PRIVACY CONCERNS WITH COMMERCIAL ARTIFICIAL INTELLIGENCE FOR HEALTHCARE

Report Funded by the Office of the Privacy Commissioner of Canada

Blake Murdoch, Allison Jandura & Timothy Caulfield
Health Law Institute, Faculty of Law, University of Alberta
March 2021

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Artificial intelligence (AI) are increasingly being developed and implemented in healthcare. This presents privacy issues since many AI are privately owned and rely on public-private partnerships and data sharing arrangements for mass quantities of patient health information. We investigated the Canadian legal and policy framework focusing on two issues: first, the potential for inappropriate treatment, use or disclosure of personal health information by private AI companies, and second, the potential for privacy breaches that use newly developed AI methods to reidentify patient health information. We analyzed Canadian legislation, focusing on the federal *Personal Information Protection and Electronic Documents Act,* as well as applicable common law relating to torts and fiduciary obligation and key Canadian research ethics policy, namely the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans.* Our key findings and recommendations are summarized below.

Findings and Recommendations

- The scope of data made accessible to private AI companies should be firstly based on respect of patients' informed consent and rights of ongoing control over their private information, and after that, proportional to the likelihood and meaningfulness of the potential benefits the AI can provide.
- Patients have a general right to informed consent for the use and disclosure of their personal health information, and have an ongoing control interest which necessitates the need for recontact for any new uses or disclosures. Public-private partnerships implementing healthcare AI should prioritize the ability to recontact patients.
- Patients have a general right of withdrawal from participation in healthcare AI. AI companies will need to plan for the contingencies associated with data removal after its integration.
- Altering regulation to place more custodianship responsibility onto domestic third parties that are transferred patient heath information

would help contribute to the safe future implementation of healthcare AI.

- Greater cooperation between provinces to generate more consistency in the regulation that applies to commercial AI companies could help their implementation and to encourage compliance.
- Penalties levied against AI companies for breach of privacy requirements should in our view not be fixed or limited in any way that could fail to deter malfeasance.
- The concept of "non-identifiable information" is increasingly questionable or even dubious. The subsection of health information that could arguably meet this standard is decreasing quickly over time. Regulators and policymakers must incorporate into their work the reality that technical methods of breaching privacy through reidentification are quickly improving.
- Access to patient data must be predicated upon maintaining highly advanced forms of data security, and anonymization where possible. Strong privacy protection will be required in light of advancing technology that allows data to be re-identified and misused. Data security should minimize risks during data transfer, safe storage, and appropriate deletion. Further, consent requirements should disclose both any possible personal data transfers to commercial entities, and the realistic risk of privacy breach.
- The issue of data security is shared among both institutions that grant access to patient data for AI companies to utilize, and the AI companies manipulating and/or storing patient data themselves. Responsibility for security must be shared and integration must be extensive.
- Enforcement of very high standards for data protection will be key. Governments should consider creating interdisciplinary task forces focused specifically on creating, refining and implementing technical standards for protecting patient health information.

INTRODUCTION

THE RISE OF HEALTHCARE ARTIFICIAL INTELLIGENCE

There is a growing public discussion about the risks and benefits of artificial intelligence (AI) and how to manage its development.[1] Machine learning is a branch of AI that involves training an algorithm to execute a task by recognizing patterns from large datasets.[2]

Advances in healthcare artificial intelligence are occurring rapidly and will soon have a significant impact on patient care. AI may be used in a variety of healthcare contexts that each raise distinct ethical considerations, including process optimization, pre-clinical research, and selection of clinical pathways. And it will likely be used in both patient-facing applications and population level applications.[2] Several new AI technologies are approaching feasibility and a few are close to being integrated into healthcare systems.[3,4] In radiology, AI is proving to be useful for the analysis of diagnostic imagery.[5,6] For example, researchers at Stanford have produced an algorithm that can interpret chest X-rays for 14 distinct pathologies in just a few seconds.[7] Radiation oncology, organ allocation, robotic surgery and several other

---

[1] Hamid, S. (2016). The Opportunities and Risks of Artificial Intelligence in Medicine and Healthcare. *CUSPE Communications* https://doi.org/10.17863/CAM.25624.
[2] Smith MJ, Bean S. AI and Ethics in Medical Radiation Sciences. Journal of medical imaging and radiation sciences. 2019 Dec;50(4 Suppl 2):S24-6.
[3] Jiang F, Jiang Y, Zhi H, Dong Y, Li H, Ma S, Wang Y, Dong Q, Shen H, Wang Y. Artificial intelligence in healthcare: past, present and future. Stroke and vascular neurology. 2017 Dec 1;2(4):230-43.
[4] Johnson KW, Soto JT, Glicksberg BS, Shameer K, Miotto R, Ali M, Ashley E, Dudley JT. Artificial intelligence in cardiology. Journal of the American College of Cardiology. 2018 Jun 4;71(23):2668-79.
[5] Radiological Society of North America. Artificial Intelligence Shows Potential for Triaging Chest X-rays. 2019 Jan 22. https://www.rsna.org/en/news/2019/January/AI-for-chest-x-rays. Accessed 2019 Dec 16.
[6] European Society of Cardiology. Machine learning overtakes humans in predicting death or heart attack. EurekAlert! 2019 May 12. https://eurekalert.org/pub_releases/2019-05/esoc-mlo050719.php. Accessed 2019 Dec 16.
[7] Armitage H. Artificial intelligence rivals radiologists in screening X-rays for certain diseases. Stanford Medicine News Center. 2018 Nov 20. https://med.stanford.edu/news/all-news/2018/11/ai-outperformed-radiologists-in-screening-x-rays-for-certain-diseases.html. Accessed 2019 Dec 16.

healthcare domains also stand to be significantly impacted by AI technologies in the short to medium term.[8,9,10,11,12] In the United States, the Food and Drug Administration [FDA] recently approved one of the first applications of machine learning in clinical care – software to detect diabetic retinopathy from diagnostic imagery.[13,14]

AI have several unique characteristics compared with traditional health technologies. Notably, they can be prone to certain types of errors and biases,[15,16,17,18] and often cannot easily or even feasibly be supervised by human medical professionals. The latter is because of the "black box" problem, whereby learning algorithms' methods and 'reasoning' used for reaching their conclusions are partially or entirely opaque to human observers.[11,16] This opacity may also apply to how health and personal information is used and manipulated if appropriate

