Canadian Journal of Bioethics
Revue canadienne de bioéthique

Canadian Journal of Bioethics
Revue Canadienne de Bioéthique

Privacy Considerations in the Canadian Regulation of Commercially-Operated Healthcare Artificial Intelligence

Blake Murdoch, Allison Jandura et Timothy Caulfield

Volume 5, numéro 4, 2022

URI : https://id.erudit.org/iderudit/1094696ar
DOI : https://doi.org/10.7202/1094696ar

Aller au sommaire du numéro

Éditeur(s)

Programmes de bioéthique, École de santé publique de l'Université de Montréal

ISSN

2561-4665 (numérique)

Découvrir la revue

Citer cet article

Murdoch, B., Jandura, A. & Caulfield, T. (2022). Privacy Considerations in the Canadian Regulation of Commercially-Operated Healthcare Artificial Intelligence. *Canadian Journal of Bioethics / Revue canadienne de bioéthique*, *5*(4), 44–52. https://doi.org/10.7202/1094696ar

Résumé de l'article

L'intelligences artificielle (IA) est de plus en plus développées et mises en oeuvre dans le domaine des soins de santé. Cela pose des problèmes de protection de la vie privée, car de nombreuses IA sont privées et dépendent d'accords de partage de données pour des quantités massives d'informations sur la santé des patients. Nous avons étudié le cadre juridique et politique canadien en nous concentrant sur la réglementation relative à la possibilité d'une utilisation ou d'une divulgation inappropriée de renseignements personnels sur la santé par des entreprises privées d'IA. Nous avons notamment analysé les lois fédérales et provinciales, la common law et la politique d'éthique de la recherche. Notre évaluation des divers cadres réglementaires a révélé qu'ensemble, ils exigent que les entreprises privées d'IA et leurs partenaires dans la mise en oeuvre des soins de santé respectent des normes élevées de protection de la vie privée qui privilégient l'autonomie des patients, à quelques exceptions près. Nous avons constaté que les systèmes d'IA dans le domaine des soins de santé doivent être conformes aux règles et aux normes éthiques fondamentales consacrées par la loi et l'éthique de la recherche, même si cela pose des problèmes de mise en oeuvre. Les accords de partage de données doivent être axés sur une intégration étroite, avec des niveaux élevés de sécurité des données, une surveillance étroite et le maintien du contrôle des données par le patient.

Canadian Journal of Bioethics
Revue Canadienne de Bioéthique

B Murdoch, A Jandura, T Caulfield
Can J Bioeth / Rev Can Bioeth. 2022;5(4):44-52

ARTICLE (ÉVALUÉ PAR LES PAIRS / PEER-REVIEWED)

Privacy Considerations in the Canadian Regulation of Commercially-Operated Healthcare Artificial Intelligence

Blake Murdoch[a], Allison Jandura[a], Timothy Caulfield[a]

Résumé
L'intelligences artificielle (IA) est de plus en plus développées et mises en œuvre dans le domaine des soins de santé. Cela pose des problèmes de protection de la vie privée, car de nombreuses IA sont privées et dépendent d'accords de partage de données pour des quantités massives d'informations sur la santé des patients. Nous avons étudié le cadre juridique et politique canadien en nous concentrant sur la réglementation relative à la possibilité d'une utilisation ou d'une divulgation inappropriée de renseignements personnels sur la santé par des entreprises privées d'IA. Nous avons notamment analysé les lois fédérales et provinciales, la common law et la politique d'éthique de la recherche. Notre évaluation des divers cadres réglementaires a révélé qu'ensemble, ils exigent que les entreprises privées d'IA et leurs partenaires dans la mise en œuvre des soins de santé respectent des normes élevées de protection de la vie privée qui privilégient l'autonomie des patients, à quelques exceptions près. Nous avons constaté que les systèmes d'IA dans le domaine des soins de santé doivent être conformes aux règles et aux normes éthiques fondamentales consacrées par la loi et l'éthique de la recherche, même si cela pose des problèmes de mise en œuvre. Les accords de partage de données doivent être axés sur une intégration étroite, avec des niveaux élevés de sécurité des données, une surveillance étroite et le maintien du contrôle des données par le patient.

