to follow the steps outlined below to perform the intended secondary use or intended information sharing exercise.

1. A Research Ethics Committee provides an ethics waiver of consent, allowing for the use or sharing thereof for the purposes established in the core consent elements without obtaining consent from the research participants.

2. The research participants are re-contacted for the purpose of providing consent to the use of their information, in accordance with the core consent elements of the information use or information sharing initiative. Research Ethics Committees (RECs) are often required to approve the recontact of research participants for the purposes of obtaining consent to the further use of their research information.

3. Another source of legal authorization that allows research participants to use or share the information for the purposes established in the core consent elements. Legal authorization exists for downstream recipients to use or access such information for the purposes established in the core consent elements.
4. Information that is anonymized prior to its use or the sharing thereof can generally be used or shared without obtaining research participant consent, subject to local legal or ethical requirements and applicable formalities.

**Examples of Retrospective Consent Filters used to assess the potential to use or to share information in reliance on an existing informed consent to research participation, or to determine the additional steps required to deposit information in a repository, are replicated below:**

The International Cancer Genome Consortium (ICGC)

![ICGC-ARGO consent assessment tool for participation.](image)

---

**FIGURE 2 | ICGC-ARGO consent assessment tool for participation.**
The COVID-19 Immunity Task Force

**STEP I:**

Is there an appropriate authorization in place to generate the intended data from the consented biological sample or samples? (If yes, e.g., a valid research ethics consent, a research ethics committee waiver of consent requirement, or an applicable regulatory or statutory authorization allowing for the contribution of the data).

- If the question is **not applicable** because the biological sample has already been analyzed and the concerned data has already been derived, please proceed to **STEP II**.
- If the answer is **Yes**, please proceed to **STEP II**.
- If the answer is **No**, the tissue sample cannot be used to generate data for the CITF without first obtaining an appropriate approval or ethics waiver. Please proceed to **STEP III**.

**STEP II:**

**Question 1:** Has the sample donor or research participant provided informed consent to general research use:

<table>
<thead>
<tr>
<th>Does the consent form indicate that:</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Data can be used for any future, unspecified research purpose?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Data will be shared through a registered access or controlled access database that allows researchers in any part of the world to access the data for any approved research purpose?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- If you have answered yes to both questions, your datasets can be deposited in the CITF Database. (Please note that some institutional policies may require local ethics committee approval, or other regulatory approval, before data can be deposited in the CITF Database).
- If you have answered no to either question, please proceed to **Question II**, below.

**Question 2:** Has the sample donor or research participant provided informed consent to all of the following:

<table>
<thead>
<tr>
<th>The informed consent form or other valid record of consent indicates consent to the following:</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) The intended serological, immunological, and other tests can be performed using the collected samples?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Data will be shared internationally?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c) Data may be stored on centralized servers including outside the province or country of collection, and on cloud servers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d) Data will be stored for an indefinite period of time?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e) The withdrawal of data is not possible if already used or published.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>f) There is a possible risk of re-identification in the future?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g) Data can be used to perform future health research on COVID-19 and related health outcomes?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>h) Data can be used for commercial research purposes?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>i) Coded data can be shared with approved researchers through a controlled access mechanism?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>j) Public sharing of anonymized or aggregated data?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- If you have answered yes to all of the above, your data can be deposited directly in the CITF Database.
- If you have answered no to any of the above, please proceed to **STEP III** to determine if re-consent of donors is possible, or whether a consent waiver should be obtained from the appropriate research ethics committee or equivalent body.
Step III:

Question 1:

<table>
<thead>
<tr>
<th>Re-contact / re-consent</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Does your consent form or other applicable local policy allow for re-contact of donors/research participants?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Is it feasible for you to re-contact and re-consent your donors/research participants for inclusion in the CITF Database?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

➢ If you have answered yes to both questions, please re-contact and re-consent the donors and include the CITF Minimum Informed Consent Elements in your consent materials. The CITF Model Informed Consent Materials can be used to obtain this consent.

➢ If you have answered no to either question, please proceed to Question II, below.

