



Pandemics, privacy, and public health research

Alexander Bernier¹ · Bartha Maria Knoppers¹

Received: 8 April 2020 / Accepted: 8 June 2020 / Published online: 26 June 2020
© The Author(s) 2020

Abstract

Sharing data expediently for pandemic response purposes exposes healthcare providers in Canada to significant regulatory uncertainty. Duplicative and contradictory ethical and legal duties flowing from overlapping sources can stifle flows of medical data among clinicians, researchers, and institutions. Authorities should support caregivers and accelerate research by providing clear guidance to the health sector. Institutions should foster robust data stewardship and standardize their practices to those recognized among the international health informatics community. Reform is critical to ensuring Canadian healthcare providers can deliver efficient health responses that are integrated with dispersed and disparate national and international approaches.

Résumé

Les chercheurs et cliniciens canadiens désirant tenter le partage rapide des données médicales dans le cadre d'une mobilisation contre la pandémie se retrouvent assujettis à un régime juridique incertain. Les obligations qui leur sont imposées par l'éthique tant que par le droit peuvent s'avérer complexes et contradictoires, en raison du chevauchement de plusieurs politiques, règlements et lois. Il est impératif que les autorités se prononcent afin d'éclaircir les démarches que doivent entreprendre les fournisseurs de soins de santé en partageant les données médicales. Les institutions, quant à elles, devraient concilier leurs pratiques de gouvernance des données à celles employées à l'échelle mondiale par les organismes internationaux œuvrant dans le domaine de la santé. Une solution durable permettant le partage pancanadien et international des données de santé nécessitera désormais la refonte de la législation sibylline actuellement en vigueur.

Keywords COVID-19 · Data sharing · Health policy · Health governance · Pandemic · Privacy

Mots-clés COVID-19 · Partage des données · politique de santé · gouvernance de la santé · pandémie · vie privée

Introduction

Worldwide, the COVID-19 pandemic is inspiring clinicians and researchers to pool data and design data repositories for long-term public health research. Ensuring compliance with Canadian privacy regulations creates significant challenges for such efforts. Coordinated and collaborative data stewardship strategies are needed.

Challenges for collaboration

First, Canada's privacy laws are non-harmonized for different categories of entities. Private sector, public sector, and health sector entities can find themselves subject to a labyrinthine variety of obligations across their public and private functions. For a pandemic response, this can mean that private-sector clinicians attempting to share data with larger institutional actors such as hospitals and universities will face challenges in ensuring that the privacy law obligations imposed on the clinic and those imposed on the hospital are compatible (Power 2017).

Second, Canada's private sector privacy laws differ considerably from one province to the next, and the applicable law varies depending on whether data are used within a province's borders or interprovincially. In the case of internal use, the local provincial laws will apply unless the province has not enacted such laws, in which case Canada's federal *Personal*

✉ Alexander Bernier
alexander.bernier@mail.mcgill.ca

¹ Centre of Genomics and Policy, Faculty of Medicine, McGill University, 740, Avenue Dr. Penfield, Suite 5200, Montreal, Quebec H3A 0G1, Canada

Information Protection and Electronic Documents Act (PIPEDA) applies instead. Regarding interprovincial use, PIPEDA will generally apply. In some provinces such as Quebec, provincial and federal authorities disagree as to whether the local provincial law, the federal PIPEDA, or both are applicable to interprovincial data transfers (Power 2017).

Third, certain provinces have strict requirements governing the interprovincial or international use of patient and research participant data. These limits differ from province to province but can operate to restrain clinicians and researchers from hosting or transferring data extra-provincially (Power 2017).

Challenges for public health and research

For research purposes, Canada's ethics guidance and laws generally recognize broad consent with appropriate governance (Canada Tri-Council 2018). However, certain provincial laws, such as Alberta's *Health Information Act* (HIA), impose special requirements on the contents of consent forms that could create difficulties in standardizing pan-Canadian consent materials across the clinical and research settings (Inions et al. 2018). Other provinces impose prohibitive formal requirements on the contents of data transfer agreements and research plans (Dove and Phillips 2015).

Healthcare practitioners face more onerous requirements in obtaining research consent than clinical consent. Research consent must be clearly distinguished from clinical consent (Canada Tri-Council 2018). These requirements could be difficult to discharge systematically due to the high volume of patient inflows experienced during a pandemic, which impose considerable strain on the resources of healthcare institutions.