Mots-clés
droit de la santé, vie privée, intelligence artificielle, bioéthique, législation, Canada

Abstract
Artificial intelligence (AI) is increasingly being developed and implemented in healthcare. This presents privacy issues since many AI systems are privately owned and rely on data sharing arrangements for mass quantities of patient health information. We investigated the Canadian legal and policy framework focusing on regulation relevant to the potential for inappropriate use or disclosure of personal health information by private AI companies. This included analysis of federal and provincial legislation, common law and research ethics policy. Our evaluation of the various regulatory frameworks found that together they require private AI companies and their partners in healthcare implementation to meet high standards of privacy protection that prioritize patient autonomy, with limited exceptions. We found that healthcare AI systems are required to be consistent with the rules and foundational ethical norms enshrined in law and research ethics, even if this poses challenges to implementation. Data sharing arrangements must focus on tight integration with high levels of data security, strong oversight and retention of patient control over data.

Keywords
health law, privacy, artificial intelligence, bioethics, legislation, Canada

Affiliations
[a] Health Law Institute, Faculty of Law, University of Alberta, Edmonton, Alberta, Canada
Correspondance / Correspondence: Blake Murdoch, bmurdoch@ualberta.ca

INTRODUCTION

Advances in artificial intelligence (AI) are occurring rapidly and will soon have a significant impact on medical 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. It will likely be used in both patient-facing and population level applications (1-3). Several new AI technologies are approaching feasibility, and a few are in the process of being integrated into healthcare systems (4,5). Radiation oncology, organ allocation, robotic surgery, and several other healthcare domains stand to benefit from AI technologies in the short to medium term (6-10).

AI systems have several unique characteristics compared with traditional health technologies. Notably, they can be prone to certain types of errors and biases (11-14), and often cannot be easily 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 (9,12). This opacity may also apply to how health and personal information is used and manipulated.

Many AI technologies are developed and maintained by private companies and will be implemented in partnership with public healthcare providers. Health-related AI are being developed both with personal health information and data that falls outside the boundaries of regulation of personal health information, such as secondary uses of de-identified data and certain data arising from commercial digital products. The use of commercial AI in healthcare 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 (15). Canadian law protects privacy, including the *Personal Information Protection and Electronic*

ISSN 2561-4665

Documents Act, SC 2000, c 5 [PIPEDA], provincial privacy and health information statutes, and jurisprudence such as *McInerney v McDonald*, 1992 CANLII 57 (SCC), which we explore further below.

Respect for privacy is an important ethical principle in healthcare because it flows from a patient's autonomy, personal identity and well-being (16). Privacy has both intrinsic and extrinsic value, and a privacy offense can occur regardless of whether actual harm was done to the compromised individual (17). Healthcare AI relates to informational privacy, that is, to the use and control over one's personal information (18). AI privacy issues arise both with respect to the entities collecting personal information, and the threat of malicious cyberattacks (19). Here we explore the application of the existing Canadian legal and research ethics frameworks to privacy issues with commercial healthcare AI implementation. We focus our analysis primarily on the risks of inappropriate handling, use or disclosure of personal health information by private AI companies, and also touch on the potential for privacy breaches that could result in the reidentification of patient health information. Analysis of the various regulatory frameworks shows that together they require private AI companies and their partners in healthcare implementation to meet high standards of privacy protection that prioritize patient autonomy, with limited exceptions.

PRIVACY CONCERNS

Inappropriate handling, use or disclosure of personal health information by private actors is a major privacy concern. 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 and implementing large investments in healthcare technology, much of which involves AI (20). Information sharing agreements can be used to contractually grant these private institutions access to government-held patient health information. Health information has considerable economic value to commercial entities for developing and using AI deep learning for profitable purposes and otherwise. This can be particularly so when it is combined with other personal information from "disparate domains" of an individual's life to allow AI to make additional inferences about an individual (21-25).

Public-private partnerships with tech companies have sometimes 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 (21). There was concern around patient control over use of personal data, as critics noted that patients were not afforded agency nor were privacy impacts properly discussed (21). One English Department of Health advisor said the patient information was obtained on an "inappropriate legal basis" (26). Google subsequently took direct control over DeepMind's app, transferring control over stored patient data from the United Kingdom to the United States, generating further controversy (27). The ability of a large tech company to "annex" mass quantities of private patient data to another jurisdiction is a new reality of big data, and there can be insufficient protections to guarantee that problematic external and/or third-party transfers do not occur. The concentration of technological innovation and knowledge in big tech companies can create power imbalances where public institutions could become more dependent and less equal partners in health tech implementation. These power imbalances can be factors causing and/or exacerbating the risk of inappropriate acquisition and treatment of personal health information.