Question 2:

<table>
<thead>
<tr>
<th>Consent waiver</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Is it possible for you to apply to a local ethics committee (or equivalent) to obtain a waiver of consent requirement to deposit your dataset in the CITF Database?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Is it possible for you to apply to a local ethics committee (or equivalent) to obtain an authorization to “anonymize”/de-identify the data to deposit it in the CITF Database?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

➢ If you have answered yes to either question, please request and obtain a consent waiver according to your local procedures, or “anonymize”/de-identify your dataset following local requirements.

➢ If you have answered no to both questions, your data cannot be deposited in the CITF Database.
APPENDIX E: Security Safeguards

Common Information Handling Practices Recommended by Courts and Regulators

Regulators and courts have recommended the adoption of the following general information handling practices for the purpose of ensuring compliance with security requirements:

Organizational safeguards:

- Limiting user access rights to record containing personal information to the minimum necessary to perform their functions.
- Binding agents or employees to respect a confidentiality agreement that contains a non-disclosure covenant.\textsuperscript{339}
- Using contracts to establish the respective rights and obligations of affiliates, third-party service providers, and of the health information custodian itself in the collection, use, and disclosure of personal health information.\textsuperscript{340} This can be achieved through the use of a master governance document establishing the overall information flows and privacy management practices throughout the organization, and using further contracts to establish the specific details of such information flows and practices.\textsuperscript{341}

If significant quantities of sensitive information are being shared with third-party service providers, contracts used to share information should, according to the Office of the Privacy Commissioner of Canada, stipulate the following:\textsuperscript{342}

- The information being shared with the third-party institution.
- The specific rules, regulations, and requirements that information recipients must uphold (including the legal obligations from the source jurisdiction, where applicable, that must continue to be complied with, and other policies governing the use of the information).
- The respective roles and responsibilities of stakeholders in the institution sharing the information and of the recipient institution regarding issues such as decision-making, safeguards, and breach-response.
- How the information can be used.
- How and when the information must be destroyed.
- Reporting and oversight mechanisms anticipated to ensure compliance with the agreement.

\textsuperscript{340} Saskatchewan OIPC, \textit{supra} n. 116 pp. 43, 99-100.
\textsuperscript{341} Ibid at p. 43.
Centre of Genomics and Policy

- Establish a clear contractual right to audit the activities of affiliates and third-party service providers.\(^{343}\)

Ongoing audit of required security practices:

- Third-party service providers must be required to demonstrate compliance with recognized security standards (e.g. ISO Security Standards) and be subject to audits from auditors that are recognized in the field.\(^{344}\)

**Technological safeguards:**

**Implementation and audit of user access controls using technological systems**

- Limiting user access to only to those records that are required for the user to fulfill their functions.\(^ {345}\)

- Ensuring that user access to specific records hosted on informatics platforms can be audited on a per-user and per-access basis.\(^ {346}\)

- Performing audits of user access on a frequent basis, both where justified by the circumstances (e.g., following a potential security incident, or where unusual network activity is detected) and at random.\(^ {347}\)

- Integrating granular access controls to technological platforms that allow information access permissions to be regulated on a per-role or a per-user basis.\(^ {348}\)

**Ensure that access credentials are managed in a secure fashion**

- Require users to establish a unique and secure password prior to accessing information.\(^ {349}\)

- Implement secure access mechanisms such as two-factor authentication.\(^ {350}\)


\(^{345}\) Ontario IPC, Order HO-013 (2014). See also: McIsaac et al., *supra* n.339.


\(^{347}\) Ontario IPC, Order HO-013 (2014). See also: McIsaac et al., *supra* n. 339.

\(^{348}\) Ontario IPC, Order HO-002 (2006). See also: McIsaac et al., *supra* n. 339.


\(^{350}\) *Ibid* at para 66.
Manage and mitigate security vulnerabilities

- Implement basic information security practices including encryption of credentials and the maintenance of valid SSL certificates. Encryption at rest can sometimes be required for highly sensitive information.
- Identify security vulnerabilities through the use of internal and external audits (including audits for compliance with ISO standards, internal and external penetration testing, and maintaining penetration testing reports).
- Perform network segregation (i.e., the separation of information using network architecture and firewalls) to keep apart information that has different functions, and further segregate information according to the sensitivity thereof.
- Ensure that security vulnerabilities are remediated in reliance on the following measures:
  1. Continuous identification and ‘flagging’ of vulnerabilities.
  2. Systems in place to ensure the rectification of vulnerabilities identified.
  3. Verification and confirmation that identified vulnerabilities are rectified.