Canada's privacy laws create special powers for national public health authorities to requisition and share data liberally across healthcare actors and across provincial borders during a public health emergency without obtaining individual consent (Office of the Privacy Commissioner of Canada [OPC] 2020). However, the permitted purposes of data collection, use, and disclosure in such circumstances are limited to the requirements of emergency response. If clinicians and researchers wish to reuse the data generated for future epidemiological and healthcare research, they may be required to satisfy the more onerous burden of obtaining either individual participant consent or research ethics waivers of consent, coupled with institutional custodians' approvals, as well as the necessary, project-specific research ethics approvals (Dove and Phillips 2015; Council of Canadian Academies 2015). This requires them to consider the compatibility of the legal requirements applicable to researchers in each sector (private, public, health) and arising in each applicable provincial and federal law (Power 2017). This could force clinicians and researchers to decide between the immediate pooling of data for a robust emergency response, and the slower pooling of data to secure its future availability to researchers.

Responsive and responsible data stewardship

Faced with ethical and regulatory barriers to efficient data pooling, we impel clinicians and researchers to turn to the governmental actors most capable of orchestrating a coordinated, data-driven response to a health crisis. Ministers and national public health authorities are imbued with exceptional powers to facilitate the transfer and reuse of data for a wide range of purposes. Furthermore, some Canadian privacy laws allow the broad transfer of health data to combat a health risk to known persons, or to provide healthcare to the person that the data concerns (Canada Tri-Council 2018). Privacy Commissioners and other bodies responsible for enforcing privacy laws have expressed willingness to cooperate and facilitate an efficient crisis response (OPC 2020). Healthcare practitioners should consider these options in opening immediate channels for data sharing.

For a coordinated long-term response to epidemic threats, including COVID-19, Canadian researchers should coordinate their data collection and data governance practices with those of established international consortia to facilitate efficient data deposit (Council of Canadian Academies 2015). Institutional research ethics committees, in coordination with institution heads, can agree to a singular multi-site ethics review of an international or international research project to increase efficiency and ensure the consistency of collection and storage practices across research sites (Canada Tri-Council 2018; Council of Canadian Academies 2015). Institutions can manage their data releases using Data Access Committees (DACs) and Data Access Compliance Offices (DACOs), teams of multidisciplinary scientific members and ethico-legal specialists, to ensure the compliance of each data release to ethics, law, and local policies (Joly et al. 2012). Data can be made anonymous using statistical or algorithmic deidentification methods or appropriate aggregation methods and circulated openly, but anonymized data often retain only negligible scientific utility (Langarizadeh et al. 2018).

The COVID-19 pandemic has lain bare the fault lines in Canada's health data regulation. Fundamental reforms will be necessary to enable efficient responses to future health emergencies and to ensure that Canadian healthcare providers are not unduly precluded from granting Canadians high-quality medical care as data-driven approaches continue to reshape the health sector (Beauvais and Knoppers 2020).

Proposed regulatory reforms

The use of localized, divergent rules to govern data processing activities in Canada and other jurisdictions, including the European Union, has attenuated international research collaboration for fear of legal non-compliance (Peloquin et al. 2020). Health data custodians in Canada have favoured the

creation of data repositories that are provincial or purpose-specific rather than multipurpose or pan-Canadian, due to the complexities inherent in ensuring holistic privacy law compliance (Council of Canadian Academies 2015).

Healthcare entities would benefit from the streamlining of regulatory obligations across sectoral and territorial boundaries. Requirements to restrict data reuse to the initial purposes of collection, or to retain data within prescribed territorial boundaries, are difficult to reconcile with the international nature of a collaborative pandemic response, and the potential to use data for flexible secondary purposes (Council of Canadian Academies 2015).