The DeepMind example suggests that appropriate safeguards must be in place to maintain privacy and patient agency in the context of commercial transfer of health information. Smaller companies may in some respects be even less able to be held to account because they can easily fail, going bankrupt and/or being purchased by larger companies (along with all their data and intellectual property). AIs pose a novel challenge because they can require access to large quantities of patient data and the way in which the data is used may evolve over time (28). The location and ownership of servers and computers that store and access patient health information will therefore be an important consideration.

A second concern worth briefly noting is the risk of inappropriate technology-driven reidentification of de-identified or anonymized patient health information. De-identified information is information that has personal identifiers removed where the data custodian retains a way to relink the identifiers in the future, and fully anonymized data theoretically should not be re-identifiable. Health information breaches are on the rise in Canada (29-31), and AIs and other algorithms are contributing to a growing inability to protect health information (32-33). Recent studies have highlighted how emerging computational strategies can identify individuals from information in health data repositories (34), with the result that information that has been anonymized and scrubbed of all identifiers can be reidentified (35-38). This sort of re-identification can "effectively nullify scrubbing and compromise privacy." (39) Hostile reidentification techniques could increase the risks of privacy breach from allowing private AI companies to control patient health information, even when it is "anonymized." It also raises questions of liability, insurability, and other practical issues that are somewhat distinct from circumstances where public health information custodians control patient data.

LEGISLATION

The web of Canadian privacy legislation

There is a lack of true and complete standardization of privacy legislation in Canada, both inter and intra-provincially. And AI companies can be required to comply with multiple overlapping pieces of legislation (40). 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 (GDPR) and/or the Health Insurance Portability and Accountability Act (HIPA) might also need

to be respected (41-42). While it is beyond the scope of this article to consider the application of extraterritorial regulation, these rules could have important implications for the use of commercial AIs 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. PIPEDA is a key statute to consider in relation to the privacy issues stated above, due to its applicability to federally and some provincially regulated private corporations who develop and implement AI technologies (43). Provincial legislation that 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 many of the provisions of PIPEDA.

Provincial health information protection legislation and, in some cases, provincial public sector privacy regulation, are also relevant for the commercial transfers of health information that implementation of new technologies will necessitate. Patient health data is protected by provincial personal information legislation and health information legislation where applicable (44). As above, 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 many cases (45). Other provinces also have health privacy laws, but they have not been declared substantially similar and thus are not exempt from the rules in PIPEDA. Again, AI companies will sometimes have to comply with multiple overlapping pieces of legislation (41).

There is regulatory complexity to potential arrangements with AI companies that use mass quantities of patient health information. Hospitals or public healthcare providers implementing private AIs will be required to comply with all relevant privacy and health information legislation. Any commercial activities done by contractors or collaborators may be required to comply with applicable provincial legislation and PIPEDA (45). 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 (45). Because the provincial locales of data collection and server installation can change applicable regulation, there could be incentives to prioritize work in jurisdictions with the most favourable data storage obligations. PIPEDA helps to resolve some of these concerns, though greater cooperation between provinces to generate more consistency in regulation that applies to commercial AIs could help to better regulate the extent of activities they can undertake.

The intent of this piece is not to deal with the nuanced interactions between federal and provincial statutes in each individual province, but to note broadly applicable rules that are of particular importance to private implementations of healthcare AIs and the privacy concerns we delineated. It is conceivable that a healthcare AI company could operate entirely within a single province. However, 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 or a few jurisdictions, we can reasonably conclude that PIPEDA will apply in most cases.

Patient health information and data security

Preparing for potential security breaches, including those that result in reidentification by machine learning algorithms, is a legal obligation of corporate data custodians. Preventative measures are required, which PIPEDA specifically enshrines. 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 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 update their systems. 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 multinational tech conglomerate. Where possible, 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.

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.” (43) 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.” (43)

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 AIs. It indicates that any use by the AI company of patient health data that does not relate directly to 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 new use for the data generally results in a requirement for recontact and reconsent. That being said, there is a limited 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 could occur 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 between public and private actors, it can be feasible to coordinate recontact. This sort of integration could be prioritized in order to uphold 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." (43) AI companies will need to plan for the contingencies associated with data removal after its integration into AIs, and the computing logistics relating to extracting a patient's data could be complex.