Physical safeguards:

- Holding paper records, servers, and networking equipment in locked spaces.
- Ensuring that paper records slated for destruction are securely shredded or otherwise irreversibly destroyed.
- Keeping records on encrypted devices while they are being transported from one place to another, and keep them in an encrypted form if held on computer that is in an individual’s home (or similarly shared space).

---

353 OPC, PIPEDA Report of Findings #2019-001: Investigation into Equifax Inc. and Equifax Canada Co.’s compliance with PIPEDA in light of the 2017 breach of personal information, supra n. 342 at paras 118-123.
354 Ibid at paras. 29-34.
355 Ibid at para. 27.
356 Saskatchewan OIPC, supra n. 116.
357 Ibid.
358 Newfoundland and Labrador IPC, Report PH-2012-001-2012. See also: McIsaac et al., supra n. 339.
APPENDIX F: Primer on Technological Approaches to Information Governance

Tool: Quantitative Assessments of Information Identifiability

Quantitative metrics for assessing information identifiability have been devised to help assess if the information poses a significant risk of inducing individual re-identification.

K-anonymity is one of the most prominent quantitative methods used to assess the identifiability of information. This assessment is performed in determining which variables in a structured dataset are potential identifiers (i.e., elements that could be used to perform the identification of a concerned individual), and then in determining how many different individual records share the same combination of identifiers in an overall dataset.

This requires the data users to compare the records in the dataset, to see which records have significant amounts of data in common, and which do not. For instance, this can require examining the values for each record associated with potential identifiers such as age and weight, and determining if a sufficient number of other records are comprised in the dataset that belong to individuals of the same age and weight. If yes, this demonstrates that it will not be possible to perform re-identification of individuals based on the attributes concerned, because these attributes are shared by a large number of persons and therefore making them known does not create privacy risks.

If a sufficient number of individuals share each combination of potential identifiers represented in a dataset, the information can be considered ‘k’ - anonymized.359 If a dataset is ‘k’ anonymized, it means that each individual in the dataset shares their combination of potential identifiers with at least ‘k’ individuals in the dataset (including themselves).

The central idea is that a potential identifier is a personal attribute that could help determine who a specific person is from amongst the general population. These include age, gender and profession, amongst others. If all individuals in a dataset have potential identifiers that are indistinguishable from those of a large enough group of other individuals in that dataset, the dataset can be presumed anonymized. This is the case since it can be demonstrated that each individual in the dataset has the same attributes as a certain number of other individuals comprised in the dataset. It is therefore possible to infer that each individual in the dataset has the same attributes as a certain number of other individuals in the general population, and that sharing the information does not create a privacy risk.360

Canadian regulators have published guidance that uses k-anonymization techniques to assess the identifiability of structured datasets. Canadian regulators, as well as Health Canada, generally propose that structured data should be considered anonymized if it can meet a certain threshold of ‘k’ anonymity. This standard is met if a certain number of records contain each combination of potential identifiers present in the dataset. For public releases, this is generally held to require

---

359 El Emam & Dankar, supra n. 156.
360 El Emam & Arbuckle, supra n. 156 at Part 2: A Risk-Based de-Identification Methodology.
at minimum 11 records to contain the least common combination of potential identifiers in the dataset \((k = 0.09)\), or 20 records for more strict applications \((k = 0.05)\). Less stringent standards are relied on for controlled information releases.\(^{361}\)

**Tool: Differential Privacy and Genomic Beacon Systems**

The following two technological tools can be used for the purpose of ensuring that aggregate information does not create a risk of causing the re-identification of the individuals whose information is contained in the aggregate dataset.

**Differential privacy**

Differential privacy is used to safeguard aggregate quantitative data from attempted re-identification. This is achieved in providing a mathematical guarantee that the inclusion or exclusion of a single individual’s record in the overall dataset cannot significantly change the aggregate results returned in aggregating the data or performing a query for information from a subset of the overall dataset.\(^{362}\) This protects the individuals comprised in the dataset from attempted re-identification performed in comparing the results of the aggregation process – or similar data queries – with and without a targeted individual’s data included.