---

[8] Thompson RF, Valdes G, Fuller CD, Carpenter CM, Morin O, Aneja S, Lindsay WD, Aerts HJ, Agrimson B, Deville Jr C, Rosenthal SA. Artificial intelligence in radiation oncology: a specialty-wide disruptive transformation? Radiotherapy and Oncology. 2018 Dec 1;129(3):421-6.
[9] Canadian Blood Services. Kidney Paired Donation (KPD) Program. 2019. https://profedu.blood.ca/en/organs-and-tissues/programs-and-services/kidney-paired-donation-kpd-program.
[10] Rabbani M, Kanevsky J, Kafi K, Chandelier F, Giles FJ. Role of artificial intelligence in the care of patients with nonsmall cell lung cancer. European journal of clinical investigation. 2018 Apr;48(4):e12901.
[11] O'Sullivan S, Nevejans N, Allen C, Blyth A, Leonard S, Pagallo U, Holzinger K, Holzinger A, Sajid MI, Ashrafian H. Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. The International Journal of Medical Robotics and Computer Assisted Surgery. 2019 Feb;15(1):e1968.
[12] Hashimoto DA, Rosman G, Rus D, Meireles OR. Artificial intelligence in surgery: promises and perils. Annals of surgery. 2018 Jul 1;268(1):70-6.
[13] Gershgorn D. The FDA just opened the door to let AI make medical decisions on its own. Quartz. 2018 Apr 13. https://qz.com/1251502/the-fda-just-opened-the-door-to-let-ai-make-medical-decisions-on-its-own/. Accessed 2019 Dec 17.
[14] FDA. FDA permits marketing of artificial intelligence-based device to detect certain diabetes-related eye problems. 2018 Apr 11. https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-artificial-intelligence-based-device-detect-certain-diabetes-related-eye. Accessed 2019 Dec 17.
[15] Dietterich T. Overfitting and undercomputing in machine learning. ACM computing surveys. 1995 Sep 1;27(3):326-7.
[16] Mukherjee S. A.I. Versus M.D. The New Yorker. Annals of Medicine, April 3, 2017 Issue. 2017 Mar 27. https://www.newyorker.com/magazine/2017/04/03/ai-versus-md. Accessed 2019 Dec 17.
[17] Cuttler M. Transforming health care: How artificial intelligence is reshaping the medical landscape. CBC News. 2019 Apr 26. https://www.cbc.ca/news/health/artificial-intelligence-health-care-1.5110892. Accessed 2019 Dec 17.
[18] Char DS, Shah NH, Magnus D. Implementing machine learning in health care—addressing ethical challenges. The New England journal of medicine. 2018 Mar 15;378(11):981.

safeguards are not in place. Therefore, the regulatory systems used for approval and ongoing oversight will often also need to be unique.

Health Canada is currently studying potential applications of AI and recently established a Digital Health Review Division to develop and implement a unique review process for these technologies.[19] As such, AI is a novel frontier in Canadian healthcare, and one currently without a comprehensive legal and regulatory framework.

The use of commercial AI in healthcare also raises significant privacy concerns. Privacy has been identified as a fundamental human right in the Universal Declaration of Human Rights at the 1948 United National General Assembly.[20] Privacy is an important ethical principle in healthcare because it flows from a patient's autonomy, personal identity and well-being.[21] Healthcare AI relates to informational privacy, that is to say to the use and control over one's personal information.[22] AI privacy issues arise both with respect to the entities collecting personal information and the threat of malicious cyberattacks.[23]

Privacy of personal health information broadly encompasses consent for uses, security measures and access. MJ Smith et al. identify potential privacy concerns associated with whether patients are aware of:

---

[19] Health Canada. Notice: Health Canada's Approach to Digital Health Technologies. 2018 Apr 10. https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/announcements/notice-digital-health-technologies.html. Accessed 2019 Dec 17.
[20] United Nations. Universal Declaration of Human Rights. 1948 Dec 10. https://www.un.org/en/about-us/universal-declaration-of-human-rights. Accessed 2021 Mar 23.
[21] Reddy S, Allan S, Coghlan S, Cooper P. A governance model for the application of AI in health care. J Am Med Inform Assoc. 2020;27(3):491-7 at 492. https://pubmed.ncbi.nlm.nih.gov/31682262/
[22] van den Hoven van Genderen, R. Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics. European Data Protection Law Review (EDPL). 2017;3(3):338-352 at 339. https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl3&div=62&id=&page=
[23] Pesapane F, Volonte C, Codari M, Sardanelli F. Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. Insights into Imaging. 2018;9(5):745-53 at 749. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6206380/

> "(1) the extent to which their data are undergoing secondary use; (2) which portions of their data are involved; (3) who can access their data; (4) the extent to which data anonymization is effective and complete; (5) whether data could potentially be used in a way that is harmful to them; (6) whether their data are being used for the financial benefit of others; and (7) whether a change in data privacy policies in the future will affect the care they will receive. The collection and use of a patient's data for these purposes also clearly implicates questions of informed consent."[2]

The purpose of this research was to investigate the application of the existing Canadian legal and research ethics frameworks to the issue of commercial healthcare AI implementation, in accordance with the research questions stated below.

QUESTIONS INVESTIGATED

COMMERCIAL INVOLVEMENT IN IMPLEMENTATION AND MAINTENANCE OF HEALTHCARE AI

A significant portion of existing technology relating to machine learning and neural networks rests in the hands of large tech corporations. Google, Microsoft, IBM, Apple and other companies are all "preparing, in their own ways, bids on the future of health and on various aspects of the global healthcare industry."[24] Information sharing agreements can be used to grant these private institutions access to patient health information. Health information, particularly identified or re-identified patient data, has considerable economic value to commercial entities for the purpose of AI deep learning.[25]

Some recent public-private partnerships for implementing machine learning have resulted in poor protection of privacy. For example, DeepMind, owned by Alphabet Inc. (hereinafter referred to as Google), partnered with the Royal Free London NHS Foundation Trust in 2016 to use machine learning to assist in the management of acute kidney injury.[24] Critics noted that patients were not afforded agency over the use of their information, nor were privacy impacts adequately discussed.[24] A senior advisor with England's Department of Health said the patient info was obtained on an "inappropriate legal basis".[26]

Further controversy arose after Google subsequently took direct control over DeepMind's app, effectively transferring control over stored patient data from the United Kingdom to the United States.[27]

---

[24] Powles J, Hodson H. Google DeepMind and healthcare in an age of algorithms. Health and technology. 2017 Dec 1;7(4):351-67. https://link.springer.com/article/10.1007/s12553-017-0179-1.
[25] Winter JS, Davidson E. Governance of artificial intelligence and personal health information. Digital Policy Regulation and Governance. 2019;21(3):280-90 at 285-286. https://www.emerald.com/insight/content/doi/10.1108/DPRG-08-2018-0048/full/html
[26] Iacobucci G. Patient data were shared with Google on an "inappropriate legal basis," says NHS data guardian. BMJ. 2017;357:j2439.
[27] Vincent J. Privacy advocates sound the alarm after Google grabs DeepMind UK health app. The Verge. 2018 Nov 14. https://www.theverge.com/2018/11/14/18094874/google-deepmind-health-app-privacy-concerns-uk-nhs-medical-data. Accessed 2019 Dec 17.

The ability to essentially "annex" mass quantities of private patient data to another jurisdiction is a new reality of big data and one at more risk of occurring when implementing commercial healthcare AI. The concentration of technological innovation and knowledge in big tech companies could create power imbalances where public institutions could become more dependent and less equal partners in health tech implementation.

While some of these violations of patient privacy may have occurred in spite of existing privacy laws, regulations and policies, it is clear from the DeepMind example that appropriate safeguards must be in place to maintain privacy and patient agency in the context of these public-private partnerships. Beyond the possibility for general abuses of power, AI poses a novel challenge because the algorithms often require access to large quantities of patient data and may use the data in different ways over time.[28] The location and ownership of servers and computers that store and access patient health information for healthcare AI to use are important in these scenarios. Regulation could require that patient data remain in the jurisdiction from which it is obtained, with few exceptions. This would also help to more equitably distribute the economic and related social benefits of these technologies.