Third party transfers

Third party transfers pose a significant risk to patient health information. Transfers like seen in the DeepMind example, as well as more normal course of business transfers to contractor partners, can result in insufficient data protection and inappropriate use or disclosure by private AI companies. Privacy issues that arise from outsourcing and information transfer may need to be addressed differently depending on the applicable provincial laws, whether the data is transferred to a location outside of Canada, and whether the data remains in Canada but is controlled by a company that is primarily based outside Canada. This is in part because the health information is subject to the laws of the jurisdiction in which is it located.

PIPEDA, unlike some provincial privacy legislation, does not apply to third party providers that receive information as part of a transfer (46). 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 AIs could be transferred for similar commercial purposes. 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 (44). 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 personal data. It is at the discretion of individual organizations to assess whether personal information is too sensitive or a risk of disclosure is too great to enter into a given agreement.

Third parties to commercial healthcare AI implementations, 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 by third parties with the only likely outcome being financial loss, there is insufficient protection against the use of ruthless economic calculation to justify unapproved use of health information. Especially for domestic third parties over which governments have clear jurisdiction, it is problematic for patient privacy to allow third parties to fail to protect health information whenever it is economically beneficial to do so. It is possible that the remedies under PIPEDA may be insufficient to deter large companies from strategically breaching regulation. As such, altering regulation to place more custodianship responsibility onto domestic third parties in control of patient heath information could be one way for regulators to reduce this risk.

In an international context, it may be difficult to make changes to this system without directly hampering cross-border commerce and the related ability to move private data internationally. However, PIPEDA was not necessarily created with the entire requisite 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 law, policymakers might consider further regulation specific to this area that would provide protections for health information that may be crossing borders, while giving due consideration to the personal information protections existing in other jurisdictions (47).

COMMON LAW

Torts

While the respective Canadian legislative frameworks override the common law, it will still be important in some instances where personal information is or could be mishandled by private AI companies. Torts can of course also be relevant to intentional, targeted security breaches. 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 involve individuals' informational privacy. 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 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.

Intrusion upon seclusion is a novel common law cause of action. It was recognized by the Ontario Court of Appeal in *Jones v Tsige* (52). 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.

This tort is important in part because unlike British Columbia and Alberta, Ontario does not have a statutory cause of action to address breaches of privacy. Section 65(3) of *Personal Health Information Protection Act* (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. The Ontario Court of Appeal in *Hopkins v Kay*, 2015 ONCA 112 held that the PHIPA 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 (53). Common law tort causes of action like intrusion upon seclusion 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 (54).

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

Fiduciary and professional obligations

As affirmed by the Supreme Court in *McInerney v MacDonald*, physicians owe a fiduciary duty to their patients, which includes the duties of utmost good faith and loyalty (55). 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." (59) Because the patient confides this information under no personal obligation to do so, and because 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." (59)

The nature of the fiduciary relationship between physicians and patients raises questions about liability in circumstances where a "black box" AI is involved (56,57), including where there could be a breach of the patient's privacy. Physicians will likely be required to obtain patients' informed consent with respect to the risks of data sharing of their personal information and re-identification of their data. They also are likely to be involved in advising patients about the technologies and how they use private data. An inability for providers and patients to understand or fully predict the future uses of data by third party AIs poses potential challenges to obtaining informed consent, and common law is historically less accepting of concepts like broad consent for future use than is regulation. If physicians cannot understand or explain how an AI's decision will be made, it can raise concern as to whether consent is truly informed. Also, because integration of AI into healthcare can result in situations where access to care is dependent upon a patient agreeing to broad consent for future unknown uses of data, there can be an element of undue pressure in the collection of consent that may compromise privacy rights. This would raise questions about whether a collecting physician is meeting their duty of care to prioritize the patient's interests above others. The problem may require considering some careful alterations to the limits of physicians' fiduciary duty under Canadian law, including the possibility of legislative intervention to cleave away some of the traditional responsibility placed on physicians and attribute those portions wholly to AI companies themselves.

In addition to fiduciary obligations, there are well-established professional regulatory mechanisms to address professional 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 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

At least initially, most implementations of privately developed healthcare AI in Canada will begin via research-based pilot projects. This provides the governmental data custodian with proof of efficacy and safety prior to broad implementation. Several

provinces' health information legislation, an example being Alberta's *Health Information Act*, largely offload many decisions about the permissibility of research uses of and consents for collection of health information to research ethics boards. Hence, many research ethics rules will be determinative in terms of how private AI companies obtain and use patient data.