This comparison is made for the purposes of determining if that person’s record is contained in the aggregate dataset, which can be inferred if the aggregate result or queried result changes in an amount that is similar to the targeted individual’s known data.\(^{363}\)

Differential privacy is often achieved in adding noise (i.e., minute and random changes) to the results of queries, or to the results of the aggregation process, to slightly change the results from the true value and therefore preserve the anonymity of the individuals comprised in the datasets used.

**Beacon Systems**

Genomic Beacon Systems are used to help researchers determine if a pool of genetic information contains records that are of research interest to external researchers, prior to their application for access to the individual records held in controlled access.\(^{364}\) To do this, the Beacon system allows researchers to send binary queries regarding the presence or absence of genetic variants that are of research interest to them in the pool of data. The Beacon therefore reveals the presence or absence of the concerned variants in the pool of data.

The data governance challenge inherent in using a Beacon, however, is that certain genetic variants, or certain combinations of genetic variants, are quite rare. It is therefore conceivable that a motivated attacker could compare the known genetic variants of concerned individuals to the genetic variants that a Beacon holds secure. If rare variants belonging to a known person are

---


\(^{362}\) Dwork, *supra* n. 157.

\(^{363}\) *Ibid.*

\(^{364}\) Fiume et al. *supra* n. 158.
replicated in a Beacon System, it stands to reason that the concerned individual’s data is held in the underlying pool of data.\(^{365}\)

To safeguard against this risk, designers can integrate certain privacy controls to a Beacon. For example, one potential solution is for a Beacon to return false results if a sufficient number of queries are made that target the genetic information of single underlying individual. One other prospective solution is to allow each user or IP address a maximum budget of ‘queries’ of the Beacon, to reduce the potential for computer programs to systematically query the Beacon for the genetic information of known individuals to try and re-identify known individuals through trial-and-error.\(^{366}\)

**Tool: Model-to-Data Approaches – Federated Learning and Swarm Learning**

Machine learning is a computer science technique used to teach a computational system to perform a specified task, or to recognize patterns in data.\(^{367}\) Machine learning is performed in providing training data to an untrained algorithm so that the algorithm learns from that data how to perform a task, or how to identify patterns in similar data.\(^{368}\) Traditional approaches to performing machine learning entail the use of data that is stored on a local computer system to train the concerned algorithm.\(^{369}\)

Computer scientists have recognized logistical challenges in storing large quantities of data in a central location, and potential legal compliance issues inherent in moving large quantities of data from disparate institutions to a central location. Therefore, approaches to performing machine learning that do not require the centralization of the data used have been devised.\(^{370}\) One such technique is ‘federated learning.’ In performing federated learning, various local data storage solutions run similar data analysis procedures on their local data and subsequently exchange the parameters and results of this analysis with a central recipient. This maintains privacy and security in eliminating the need to transfer the concerned data.\(^{371}\) The local entities and central entity are in a constant state of communication, to refine and ameliorate the analysis performed. In this model, data is not exchanged between the different entities, but rather, only the results of the analysis performed are shared.\(^{372}\)

Swarm learning is similar to federated learning in several respects. Both approaches involve local entities exchanging the results of analysis instead of exchanging data. Swarm learning, however, does not require a central computational entity to assimilate the results of local analyses. Each local computational network is able to communicate the results of its analysis with other local networks without requiring a central point of communication. As there is no central node responsible for assimilating the results of each local analysis, there is no risk that a

---

\(^{365}\) Raisaro et al. *supra* n. 158.

\(^{366}\) Ibid.


\(^{368}\) Ibid.

\(^{369}\) Warnat-Herresthal et al. *supra* n. 159.


\(^{371}\) Kaisissi et al. *supra* n. 160.