Strong privacy protection is realizable when institutions are structurally encouraged to cooperate to ensure data protection by their very designs.[29] For example, commercial healthcare AI platforms could be designed from the ground up for close integration with public health systems, and could build in transparency and feedback loops that allow regulators to ensure protocols are being followed. This is key because while it is possible to create public-private partnership where

[28] He J, Baxter SL, Xu J, Xu J, Zhou X, Zhang K. The practical implementation of artificial intelligence technologies in medicine. Nature medicine. 2019 Jan;25(1):30-6.
[29] Jaremko JL, Azar M, Bromwich R, Lum A, Cheong LA, Gibert M, et al. Canadian Association of Radiologists White Paper on Ethical and Legal Issues Related to Artificial Intelligence in Radiology. Canadian Association of Radiologists Journal-Journal De L Association Canadienne Des Radiologistes. 2019;70(2):107-18. https://pubmed.ncbi.nlm.nih.gov/30962048/

the protection of privacy is manageable, these partnerships can introduce competing goals. As we have seen, corporations may not be sufficiently encouraged to always maintain privacy protection if they can monetize the data or otherwise gain from them, especially if the legal penalties are not high enough to discourage this behaviour.[30] Because of these and other concerns, there have been calls for greater systemic oversight of big data health research and technology.[31]

Based on the above, the first research focus was on the potential for inappropriate treatment, use or disclosure of personal health information by private AI companies.

THE THREAT OF AI-DRIVEN DATA BREACHES AND REIDENTIFICATION OF PATIENT DATA

Another concern with big data use of commercial AI relates to the external risk of privacy breaches from highly sophisticated algorithmic systems themselves. Health information breaches are on the rise in Canada.[32,33,34] And while they may not be widely used by criminal hackers at this time, AI and other algorithms are contributing to a

[30] Federal Trade Commission. FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. 2019 Jul 24. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions. Accessed 2021 Mar 26.
[31] Vayena E, Blasimme A. Health research with big data: Time for systemic oversight. The journal of law, medicine & ethics. 2018 Mar;46(1):119-29. https://journals.sagepub.com/doi/abs/10.1177/1073110518766026.
[32] CBC News. LifeLabs pays ransom after cyberattack exposes information of 15 million customers in B.C. and Ontario. 2019 Dec 17. https://www.cbc.ca/news/canada/british-columbia/lifelabs-cyberattack-15-million-1.5399577. Accessed 2019 Dec 17.
[33] Hunter J. Privacy breach in B.C. health ministry led to freeze on medical research data. The Globe and Mail. 2016 Apr 26. https://www.theglobeandmail.com/news/british-columbia/privacy-breach-in-bc-health-ministry-led-to-freeze-on-medical-research-data/article29767108/. Accessed 2019 Dec 17.
[34] Solomon H. Cost of Canadian data breaches continues to rise, says study. IT World Canada. 2018 Jul 11. https://www.itworldcanada.com/article/cost-of-canadian-data-breaches-continues-to-rise-says-study/406976. Accessed 2019 Dec 17.

growing inability to protect health information.[35,36] A number of recent studies have highlighted how emerging computational strategies can be used to identify individuals in health data repositories managed by public or private institutions.[37] And this is true even if the information has been anonymized and scrubbed of all identifiers.[38] A study by Na et al., for example, found that an algorithm could be used to re-identify 85.6% of adults and 69.8% of children in a physical activity cohort study, "despite data aggregation and removal of protected health information."[39] A 2018 study concluded that data collected by ancestry companies could be used to identify approximately 60% of Americans of European ancestry and that, in the near future, the percentage is likely to increase substantially.[40] Furthermore, a 2019 study successfully used a "linkage attack framework" – that is, an algorithm aimed at re-identifying anonymous health information – that can link online health data to real world people, demonstrating "the vulnerability of existing online health data."[41]

And these are just a few examples of the developing approaches that have raised questions about the security of health information framed as being confidential. Indeed, it has been suggested that today's "techniques of re-identification effectively nullify scrubbing and

---

[35] University of California – Berkeley. Artificial intelligence advances threaten privacy of health data. EurekAlert! 2019 Jan 3. https://www.eurekalert.org/pub_releases/2019-01/uoc--aia010319.php. Accessed 2019 Dec 17.
[36] Kolata G. Your Data Were 'Anonymized'? These Scientists Can Still Identify You. New York Times. 2019 Jul 23. https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html.
[37] Hayden EC. Privacy loophole found in genetic databases. Nature News. 2013 Jan 17. https://www.nature.com/news/privacy-loophole-found-in-genetic-databases-1.12237. Accessed 2019 Oct 4.
[38] Z Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y. Identifying personal genomes by surname inference. Science. 2013 Jan 18;339(6117):321-4. https://science.sciencemag.org/content/339/6117/321.short.
[39] Na L, Yang C, Lo CC, Zhao F, Fukuoka Y, Aswani A. Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. JAMA network open. 2018 Dec 7;1(8):e186040-. https://jamanetwork.com/journals/jamasurgery/fullarticle/2719130.
[40] Erlich Y, Shor T, Pe'er I, Carmi S. Identity inference of genomic data using long-range familial searches. Science. 2018 Nov 9;362(6415):690-4. https://science.sciencemag.org/content/362/6415/690.short.
[41] Ji S, Gu Q, Weng H, Liu Q, Zhou P, He Q, Beyah R, Wang T. De-Health: All Your Online Health Information Are Belong to Us. arXiv preprint arXiv:1902.00717. 2019 Feb 2. https://arxiv.org/abs/1902.00717.

compromise privacy".[42] Relatedly, the Privacy Commissions of Canada and British Columbia found in February 2021 that Clearview AI, which had scraped billions of images of people from across the internet and marketed this database to law enforcement for commercial purposes relating to identification were in breach of privacy law.[43] This is an emerging area of concern that is highly applicable to the healthcare space.

This reality potentially increases the privacy risks of allowing private AI companies to control patient health information, even in circumstances where "anonymization" occurs. It also raises questions of liability, insurability and other practical issues that differ from instances where state institutions directly control patient data. Considering the variable and complex nature of the legal risk that those who develop and maintain private AI could take on when dealing with high quantities of patient data, carefully constructed contracts will need to be made delineating the rights and obligations of the parties involved, and allocation of contractual responsibility and risk for the various potential negative outcomes.

Based on the above, the second research focus was Potential for privacy breaches that use AI to reidentify patient health information.

[42] Lubarsky B. Re-Identification of "Anonymized Data". UCLA L. REV. 1701;1754(2010). https://georgetownlawtechreview.org/wp-content/uploads/2017/04/Lubarsky-1-GEO.-L.-TECH.-REV.-202.pdf.

[43] Crawford T. Canadian privacy commissioners find Clearview AI's scraping of images violated privacy. Vancouver Sun. 2021 Feb 3. https://vancouversun.com/news/canada-and-b-c-privacy-commissioners-finds-clearview-ais-scraping-of-images-violated-privacy. Accessed 2021 Mar 29.