Government and industry stakeholders, as well as academic commentators, have recognized that procedural mechanisms for regulating privacy are difficult to reconcile with continuous technological disruption and innovation in the digital age; technology-neutral, principle-driven protections are more adaptable to the ever-shifting context of data use than are formalistic rules (Department of Justice 2019). Canada's Department of Industry, Canada's Department of Justice, and the OPC have made recent proposals for reform. The establishment of data trusts, banks of data that are created for broad reuse for approved purposes, is proposed. Also propounded are exceptions to the requirement to obtain consent to collect, use, or disclose data for purposes in the public interest or arising in the ordinary course of business. Streamlining enforcement procedures across provincial and sectoral boundaries is also suggested. Increased audit and enforcement powers for regulators are endorsed, and heightened individual rights to control, transfer, and erase data are advocated for individuals. In sum, the recommendations favour decreased procedural burdens for data use generally, counterbalanced by increased substantive protections for individuals against unconscionable uses of their data (Department of Justice 2019; Innovation, Science, and Economic Development Canada 2019; OPC 2019). We propose regulatory approaches to actualize these policy objectives.

Harmonizing data stewardship and regulatory oversight

First, the regulatory regime applicable to health research consortia should be harmonized across national and sectoral boundaries, whether by legislation or through the standardization of enforcement practices by Privacy Commissioners (OPC 2019). Uniform privacy laws across Canadian provinces can foster increased predictability and public trust, as privacy obligations will be consistent across all public institutions. Canadians are thus assured that their data are subject to the same protections irrespective of the institution responsible for their safekeeping. Furthermore, the synchronization of privacy regimes allows for the central administration of health

data. Central data management prevents the replication of collection and storage processes for the same data across multiple repositories. To implement such a method without derogating from the shared federal and provincial oversight of health data, privacy regulators can subject government-created data repositories to delegated oversight performed by a designated Privacy Commissioner in accordance with a commonly chosen privacy law, irrespective of the provenance of the data stored in the repository. In research ethics oversight, such imperatives have prompted the adoption of delegated review models, wherein one research ethics board performs ethics review of a research project across multiple sites (Zawati et al. 2015). An equitable pandemic response will benefit from consistent regulation and coordinated oversight.

Second, blanket doctrines of purpose limitation and temporal limits to the use and storage of data should be disfavoured. Instead, individuals should be granted fundamental rights in their data, drawing from human rights legislation such as the *Charter of Rights and Freedoms*. Such rights must be supported by broad audit and enforcement powers apportioned to Privacy Commissioners, directly actionable rights in data for patients and research participants, and obligations for data custodians to demonstrate that privacy has been accounted for in organizational structure and technological design (OPC 2019). In empowering individuals and Privacy Commissioners to hold entities accountable for their uses of health data, legislators can ensure that the interests of vulnerable groups are not disregarded, as they might be in the present model that relies principally on self-regulation. A rights framing enables the explicit balancing of individual, community, and public interests in data. Justly balancing such interests during a pandemic is best achieved if consideration thereof is enshrined in the law.

Furthermore, health data are a limited resource that must be used responsibly, and not destroyed callously. Whereas it is sensible to establish maximum retention periods for personal data collected in transactional contexts, health data represent a finite resource, the collection of which can often subject individuals to hardship and sacrifice (Canada Tri-Council 2018). Using destruction obligations and preclusions on data reuse to safeguard health data can further stigmatize marginalized populations, and deny vulnerable individuals access to research benefits (Canada Tri-Council 2018). Leveraging longitudinal data from past epidemics can reduce the need for primary data collection, protecting individuals from potential health risks incurred in research participation.

Third, data localization requirements mandating data to be retained in its territory of provenance, and formal obligations that consent or compliance documentation be structured using a predetermined format, should be replaced with a more holistic obligation to ensure that data are held to an equivalent standard of protection across jurisdictions, as some Canadian provinces already do (Inions et al. 2018; Power 2017). This

encourages health data custodians to hold downstream recipients of data accountable using contractual agreements and data audit provisions tailored to the risks inherent in the specific data uses anticipated (e.g., cloud storage, algorithmic processing). Furthermore, it prevents inconsistencies in formal compliance obligations across jurisdictions from precluding otherwise responsible data transfers. Mobilizing accurate, voluminous, and compatibly formatted data across borders is a prerequisite to a public health response that ensures equitable access to scientific knowledge for all communities.

Lessons for the future

Challenges faced in sharing health data to respond to the COVID-19 epidemic demonstrate how Canada's duplicative privacy legislation can create considerable barriers for health data sharing in Canada with minimal gains in personal privacy. The failure to standardize Canada's health data regime imposes considerable institutional costs and legal risks on the healthcare sector and causes clinicians and researchers to eschew data centralization and secondary data use (El Emam et al. 2011). Reform is the only viable solution for the future, and the future is now!