\(^{372}\) Konečný et al. *supra* n. 159. See also: Warnat-Herresthal, *supra* n. 159.
central failure could disrupt the entire machine learning training process.\textsuperscript{373} Swarm learning is also more secure because it entails each participating node executing a predetermined computational process on a secure blockchain network.\textsuperscript{374}

**Tool: Homomorphic Encryption and Secure Multi-Party Computation**

Homomorphic encryption is a process enabling “computations on private health information without actually observing the underlying data.”\textsuperscript{375} This form of encryption allows computer scientists to perform operations on information, but does not allow them to access the concerned information or the results of the operations performed.\textsuperscript{376} Other trusted users can later decrypt the information and access the results of the operations performed. This can be useful, for example, in storing information on an external cloud server, to perform operations on the information without allowing the cloud service provider to access such information.\textsuperscript{377} Rendering homomorphic encryption useful in practice is still a challenge requiring considerable research and development, because most HME schemes do not allow for significant quantities of operations to be performed on the encrypted information, or else are prohibitively computationally intensive.\textsuperscript{378}

Secure multi-party computation is another method of rendering computational analysis more trusted and more secure. This entails numerous parties contributing input information to a common output calculation. Each involved actor can consult the results of the overall output calculation, but cannot observe the input information of the others involved.\textsuperscript{379} These methodologies also have certain limitations regarding their present potential for implementation, due to the high computational burden of performing SMPC and the need for all involved actors to remain connected to the Internet throughout the process.\textsuperscript{380} Certain novel forms of privacy-preserving computation anticipate the combined use of homomorphic encryption and SMPC to overcome the limitations inherent in each of these methods and enable scalable privacy-preserving information analysis to be performed amongst multiple decentralized nodes.\textsuperscript{381}

\textsuperscript{373} Yang et al. *supra* n. 161. See also: Warnat-Herresthal, *supra* n. 159.
\textsuperscript{374} *Ibid.*
\textsuperscript{375} Kocabas & Soyata, *supra* n. 162.
\textsuperscript{376} Acar et al. *supra* n. 162.
\textsuperscript{377} *Ibid.*
\textsuperscript{378} *Ibid.*
\textsuperscript{379} Scheibner et al. *supra* n. 163.
\textsuperscript{380} *Ibid.*
\textsuperscript{381} *Ibid.*
APPENDIX G: Sharing Anonymized Information

How to approach information anonymization

One potential approach to sharing information for a broad range of purposes in compliance with Canadian data protection legislation is to anonymize the information prior to the use or sharing thereof. In the main report, we discussed the general legal tests used to determine if information is regulated identifiable personal information, or is unregulated anonymized information. To determine if information is identifiable personal information, it is necessary to consider both the inherent characteristics of the information, and also the governance conditions that are applicable to its use. Coded information from which all direct identifiers have been removed, and that is held according to stringent organizational and technological governance controls, is generally considered to be anonymized according to Canadian law.

To anonymize information, it is necessary to remove its direct identifiers. It is possible to then assign a unique alphanumeric code to the remaining information to produce coded data. Ideally, this should be done in such a manner that the person or group performing the anonymization does not retain factual knowledge of which information or code belongs to which real-world, underlying individual. As a reminder, direct identifiers are elements that include name, civic address, social security number, etc. These are appellations and unique characteristics that inherently allow an individual that has knowledge of them to single out the concerned individual from amongst the general population. Previous investigation findings of the OPC suggest that if the person or group performing information anonymization retains factual knowledge of the identity of the person to whom a code or a piece of information remains, it could then be considered identifiable personal information that remains subject to Canadian data protection legislation.

Coded information and anonymization

Canadian case law and federal and provincial Privacy Commissioner findings consider that alphanumeric codes associated to individuals or their possessions will not be personal identifiers unless those codes act as direct proxies for the identities of such individuals. This means that non-identifying information will not be considered personal information if it is associated to an alphanumeric code or an object, even if that code or object is closely related to a real-world individual. Therefore, it is our position that coded information is not “about an identifiable individual” and would therefore not be related to a direct identifier, so long as it was not possible to identify the concerned individual in reliance on the code and other available information.

---

384 Canada OPC. PIPEDA Case Summary #2009-018. Psychologist’s anonymized peer review notes are the personal information of the patient.
This means that data could be considered identifiable personal information relative to the information custodian that holds a linkage log and is capable of performing identification, but is anonymized relative to third parties that do not have access to the linkage log. The linkage log here refers to the record establishing the individuals to which each code refers. Further justification for our position is adduced below.