RESEARCH METHODS

ANALYSIS OF LITERATURE

The first step of the research process was to locate and analyze academic literature relevant to the research focuses, for the purposes of both creating a literature review manuscript and providing context and content for the legal analysis and final report. Specifically, we performed searches using terms related to AI in healthcare, health information, and privacy on Google Scholar, Westlaw, CanLII, Heinonline, Web of Science, and Pubmed. From these searches we then performed iterative secondary and tertiary searches, including following references from sources to other relevant works. The findings of this research informed the Challenges section of this report.

ANALYSIS OF CANADIAN LAW

The second step of the research process was to undertake traditional legal scholarship to investigate the Canadian law relevant to the research focuses, and consider its application. Traditional legal scholarship includes the analysis of relevant legislation, case law (including historical precedent), policy and scholarly articles to discern relevant legal principles and rules that are applicable to the noted healthcare AI concerns. It allowed us to both ascertain the interaction of the law with the research focuses, and also highlight key parts of existing law and policy which led to our conclusions.

Using key search terms related to AI in healthcare, health information, and privacy, we performed searches on CanLII, Westlaw, Lexis Advance Quicklaw for relevant Canadian and international case law and legislation. From these search results, we identified additional cited and citing sources. We focused on case law and legislation from Canada, the United States, the United Kingdom, Australia, and Europe.

Findings

Legislation

Applicability concerns

There is a lack of true and complete standardization of privacy legislation in Canada, both inter and intra-provincially. AI companies will sometimes be required to comply with multiple overlapping pieces of legislation.

This is further complicated for international AI implementations involving jurisdictions like the European Union and the United States, where, for example, the General Data Protection Rule and/or the Health Insurance Portability and Accountability Act (respectively) could also need to be respected. While it is beyond the scope of this research to consider the application of extraterritorial regulation, these rules could have important implications for the use of commercial AI in healthcare that involves or requires data-sharing across borders.

In Canada, there is both federally and provincially enacted privacy legislation protecting personal information and personal health information held by private or public organizations. The *Personal Information Protection and Electronic Documents Act, SC 2000, c 5* [PIPEDA] is the key statute in this analysis, due to its applicability to federally and some provincially regulated private corporations who develop and implement AI technologies.

In addition, provincial health information protection legislation and, in some cases, provincial public sector privacy regulation are relevant for the public-private partnerships that implementation of these technologies will necessitate.

Notably, legislation which is deemed substantially similar to PIPEDA takes precedence over PIPEDA for the provincially regulated companies

and activities it covers. Certain classes of organizations and activities in provinces with substantially similar private sector privacy laws, including those functioning in Alberta, British Columbia and Quebec, are exempt from the provisions of PIPEDA. Otherwise, organizations or other persons may be required to comply with all applicable pieces of privacy legislation.[44] Some provinces' health protection legislation overrides other provincial privacy legislation with respect to health information, while others do not. Provinces with substantially similar health information privacy laws, including Ontario, New Brunswick, Newfoundland and Labrador and Nova Scotia, are exempt from PIPEDA with respect to health information in some cases. Other provinces also have health privacy laws, but they have not been declared substantially similar and thus do not necessarily override PIPEDA. As noted, this mean that AI companies will sometimes have to comply with multiple overlapping pieces of legislation.

In the context of commercial AI in healthcare, hospitals or public healthcare providers will be required to comply with all relevant privacy and health information protection legislation that is applicable to public institutions. Any commercial activities done by contractors or collaborators may be required to comply with applicable provincial legislation and PIPEDA. Moreover, any commercial activities that cross provincial borders must comply with PIPEDA, regardless of whether both provinces involved have legislation that has been deemed substantially similar. This illustrates the legal complexity of potential public-private partnerships for AI companies that utilize mass quantities of patient health information.

This regulatory system has given rise to a patchwork of varying laws, with significant operational overlap. The intent of this analysis is not to deal with the nuanced interactions between federal and provincial statutes in each individual province, but to note broadly applicable

[44] McIntyre, E. Health care professionals and the privacy rights of patients. Advocates' Quarterly. 2015;43(4):428-447 at 431.

rules that are of particular importance to private implementations of healthcare AI and the research focuses we delineated. While it is conceivable that a healthcare AI company would operate entirely within a single province, given the high likelihood of cross-province (or cross-border) transmission of patient health information for any effective and widely implemented healthcare AI system that has centralized server systems in one province, we can reasonably conclude that PIPEDA will apply in most cases. From a business planning perspective, it would be very unwise for a healthcare AI company to not be in compliance with PIPEDA for this reason. As such, PIPEDA is the most important legislation in this context and it is our focus.

Third party transfers

PIPEDA, unlike some provincial privacy legislation, does not apply to third party providers that receive information as part of a transfer.[45] A transfer to a third party, domestic or foreign, is considered a use and not a disclosure under PIPEDA.[46] A transfer must only be used for the purposes for which the information was initially collected – a common commercial example would be outsourced IT services. It is entirely possible and likely that health information needed for AI could be transferred in this way. As per Principle 4.1.3 of Schedule 1, the original organization in possession or custody of personal information is responsible for it, including where that information has been transferred to a third party, and is required to provide a comparable level of protection of the information through contractual obligations.[45] However, when information is transferred to foreign jurisdictions, it is subject to the laws of those jurisdictions. PIPEDA does not prohibit international transactions that involve the transfer of personal data. It

[45] Lambie D. Canadian Personal Data Protection Legislation and Electronic Health Records: Transfers of Personal Health Information in IT Outsourcing Agreements. Canadian Journal of Law and Technology. 2010;8:85 at 95-96.
[46] Office of the Privacy Commissioner of Canada. Processing Personal Data Across Borders: Guidelines. 2009. https://www.priv.gc.ca/media/1992/gl_dab_090127_e.pdf. Accessed 2021 Mar 24.

is up to the discretion of individual organizations whether personal information is too sensitive or a risk of disclosure is too great to enter into a given agreement.

It is easy to see how third parties to commercial AI companies, whether domestic or foreign, having only contractual obligations to protect data rather than legislative ones could lead to increased likelihood of abuse and inappropriate disclosure of patient health information. Given that contractual obligations can be breached with only financial loss, it could lead private companies to engage in a form of ruthless economic calculation to justify unapproved use of health information. Especially for domestic third parties over which governments have clear jurisdiction, we should not allow third parties to fail to protect health information whenever it is economically beneficial to do so. As such, altering regulation to place more custodianship responsibility onto domestic third parties in control of patient heath information would help contribute to the safe future implementation of healthcare AI.

In an international context, given the likely legislative intent not to gravely hamstring companies' ability to engage in cross-border commerce, it may be difficult to make changes to this system without directly hampering the ability to move private data internationally. However, PIPEDA was not necessarily created with the intention of or foresight for addressing the novel issues we now face specifically with health information and mass data uses. Given that health information is considered among the most valued and important forms of information under Canadian privacy jurisprudence, it would be good to consider further regulation specific to this area that would help better protect Canadians whose health information may be crossing borders.