Funding information This work was supported by One4ALL: "Sharing Big Data for Health Innovation Advancing the Objectives of the Global Alliance for Genomics and Health (GA4GH) Regulatory and Ethics Work Stream" Genome Canada/CIHR (2019–2022).

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Beauvais, M., & Knoppers, B. M. (2020). COVID-19: who's afraid of data sharing? Canadian Science Policy Centre. Retrieved from: <https://sciencepolicy.ca/news/covid-19-whos-afraid-data-sharing>.
- Bjerring, A. K., Brownell, M., El Emam, K., Fortier, I., Henry, D., Knoppers, B. M., Laurie, G., Lemmens, T., Morgan, M., Noseworthy, T. W., Saunders, S., Wolfson, M., & Zelmer, J. (Council of Canadian Academies). (2015). *Accessing health and health-related data in Canada: The expert panel on timely access to health and social data for health research and health system innovation*. Council of Canadian Academies.
- Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council (Canada Tri-Council). (2018). *Tri-Council policy statement 2*. Canada: Government of Canada.
- Department of Justice. (2019). Modernizing Canada's privacy act: stakeholder engagement discussion papers 1–5. Government of Canada.
- Dove, E. S., & Phillips, M. (2015). Privacy law, data sharing policies, and medical data: a comparative perspective. In A. Gkoulalas-Divanis & G. Loukides (Eds.), *Medical data privacy handbook* (pp. 639–678). Springer Link: Switzerland.
- El Emam, K., Mercer, J., Moreau, K., Grava-Gubing, I., Buckridge, D., & Joncker, E. (2011). Physician privacy concerns when disclosing patient data for public health purposes during a pandemic influenza outbreak. *BMC Public Health*, 11, 454. <https://doi.org/10.1186/1471-2458-11-454>. Retrieved from: <https://bmcpublihealth.biomedcentral.com/articles/10.1186/1471-2458-11-454>.
- Inions, N. J., Tran, L. E., & Rozovsky, L. E. (2018). *Canadian health information: A practical legal and risk management guide, fourth edition*. Toronto: LexisNexis Canada Ltd., 347 p.
- Innovation, Science, and Economic Development Canada (Department of Industry). (2019). Strengthening privacy for the digital age: proposals to modernize the Personal Information Protection and Electronic Documents Act.
- Joly, Y., Dove, E. S., Knoppers, B. M., Bobrow, M., & Chalmers, D. (2012). Data sharing in the post-genomic world: The experience of the International Cancer Genome Consortium (ICGC) Data Access Compliance Office (DACO). *PLoS Computational Biology*, 8(7). <https://doi.org/10.1371/journal.pcbi.1002549>. Retrieved from: <https://www.ncbi.nlm.nih.gov/pubmed/22807659>.
- Langarizadeh M, Orooji A, Sheikhtaheri A, & Hayn D. (2018). Effectiveness of anonymization methods in preserving patients' privacy: a systematic literature review. In Schreier G. & Hayn D., (Eds.) *Health Informatics Meets eHealth*. 248 Studies in Health Technology and Informatics 80–87. <https://doi.org/10.3233/978-1-61499-858-7-8>. Retrieved from: <http://ebooks.iospress.nl/publication/48967>.
- Office of the Privacy Commissioner of Canada. (2019). 2018–2019 Annual report to parliament on the privacy act and the personal information protection and electronic documents act. Gatineau, Quebec.
- Office of the Privacy Commissioner of Canada. (2020). *Privacy and the COVID-19 Outbreak*. Government of Canada. Retrieved from: https://priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/gd_covid_202003/.
- Peloquin, D., Dimaio, M., Bierer, B., & Barnes, M. (2020). Disruptive and avoidable: GDPR challenges to secondary research uses of data. *Eur J Hum Genet*. <https://doi.org/10.1038/s41431-020-0596-x>.
- Power, M. (2017). *The law of privacy, second edition*. Markham: LexisNexis Canada Inc..
- Zawati, M. H., Junker, A., Knoppers, B. M., & Rahimzadeh, V. (2015). Streamlining review of research involving humans: Canadian models: Table 1. *J Med Genet*, 52(8), 566–569. <https://doi.org/10.1136/jmedgenet-2014-102640>.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.