The Office of the Information and Privacy Commissioner of British Columbia has previously affirmed that it considers coded medical information from which all direct identifiers have been removed to be anonymized – and that information linkages can and should be performed on this basis.\textsuperscript{386} Similarly, the Office of the Privacy Commissioner of Canada (OPC) has previously held that non-identifying information about individuals represented through a code or a device identifier that cannot be associated with the concerned individual should be considered anonymized.\textsuperscript{387} This is true even if information linkages are made across multiple activities performed from the same device.\textsuperscript{388} Therefore, coded individual-level information, with or without information linkage being performed, can presumably also be considered anonymized if it is impossible to perform the re-identification of the concerned individual or individuals in reliance on the code. Canadian case law further supports the contention that coded information should be considered anonymized if there is no “serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.”\textsuperscript{389} Courts have considered whether different categories of codes should be considered individual ‘identifiers,’ such that information associated to those codes would be considered personal information.\textsuperscript{390} Case law has established that codes that equate the identity of an individual, such as a social insurance number or a driver’s license number, will often be considered identifiers, but that codes that do not equate the identity of the concerned individual, such as license plates, will not.\textsuperscript{391} A code that is associated to an object is not an identifier unless

\textsuperscript{388} For example, in Cadillac Fairview, the OPC, as well as the Alberta and British Columbia Commissioners, considered that an automatic system in a mall that retained information about device MAC addresses of visitors in a ‘hashed’ (scrambled) format was considered anonymized, despite the fact that the concerned system could automatically identify repeat visitors. Repeat visitors could be identified because the process of hashing the input MAC address would yield the same output information each time an individual with the same MAC address returned to the mall. (See: OPC. Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia. (2020), at paras 113-125).
\textsuperscript{389} In Leon’s Furniture, the Alberta Court of Appeal stated that codes or identification documents that equivocate an individual’s identity should be considered identifiers, whilst codes, documents and objects that are not directly related to an individual’s identity should not. The Court of Appeal considered driver’s licenses, passports, and social insurance numbers to be codes that are identifiers. The Court further held that vehicle license plate numbers should not be considered identifiers, and neither should possessions or immovable properties See: Leon’s Furniture Limited v Alberta (Information and Privacy Commissioner), 2011 ABCA 94 (CanLII) at paras. 47-50.
\textsuperscript{391} Ibid.
it also allows for an individual to be identified from amongst the broader population, alone or in combination with other available information.392

Though the Federal Court has held that codes associated to individuals might, according to Canada’s Access to Information Act, be considered inherently identifying information, this does not mean that coded information should be considered identifiable personal information. The Act, and the Court’s interpretation thereof, consider codes associated to an individual for long-term identification purposes, such as driver’s license numbers or a social insurance number, to be personal information.393 Codes used to replace identifiers for the purposes of performing individual de-identification do not necessarily render the associated information identifiable personal information.394

Considerations relative to individuals who could perform re-identification based on pre-existing knowledge

In performing the de-identification of information for the purposes of rendering it anonymized, it is important to consider whether the anonymous identifiers retained allow the individuals using the information to perform the re-identification of the concerned individuals.395

It is therefore critical to use a method of generating codes that does not allow for parties having access to the information to ascertain the identities of the persons to whom the information relates. More crucially, this also suggests that if an institution responsible for performing the de-identification of information continues to use such information for further purposes, the following additional verification is required. It will be required for the institution to ensure that it or its staff is not capable of performing the re-identification of the concerned individuals on the basis of knowledge arising prior to information anonymization being performed. This can be

392 In Public Safety, the Federal Court considered that information related to firearm serial numbers was related to an object, rather than to an identifiable natural person See: Canada (Information Commissioner) v Canada (Public Safety and Emergency Preparedness), 2019 FC 1279 (CanLII) at paras. 43-48, 80.

393 Ibid at para 47.

394 Ibid at paras 2-3. The Federal Court further confirmed that the linkage of a code or of information to an identifiable individual in a government database does not cause that code or information to be considered identifiable if the information or the code is released to third parties or to the public absent such linkage. It therefore stands to reason that information that is coded in the hands of an information custodian will not be considered identifiable in the hands of third parties, even if the custodian holds the linkage log or re-identification key required to perform the re-identification of the individual that the information concerns. This position is correct in law. However, it must be noted that health-care institutions and biomedical research communities have not harmoniously adopted this position, and that there is no consensus endorsement of this position in the policy statements of Canadian data protection authorities and government agencies. If data protection authorities or health-sector government bodies issued guidance documents that confirm this position, this could help build consensus among the Canadian healthcare and biomedical research communities, leading to the rapid adoption of this legal position and of concordant data governance practices.