Patient health information and data security

Preparing for the potential for security breaches that result in reidentification by machine learning algorithms will be a key task for

corporate data custodians. Prevention will be key, and PIPEDA specifically enshrines the requirement to protect health data. Principle 7 requires security safeguards to be appropriate to the sensitivity of information being stored. Principle 3.4 notes that patient health information is always considered the most sensitive type of information. Principle 7.2 goes requires that more sensitive information should be safeguarded by a higher level of protection. This means the best available methods of data security should be used when private AI companies are dealing with patient health information.

As data security protocols evolve, corporate data custodians will have to keep their systems up to date. It may even be necessary or desirable to use advanced algorithmic systems for self-improving the security systems used to combat potential breaches, though contracting for these types of advanced security systems is more likely when the company in question is not a large multinational tech conglomerate. Where possible, private data custodians should ensure patient data is as deidentified or anonymized as possible. The deidentification requirements found in prominent research ethics policies, which we cite further in the Canadian Research Ethics Policy section, would be strong starting points for internal data policy.

It is possible that the fines for offences under PIPEDA may be insufficient to deter large companies from strategically breaching regulation, though they may be multiplied by the number of breaches that occur, generating a much more substantial number.

Consent, recontact and ongoing control

PIPEDA has very clear consent requirements, and consent is only valid if it is "reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, use, or disclosure of the personal information to which they are consenting." It also clearly states that the reasonable expectations of the individual are relevant for the purposes of obtaining consent. An

example within the document states that "an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained."

This is about as close as one can reasonably expect a piece of general privacy legislation to come to touching directly on the issue of public-private health data sharing for medical AI. It indicates that any use by the AI company of the patient health data that does not relate directly to the medical care that the patient is consenting to is prohibited, unless the patient is properly informed of the alternative and can provide true informed consent. These rules go to the statutory principle that data may only be used or disclosed for purposes for which it was initially collected. Any use for the data generally results in a requirement for recontact and reconsent.

That being said, there is an allowance for personal information to be used without the knowledge or consent of the individual providing it. Under Principle 3 or PIPEDA, this can be allowed where it is impossible or impractical to seek consent, or when the organization cannot seek it because it does not have a direct relationship with the individual. The latter would be a common circumstance with commercial AI companies that are using de-identified data as a third party to the original custodian, the public health system. However, with proper integration in the public-private partnership, it would be entirely feasible to coordinate recontact. This sort of integration should be prioritized in order to protect patients' right to decide how their data is used.

PIPEDA also indicates that patients have an ongoing right to control the use of their data, via a right of withdrawal that is "subject to legal or contractual restrictions and reasonable notice." AI companies will need to plan for the contingencies associated with data removal after its integration into the AI, and the computing logistics relating to extracting a patient's data could be complex.

Provincial considerations in brief

Patient health data is protected by provincial personal information legislation or health information legislation where applicable.[47] Each province also has their own Privacy Commissioner. Provincial legislation regulates the collection of data, quality maintenance, security safeguards, and the right of individuals to access their own information.[45]

Most provinces have specific health information protection legislation. For example, in Ontario, the Personal Health Information Protection Act (PHIPA) applies to both public and private organizations that qualify as health information custodians. In British Columbia, the Freedom of Information and the Protect of Privacy Act (FOIPPA) applies to the public sector and the Personal Information Protection Act (PIPA) applies to the private sector. These provincial statutes can give rise to their own specific obligations, adding further complexity to the regulatory framework facing AI companies.

The issue of third party transfers exemplifies this. Privacy issues that arise from outsourcing and information transfer may need to be addressed differently depending on the applicable provincial laws, depending on whether the data is transferred to a location outside of Canada, and depending on whether the data remains in Canada but is controlled by a company that is primarily based outside Canada.[45] This is in part because the health information is subject to the laws in which is it located.[45]

There is variation in provincial legislative approaches to protecting personal information. This is illustrated by the approaches taken by British Columbia and Ontario. British Columbia's FOIPPA does not prohibit the transfer of data to third parties. Other legislation

[47] Office of the Privacy Commissioner of Canada. Provincial and territorial privacy laws and oversight. 2020 Jun 11. https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/. Accessed 2021 Mar 29.

regulating personal information held by provincial public institutions or private organizations also does not prohibit data transfer outright.[45] Yet, under section 30.1 of FOIPPA, public sector organizations – such as government healthcare providers who may enter into partnerships with privacy AI companies – are required to ensure that personal information is stored and accessed only in Canada. Further, public bodies and third parties are required to refuse requests for information by foreign governments and report requests to the minister overseeing FOIPPA.[45] The Nova Scotia Personal Information International Disclosure Protection Act has similar requirements. BC's PIPA does not have these requirements, but requires the private organizations it regulates to protect any information that is in their control.[45] In comparison, Ontario's PHIPA indirectly regulates transfers, as it limits how health custodians may use personal health information.[45] As we can see, the provincial locales of data collection and server installation can change applicable regulation, and AI companies may thus be selective about where they operate and which jurisdictions they service. Greater cooperation between provinces to generate more consistency in regulation that applies to commercial AI's could help to better control the extent of activities they can undertake.

Ultimately, the applicable Canadian legislation comes together across the provinces to create a relatively effective regulatory net that enables government bodies to control the use of data by private, domestic AI companies, but there are some areas for potential improvement. Specifically, third party transfers pose a significant risk to patient health information, and changes that offer better protections for patients could be beneficial for ensuring privacy.

COMMON LAW

Torts

While the respective legislative frameworks in Canada override the common law, it will still be important in some instances. The Supreme Court of Canada has categorized privacy interests as territorial, personal, or informational for the purpose of analysis.[48] Informational privacy may be defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[49] The privacy interests engaged by commercial AI most commonly will engage an individual's informational privacy interest. Key issues for common law responses to potential privacy breaches include whether patients have given informed consent for third party access to their health information and authorized particular uses, and ii) how a health care provider's professional and fiduciary obligations are engaged by commercial AI where there has been a privacy breach.

The torts of breach of confidence, invasion of privacy and intrusion upon seclusion may give rise to individual and class action causes of action in provinces where statutory causes of action coexist with these common law torts. However, in some provinces, such as British Columbia and Alberta, health information privacy protection legislation overrides or negates these causes of action in the context of health information, because said health information legislation creates a statutory cause of action for breach of privacy.[50] Because British Columbia has a statutory cause of action, courts in British Columbia do not recognize the common law tort of intrusion upon seclusion.

[48] R v Dyment, 1988 2 SCR 417 at 428-429, aff'd R v Spencer 2014 SCC 43 at para 35.
[49] R v Tessling, 2004 SCC 67 at para 23, citing A. F. Westin, *Privacy and Freedom* (1970).
[50] See Mohl v. University of British Columbia, 2009 BCCA 249, 271 B.C.A.C. 211; Facilities Subsector Bargaining Association v. British Columbia Nurses' Union, 2009 BCSC 1562.

Intrusion upon seclusion is a novel common law cause of action. It was recognized by the Ontario Court of Appeal in *Jones v Tsige.*[51] The tort of intrusion upon seclusion is a form of breach of privacy that involves access of private information for an unauthorized purpose.[52] Further dissemination is not an element of this tort. In order to establish intrusion upon seclusion, the claimant must establish that the invasion was highly offensive and caused distress, humiliation, or anguish on an objective standard. Proof of economic harm is not required.

Unlike British Columbia and Alberta, Ontario does not have a statutory cause of action to address breaches of privacy.[53] The Ontario Court of Appeal in *Hopkins v Kay*, 2015 ONCA 112 held that the *Personal Health Information Protection Act* does not preclude the existence of a common law claim for intrusion upon seclusion because PHIPA does not create a statutory cause of action for breach of privacy.[54] Common law tort causes of action may allow the Court to grant remedies to plaintiffs whose health information privacy has been breached if legislation does not provide an equivalent cause of action. Types of harm to a patient that can occur from data privacy breaches may include discrimination or humiliation, and violation of a patient's human dignity.[29]

Reliance on common law principles is thus an enforcement mechanism that can sometimes be used in cases of misuse of patient health information by private AI companies, and is a relevant factor in the deterrence thereof.

[51] *Jones v Tsige*, 2012 ONCA 32.
[52] *Oliveira v. Aviva Canada Inc. et al*, 2017 ONSC 6161, at para 8. http://canlii.ca/t/hkpw1
[53] Section 65(3) of PHIPA allows plaintiffs to recover damages for mental anguish not exceeding $10,000 arising from a defendant's wilful or reckless contravention under the Act. This limits an individual's ability to recover under PHIPA. See also Hopkins v Kay at paras 23, 44.
[54] Hopkins v. Kay, 2015 ONCA 112, http://canlii.ca/t/ggbt6 at paras 3, 71.

Fiduciary and professional obligations

As affirmed by the Supreme Court in *McInerney v MacDonald*,[55] physicians owe a fiduciary duty to their patients, which includes the duties of utmost good faith and loyalty. Patients have a reasonable expectation that these duties will be respected when they release their personal health information to their physicians. The court held in McInerney that physicians hold personal health records of patients in a "fashion somewhat akin to a trust" and that the record is "to be used by the physician for the benefit of the patient."[55] Because the patient confides this information under no personal obligation to do so, and because the of the nature of the fiduciary relationship, it gives rise to an "expectation that the patient's interest in and control of the information will continue."[55]

The nature of the fiduciary relationship between physicians and patients raises questions about circumstances where a "black box" AI is involved, and about liability is there is a breach of the patient's privacy. Physicians are likely required to obtain each patient's informed consent with respect to the risks of data sharing of their personal information and re-identification of their data. An inability for providers and patients to understand or fully predict the future uses of data by third party AI poses potential challenges to obtaining informed consent. The common law has, historically, been less accepting of things like broad consent for future use than as seen with some health information regulation and research ethics policy.[56]

In addition to fiduciary obligations, there are well-established professional regulatory mechanisms to address employees who intentionally breach privacy rules. This would include disciplinary proceedings through self-regulating colleges of physicians and surgeons, or colleges and regulators of other health professions. These

[55] *McInerney v. MacDonald*, 1992 CanLII 57 (SCC), [1992] 2 SCR 138.
[56] Caulfield T, Murdoch B. Genes, cells, and biobanks: Yes, there's still a consent problem. PLoS biology. 2017 Jul 25;15(7):e2002654.

are not part of the common law, but should be briefly noted. Operators or owners of private AI companies who are regulated health professionals may continue to be subject to certain professional rules through their work in the organization, especially if they are to any extent directly engaged in gathering health information and if they establish a direct working relationship with patients.

CANADIAN RESEARCH ETHICS POLICY

The Tri Council Policy Statement: Ethical Conduct for Research Involving Humans (2018) [TCPS2] is the key research ethics policy in Canada that would be applicable to any research involving healthcare AI and human patients.[57] (See Appendix A for a summary of key excerpts from the TCPS2.) While not a law or regulation, the TCPS2 sets the ethical norms that all federally funded researchers and research institutions must follow. It is important to note that the TCPS2 does not take precedence over common law or legislation and, as such, researchers should be reminded that the must comply with both existing law and research ethics policies.

Chapter 3 of the TCPS2 delineates the requirements of informed consent for participation in research. It states that researchers must provide "full disclosure of all information necessary for making an informed decision to participate in a research project."[57] This includes, on the subject of privacy, "an indication of who will have access to information collected about the identity of participants; a description of how confidentiality will be protected (Article 5.2); a description of the anticipated uses of data; and information indicating who may have a duty to disclose information collected, and to whom such disclosures could be made." This statement establishes disclosure of data security and confidentiality measures as key aspects of informed consent. And

[57] Canadian Institutes of Health Research. Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans [TCPS2 2018]. https://ethics.gc.ca/eng/documents/tcps2-2018-en-interactive-final.pdf

because consent must be an ongoing process by which there is an ongoing duty to provide participants with "all information relevant to their ongoing consent to participate," material changes in privacy protection likely give rise to a duty to recontact.[58] All this being said, we will see that there are exceptions to informed consent that can mean participants' data is used without their knowledge and for purposes unknown to them.

Chapter 5 is dedicated to privacy and confidentiality policy. It defines privacy as "an individual's right to be free from intrusion or interference by others," stating it is fundamental and exists "in relation to [patients'] bodies, personal information, expressed thoughts and opinions, personal communications with others, and spaces they occupy."[57] Privacy is also considered inextricably linked to informed consent, and is said to have been respected "if an individual has an opportunity to exercise control over personal information by consenting to, or withholding consent for, the collection, use and/or disclosure of information."[57]

Despite this statement, the TCPS2 does not always require informed consent for use of patient data. Identifiable health information can generally only be used for secondary purposes with informed consent, but anonymized or de-identified patient information can be used without informed consent where there is research ethics board approval. The TCPS2 acknowledges that the "use of indirectly identifying, coded, anonymized or anonymous information for research may still present risks of re-identification."[57] One instance in which the risk of re-identification grows is where researchers are linking data from one database to that over another. Here, the policy notes that "only a restricted number of individuals should perform the function of merging databases," and that "[r]esearchers should use enhanced security measures to store the merged file."[57]

[58] Caulfield T, Murdoch B, Ogbogu U. Research, Digital Health Information and Promises of Privacy: Revisiting the Issue of Consent. Canadian Journal of Bioethics/Revue canadienne de bioéthique. 2020;3(1).

As one might expect from a broad policy document of this nature, there is not a detailed set of technical requirements and best practices for how to protect privacy in various circumstances. A lack of detailed technical guidance is common for policy that does not want to be unintentionally restrictive in its interpretation and application. However, in the future it may be important to either include technical requirements for data security and de-identification, or at least to refer to the recommendations of a working group that specializes in the area in a way that makes its standards binding.

The TCPS2's distinction between anonymous and deidentified data is worth further exploration. It states that the best way to protect participants is through the use of anonymous or anonymized data, except that this is not desirable because it prohibits return of results and future linkages of that person's data.[57] It calls de-identified data in which the key code is "accessible only to a custodian or trusted third party" the "'next best' alternative."[57] However, while this may still generally be true, the noted advances in re-identification threaten not only de-identified data but also data previously considered fully anonymous. In the face of machine learning re-identification schemes, these two terms may no longer be as distinct as they once were.