395 In University of Alberta, the Alberta Court of Appeal concluded that it was not unreasonable for the Information and Privacy Commissioner to conclude that summary-level records about the job performance of multiple professors, including the applicant, were identifiable personal information in the context of their use. The University had made available a list of information about its professors in a de-identified format, including information about their performance. The list contained first a numerical record of the number of papers accepted for publication during the reporting period, and second a numerical record of the number of papers accepted and published during the reporting period. Third, the list also established that the applicant was one of only two professors to receive a double merit increment for his work. The information in the record was considered to be personal information, because those in possession of the record could infer the identities of the professors concerned through their own outside knowledge of the professors’ academic performance and their number of publications. See: University of Alberta v Alberta (Information & Privacy Commissioner), 2009 ABQB 112.
achieved in ensuring that staff members that are responsible for performing record de-
identification are not afterwards involved in the ongoing data analysis or data management
activities that involve the resulting, anonymized information.

The role of governance conditions in determining if information is anonymized

Case law, Privacy Commissioner investigation reports, and regulatory guidance have considered
the relationship between the governance conditions imposed on information and its identifiable
or anonymized nature. Information identifiability is determined by considering the
characteristics of the concerned information and the nature of other “available information.”
The methods of information governance used to safeguard information are therefore relevant to
assess what other information is available for such a purpose.

Further, the methods of information governance used to safeguard information can also be
relevant to determine whether or not a “serious possibility” of individual re-identification
exists. As previously stated, government information held confidential is generally not
considered to be ‘available’ for the purposes of determining if information is identifiable, for
example. The purpose for which information is used is also material to determining if
information is personal information, in that its use to affect the interests of individuals to which
the information is related tends to favor the qualification of information as identifiable personal
information.

Elements of information governance that are relevant to characterising information as personal or
non-personal in nature include whether the information is subject to public release, semi-public
release, or to restricted or controlled access policies. The risk of deliberate re-identification
being performed is also a factor, considering the incentives to attempt individual re-
identification, the likelihood of success of attempt, and the number of persons that are in a
position to attempt re-identification. The risk of individual re-identification is assessed relative
to known persons, circumstances, and sources of information that could cause such re-
identification, rather than the hypothetical and unsubstantiated risk of future re-identification.

397 Gordon v Canada (Minister of Health), supra n. 24 at para. 34.
399 Canada (Information Commissioner) v Canada (Public Safety and Emergency Preparedness), 2019 FC 1279 (CanLII) at
paras 55-68.
400 Ibid at paras. 59-60.
402 Ontario IPC, supra n. 26 at p. 13.
403 Ibid at pp. 15-17.
404 Carleton University, Re 2013 CarswellOnt 19131 at paras. 36-39. Ontario (Ministry of Health), Re, 1997 CarswellOnt 7611 at
para. 17.
APPENDIX H: Opportunities From Virus Genomic Data: Summary

Contributed by: C. Colijn, A. Poon

Introduction: Classifying SARS-CoV-2 infections into known variants (variant counting) is not always enough. New variants can emerge anywhere, and we need to be in a position to detect emerging variants of public health significance in Canada. SARS-CoV-2 whole genome sequences are fundamental to this task, which requires not only sequence data but information about transmissibility, severity and immune escape. Here we summarize what can be learned from virus sequence data and the increased opportunities if additional data were made available.

Viral sequences and sample dates:

1. Identify unusual new variants, bursts of mutations, genetic changes predicted to affect transmission or immune escape, or “mutator” lineages that evolve faster than expected. These could be potential sources of further VOI and VOC.

2. Infer the geographic movements of viruses,

3. Estimate the population dynamics and effective reproduction number over time

4. Detect rapid growth in the number of published sequences of particular virus types and variants.

2-4 are subject to potentially severe bias. Without knowing the sampling (reason for sequencing) strategy, increased growth due to viral characteristics cannot reliably be separated from other possible explanations (e.g. changing contact patterns in specific settings or groups, travel-associated introductions, or sampling artefacts.