Perhaps even more importantly, under Article 5.5B, the TCPS2 does not require participant consent – only research ethics board review – for "research that relies exclusively on the secondary use of non-identifiable information." Private companies doing research involving healthcare AI will likely seek exemptions from consent where possible by using this standard (even though this does not exempt them from their legal obligations), specifically in cases where large quantities of data are required and it is acceptable for them to have been stripped of identifiers. The problem is that, as noted, the concept of "non-identifiable information" is increasingly questionable or even dubious. This section of the policy states that information must be non-identifiable "for all practical purposes." The subsection of health information that could arguably meet this standard is decreasing

quickly over time. Further revisions to the policy would help to clarify the limits of this section in the context of new technical methods for breaching privacy through reidentification.

Health information legislation grants significant discretion to research ethics boards to make determinations about the level of data security required for research. Given the lack of technical guidance in the TCPS2, this could result in circumstances where patient data access is compromised due to a lack of understanding of quickly changing data security best practices. Regulators could act to increasingly centralize control over and establish more universal (and evolving) standards for human health research data security. While this risks removing some of the nuance and circumstantial evaluation from research ethics boards' functioning, increased guidance concerning security and privacy requirements for research ethics boards dealing with AI research might be welcomed and could help to protect patients.

CONCLUSIONS

Regulation of patient data use by commercial AI companies must prioritize privacy concerns while also enabling improved patient outcomes and quality of care. The regulatory approach should be consistent with foundational ethical norms that are enshrined in law and research ethics policy, such as respect for autonomy. Below we list the main conclusions of the legal and policy research in relation to each research focus.

The potential for inappropriate, use, or disclosure of personal health information by private AI companies.

- While the regulatory framework largely creates binding obligations to protect private health information, one exception is the regulation of third parties who are transferred patient data in accordance with PIPEDA. Altering regulation to place more custodianship responsibility onto domestic third parties that are transferred patient heath information would help contribute to the safe future implementation of healthcare AI. In addition, thoughtful consideration should be given to regulation specific to international transfers of health information to third parties, as this could help better protect Canadians whose health information may be crossing borders.
- Access to patient health information should be dependent upon relevant regulatory approval. The scope of data made accessible should be firstly based on respect of patients' informed consent and rights of ongoing control over their private information, and after that, proportional to the likelihood and meaningfulness of the potential benefits the AI can provide. This would be determined by regulators based on an evidence-based assessment of the current effectiveness of the AI as noted in approved research and trials, reasonable extrapolations of effectiveness to account for future refinements, and the public health and other public implications of granting access. This assessment would need to be open the

periodical review as the AI changed over time. Access must also be predicated upon maintaining highly advanced forms of data security, and anonymization where possible.

- Greater cooperation between provinces to generate more consistency in the regulation that applies to commercial AI companies could help their implementation and to encourage compliance.
- The presence of a strong regulatory framework does not always translate to protection of patient rights if regulations are not respected by those to whom they apply and if they are not enforced by regulators. As we previously noted, technology companies have at times fragrantly disregarded the law in several jurisdictions, collecting and using data in breach of regulation and without regard for the consequences. Enforcement of the law is therefore a significant concern for maintaining privacy in this context. As such, penalties levied against AI companies in breach of privacy requirements should, in our view, not be fixed or limited in any way that could fail to deter malfeasance. They could instead guarantee that the company could not experience a net gain from the misuse of data, to avoid corporate use of a cost-benefit analysis to justify misusing data for profitability.
- Patients have a general right to informed consent for the use and disclosure of their personal health information, and have an ongoing control interest which necessitates the need for recontact for any new uses or disclosures. Integration of public-private partnerships implementing healthcare AI should prioritize the ability to recontact patients.
- Patients have a general right of withdrawal from participation in healthcare AI. AI companies will need to plan for the contingencies associated with data removal after its integration into the AI, and the computing logistics relating to extracting a patient's data could be complex.
- Regulation of health information gathered outside the traditional clinical context will become increasingly important, especially as AI

may be used for data-matching. Engagement with the public and stakeholders will be important in determining any needed additional protections for private individual health information. Recent surveys strongly suggest a large portion of the public is uncomfortable with sharing their personal health information with large technology companies.[59]

The potential for privacy breaches that use AI to reidentify patient health information.

- The concept of "non-identifiable information" is increasingly questionable. The subsection of health information that could arguably meet this standard is decreasing quickly. Regulators and policymakers must incorporate into their work the reality that technical methods of breaching privacy through reidentification are rapidly improving.
- Strong privacy protection will be required in light of advancing technology that allows data to be re-identified and misused. Data security should minimize risks during data transfer, safe storage and appropriate deletion.[29] Further, consent requirements should disclose both any possible personal data transfers to commercial entities, and the realistic risk of privacy breach.
- The issue of data security is shared among both institutions that grant access to patient data for AI companies to utilize, and the AI companies manipulating and/or storing patient data themselves. To the extent they cooperate and exchange information, the responsibility for security must be shared and integration must be extensive.
- The regulatory frameworks in Canada are up to the task of obligating AI companies to protect the privacy of their health information from hackers and sophisticated forms of reidentification. However, enforcement of very high standards for data protection will be key. Governments should consider creating

[59] Rock Health. Beyond Wellness For the Healthy: Digital Health Consumer Adoption 2018. https://rockhealth.com/reports/beyond-wellness-for-the-healthy-digital-health-consumer-adoption-2018/?mc_cid=0c97d69dbe&mc_eid=452e95c5c5. Accessed 2021 Mar 15.

interdisciplinary task forces focused specifically on creating, refining and implementing technical standards for protecting patient health information from reidentification schemes.

- In the context of research, health information legislation grants significant discretion to research ethics boards to make determinations about the level of data security required, as the Tri Council Policy Statement does not provide detailed technical data security guidance. This could result in circumstances where patient data access is compromised due to a lack of understanding of quickly changing data security best practices. If desired, regulators could act to increasingly centralize control over and establish more universal (and evolving) standards for human health research data security. While this risks removing some of the nuance and circumstantial evaluation from research ethics boards' functioning, increased guidance concerning security and privacy requirements for research ethics boards dealing with AI research might be welcomed and could help to protect patients.

Acknowledgments

The authors thank the Office of the Privacy Commissioner of Canada for funding this research. They also thank Robyn Hyde-Lay and the rest of the team at the Health Law Institute for their helpful suggestions and administrative support.

APPENDICES

APPENDIX A: SELECTED EXCERPTS FROM THE TCPS2

Article 3.2 *Researchers shall provide to prospective participants, or authorized third parties, full disclosure of all information necessary for making an informed decision to participate in a research project.*

The information generally required for informed consent includes […] an indication of what information will be collected about participants and for what purposes; an indication of who will have access to information collected about the identity of participants; a description of how confidentiality will be protected (Article 5.2); a description of the anticipated uses of data; and information indicating who may have a duty to disclose information collected, and to whom such disclosures could be made […]

Article 5.2: *Researchers shall describe measures for meeting confidentiality obligations and explain any reasonably foreseeable disclosure requirements:*

a. in application materials they submit to the REB; and
b. during the consent process with prospective participants.