---


Virus sequences and epidemiological data
1. Links to travel history allow improved identification of importation events.\(^{409}\)
2. Distinguish an emerging virus with increased transmissibility from founder and sampling effects.
3. Identify factors driving transmission across geographic regions.\(^{410}\)
4. Complement contact tracing to better understand person-to-person transmission in outbreaks, identify missing links and refine epidemiological knowledge of cluster origins (Seemann et al., 2020). This can be actionable immediately.
5. Detect genetic changes in the virus that lead to increased transmissibility or increased ability to transmit in certain settings.

Virus sequences and clinical/demographic information
1. Determine whether an emerging type causes more severe disease.\(^{412}\)
2. Determine if the risk of severe disease with a subtype is elevated in particular groups, or by specific risk factors.

Virus sequences and immunization information
1. Determine rapidly whether there is reduced vaccine efficacy against infection for an emerging virus type.\(^{413}\)
2. Determine to what extent virus subtypes cause breakthrough infections that are readily transmissible among vaccinated individuals. Epidemiological data would help to refine estimates of relative transmissibility.\(^{414}\)


Conclusions:

An emerging variant that can infect immunized individuals and transmit readily among them, and especially if it can cause severe disease among immunized individuals, would be of public health concern. Detecting whether these properties are emerging is challenging, in part because transmission inherently is a group-level phenomenon, and because a minority of COVID-19 infections cause severe disease. Furthermore, at the time of emergence, a new variant will necessarily occur in small numbers. These factors highlight the need to link multiple data sources together and to pool data across jurisdictions, in order to have the strongest possible statistical signal and the widest possible lens on the virus’ evolving phenotype.
REFERENCES

ACADEMIC LITERATURE, POLICY REPORTS, AND REGULATORY GUIDANCE


49. Ling, J., “Canada’s public health data meltdown,” (7 April 2021), online: Macleans.ca.


63. Office of the Privacy Commissioner of Canada “Provincial laws that may apply instead of PIPEDA” (2020).


69. Research and Health System Innovation “Accessing Health and Health-Related Data in Canada” (2015).


Centre of Genomics and Policy


82. Thorogood, A. “Towards Legal Interoperability in International Health Research” University of Toronto, Faculty of Law, LLM Thesis (2019).


CASES AND INVESTIGATION REPORTS


2. Board of Education of School District No. 75 (Re), 2007 CanLII 30395 (BC IPC)

3. Canada (Syndicat des agents correctionnels) c. Canada (Procureur général) 2019 FCA 212, 309 A.C.W.S. (3d) 78 at paras. 8, 42-44.

4. Canada (Information Commissioner) v Canada (Public Safety and Emergency Preparedness), 2019 FC 1279 (CanLII).


7. Carleton University, Re 2013 CarswellOnt 19131 at paras. 36-39. Ontario (Ministry of Health), Re, 1997 CarswellOnt 7611.


9. Dagg v Canada (Minister of Finance) [1997] 2 SCR 403 at para 69
Centre of Genomics and Policy


11. *Gordon v Canada (Minister of Health)* 2008 FC 258 at para 34


20. Office of the Privacy Commissioner of Canada. PIPEDA Case Summary #2009-018. Psychologist’s anonymized peer review notes are the personal information of the patient.


Centre of Genomics and Policy


**LEGISLATION**

1. *Act Respecting Health Services and Social Services*, R.S.Q., Chapter S-4.2.

2. *Act Respecting the Right of Access to Documents of Public Bodies in Nova Scotia and a Right of Privacy with Respect to Personal Information Held by Public Bodies in Nova Scotia*, S.N.S. 1993, c. 5.


5. *Act respecting the protection of personal information in the private sector* R.S.Q., Chapter P-39.1.


23. Health Information Act, S.N.W.T. 2014, c.2
24. Health Information Privacy and Management Act, S.Y. 2013 c. 16.
32. Personal Health Information Protection Act, S.O. 2004, c. 3, Sched. A.
33. Personal Health Information Privacy and Access Act, S.N.B. 2009, c. P-7.05.
34. Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, Schedule I.
35. Personal Health Information Act, C.C.S.M. c. P33.5.
38. Public Health Act, C.Q.L.R., Chapter S-2.2.