Article 5.3: *Researchers shall provide details to the REB regarding their proposed measures for safeguarding information, for the full life cycle of information: its collection, use, dissemination, retention and/or disposal.*

Factors relevant to the REB's assessment of the adequacy of the researchers' proposed measures for safeguarding information [under Article 5.3] include:

a. the type of information to be collected;
b. the purpose for which the information will be used, and the purpose of any secondary use of identifiable information;
c. limits on the use, disclosure and retention of the information;

d. risks to participants should the security of the data be breached, including risks of re-identification of individuals;
e. appropriate security safeguards for the full life cycle of information;
f. any recording of observations (e.g., photographs, videos, sound recordings) in the research that may allow identification of particular participants;
g. any anticipated uses of personal information from the research; and
h. any anticipated linkage of data gathered in the research with other data about participants, whether those data are contained in public or personal records (see also Section E of this chapter).

Article 5.4: *Institutions or organizations where research data are held have a responsibility to establish appropriate institutional security safeguards.*

Article 5.5B *Researchers shall seek REB review, but are not required to seek participant consent, for research that relies exclusively on the secondary use of non-identifiable information.*

APPENDIX B: TABLES OF PROVINCIAL PRIVACY AND HEALTH INFORMATION LEGISLATION

A. Health Information Protection Legislation

Province	Health Information Legislation	Substantially Similar to PIPEDA?
British Columbia	E-Health (Personal Health Information Access and Protection of Privacy) Act, SBC 2008, c 38, <https://canlii.ca/t/54qpf>	No.
Alberta	Health Information Act, RSA 2000, c H-5 <https://www.qp.alberta.ca/1266.cfm?page=h05.cfm&leg_type=Acts&isbncln=9780779803170>.	No.
Saskatchewan	Personal Health Information Protection Act, 2004, SO 2004, c 3, Sch A, <http://canlii.ca/t/549p5>.	No.
Manitoba	The Personal Health Information Act, CCSM c P33.5, <http://canlii.ca/t/53nd1>.	No.
Ontario	Personal Health Information Protection Act, 2004, SO 2004, c 3, Sch A, <http://canlii.ca/t/549p5>.	Yes.
Newfoundland and Labrador	Personal Health Information Act, SNL 2008, c P-7.01, <https://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm>.	Yes.
Prince Edward Island	Health Information Act, RSPEI 1988, c H-1.41, < https://www.canlii.org/en/pe/laws/stat/rspei-1988-c-h-1.41/latest/rspei-1988-c-h-1.41.html?resultIndex=11 >.	No.
Nova Scotia	Personal Health Information Act, SNS 2010, c 41, <https://www.canlii.org/en/ns/laws/stat/sns-2010-c-41/latest/sns-2010-c-41.html>.	Yes.
New Brunswick	Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05	Yes.

	<http://laws.gnb.ca/en/showfulldoc/cs/P-7.05//20200508>.	
Yukon	Health Information Privacy And Management Act, SY 2013, c 16, <http://canlii.ca/t/53l1x>.	No.
Northwest Territories	Health Information Act, SNWT 2014, c 2, <http://canlii.ca/t/52sc0>.	No.
Nunavut	Public Health Act, SNu 2016, c 13, < https://www.canlii.org/en/nu/laws/stat/snu-2016-c-13/latest/snu-2016-c-13.html >.	No.
Quebec	Act respecting the Régie de l'assurance maladie du Québec, CQLR c R-5, <https://canlii.ca/t/54c6q>.	No.

B. Public Sector Legislation

Province	**Public Sector Legislation**	**Substantially similar to PIPEDA?**
British Columbia	Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165, <https://canlii.ca/t/54x5k>.	No.
Alberta	Freedom of Information and Protection of Privacy Act, RSA 2000, c F-25, <https://canlii.ca/t/54wfj>.	No.
Saskatchewan	The Freedom of Information and Protection of Privacy Act, SS 1990-91, c F-22.01, https://canlii.ca/t/543dk.	No.
Manitoba	The Freedom of Information and Protection of Privacy Act, CCSM c F175, <https://canlii.ca/t/5449f>.	No.
Ontario	Freedom of Information and Protection of Privacy Act, RSO 1990, c F.31, <https://canlii.ca/t/54cfl>.	No.
Newfoundland and Labrador	Access to Information and Protection of Privacy Act, 2015, SNL 2015, c A-1.2, <https://canlii.ca/t/548bf>.	No.
Prince Edward Island	Freedom of Information and Protection of Privacy Act, RSPEI 1988, c F-15.01, https://canlii.ca/t/54vnx.	No.

Nova Scotia	Freedom of Information and Protection of Privacy Act, SNS 1993, c 5, https://canlii.ca/t/53gt1. Privacy Review Officer Act, SNS 2008, c 42, <https://canlii.ca/t/jr5j>. Personal Information International Disclosure Protection Act, SNS 2006, c 3, <https://canlii.ca/t/lcp7>.	No.
New Brunswick	Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6, <https://canlii.ca/t/54x66>.	No.
Yukon	Access to Information and Protection of Privacy Act, RSY 2002, c 1, <https://canlii.ca/t/5483k>.	No.
Northwest Territories	Access to Information and Protection of Privacy Act, SNWT 1994, c 20, <https://canlii.ca/t/54v56>	No.
Nunavut	Access to Information and Protection of Privacy Act, SNWT (Nu) 1994, c 20, https://canlii.ca/t/5345s.	No.
Quebec	Act respecting Access to documents held by public bodies and the Protection of personal information, CQLR c A-2.1, <https://canlii.ca/t/54vgq>.	No.

C. Non-Sector Specific Private Sector Legislation

Province	**Non-Sector Specific Private Sector Legislation**	**Substantially Similar to PIPEDA?**
British Columbia	Personal Information Protection Act, SBC 2003, c 63, <https://canlii.ca/t/52pq9>	Yes.
Alberta	Personal Information Protection Act, SA 2003, c P-6.5, <https://canlii.ca/t/5442f>	Yes.
Quebec	Act respecting the protection of personal information in the private sector, CQLR c P-39.1, <https://canlii.ca/t/53hxv>.	Yes.

Note: Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia have substantially similar health privacy laws to PIPEDA. See Canada OotPCo. Summary of Privacy Laws in Canada 2018 [Available from: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/. (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/).

Note: Ontario is changing their health information legislation. See Fabiano D, MacRae S. Fasken Martineau DuMoulin LLP. 2020. [cited 2020]. Available from: https://www.fasken.com/en/knowledge/2020/03/significant-changes-to-ontarios-health-privacy-law/. (https://www.fasken.com/en/knowledge/2020/03/significant-changes-to-ontarios-health-privacy-law/).

See Bill 188, Schedule 6 (page 11): An Act to enact and amend various statutes, 42nd Legislature, Ontario 69 Elizabeth II, 2020, 1st Sess. (2020).

(https://www.ola.org/sites/default/files/node-files/bill/document/pdf/2020/2020-03/b188ra_e.pdf).

Note: Nunavut does not have specific health information protection legislation, but instead protects health information through its recently enacted Public Health Act. See Nunavut-made Public Health Act becomes law [press release]. 2020. https://www.gov.nu.ca/sites/default/files/2020-01_nr_hea_public_health_act_becomes_law_-_eng.pdf.