Canadian research ethics boards largely rely upon the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (TCPS2), the key research ethics policy in Canada that would be applicable to almost any research involving healthcare AIs and human patients (58). 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, however, 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." (63) 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." (63) This statement establishes disclosure of data security and confidentiality measures as key aspects of informed consent. And 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 (59). That 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 that it is fundamental and exists "in relation to [patients'] bodies, personal information, expressed thoughts and opinions, personal communications with others, and spaces they occupy." (63) 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." (63) 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." (63) One instance in which the risk of re-identification grows is where researchers are linking data from one database to that of 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." (63)

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 when this is not desirable because it prohibits return of results and future linkages of that person's data (63). Data is considered de-identified data where the key code is "accessible only to a custodian or trusted third party" the "'next best' alternative." (63) 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." (63) Private companies doing research involving healthcare AIs will likely seek exemptions from consent where possible 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." (63) The subsection of health information that could arguably meet this standard is decreasing over time. Further revisions to the policy could 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 would be helpful.

CONCLUSION

Regulation of patient data use by commercial AI companies must prioritize privacy concerns while striving to improve patient outcomes and quality of care. Implementations of healthcare AIs will need to be consistent with foundational ethical norms that are enshrined in law and research ethics, including respect for autonomy. Commercial transfers of health information to implement these technologies must focus on tight integration that results in high levels of data security, strong oversight of data use and retention of patient control over use of their data. While the costs of maintaining high privacy standards to healthcare AI development and the speed of improvement of clinical care may not be insignificant, the current Canadian legal framework requires comprehensiveness with limited exceptions. If policymakers wished to reduce regulatory burden of privacy requirements because they believed it would ultimately improve patient care, changes to the Canadian framework would be required. Table 1 summarizes our key findings and recommendations concerning patient privacy for commercial AI implementation.

Table 1: Key findings and recommendations

1. ***Patients have a general right to informed consent*** for the use and disclosure of their identifiable personal health information and have an ongoing control interest which necessitates the need for recontact for any new uses or disclosures.
2. ***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.
3. ***Altering regulation to place more custodianship responsibility onto domestic third parties*** that are transferred patient heath information would address a source of risk in AI company data custodianship.
4. ***Greater cooperation between provinces to generate more consistency*** in regulation that applies to commercial AI companies could aid implementation and encourage compliance.
5. ***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 should incorporate into their work the reality that technical methods of breaching privacy through reidentification are quickly evolving.
6. ***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 methods should minimize risks during data transfer, safe storage, and appropriate deletion. Further, consent requirements must disclose both any possible personal data transfers to commercial entities, and the realistic risk of privacy breach.
7. ***Data security responsibility is shared*** among both institutions that grant access to patient data for use by AI companies, and the AI companies manipulating and/or storing patient data themselves. Required integrations may be extensive.
8. ***Governments could consider creating interdisciplinary task forces*** focused specifically on developing, refining and implementing technical standards for protecting patient health information in AI implementations.

Reçu/Received: 15/07/2021

Publié/Published: 9/12/2022

Remerciements

Merci à Ubaka Ogbogu et à Robyn Hyde-Lay pour leurs commentaires et suggestions utiles. Les auteurs tiennent également à remercier le Commissariat à la protection de la vie privée du Canada, Genome Alberta et Génome Canada pour leur généreux soutien aux projets : « Privacy and Artificial Intelligence: Protecting Health Information in a New Era » et « Precision Medicine CanPREVENT AMR. »

Acknowledgements

Thanks to Ubaka Ogbogu and to Robyn Hyde-Lay for their helpful comments and suggestions. The authors would like to thank the Office of the Privacy Commissioner of Canada, Genome Alberta and Genome Canada for their generous support of the projects: "Privacy and Artificial Intelligence: Protecting Health Information in a New Era" and "Precision Medicine CanPREVENT AMR."

Conflits d'intérêts

Aucun à déclarer

Conflicts of Interest

None to declare

Édition/Editors: Aliya Affdal

Les éditeurs suivent les recommandations et les procédures décrites dans le Code of Conduct and Best Practice Guidelines for Journal Editors de COPE. Plus précisément, ils travaillent pour s'assurer des plus hautes normes éthiques de la publication, y compris l'identification et la gestion des conflits d'intérêts (pour les éditeurs et pour les auteurs), la juste évaluation des manuscrits et la publication de manuscrits qui répondent aux normes d'excellence de la revue.

The editors follow the recommendations and procedures outlined in the COPE Code of Conduct and Best Practice Guidelines for Journal Editors. Specifically, the editors will work to ensure the highest ethical standards of publication, including: the identification and management of conflicts of interest (for editors and for authors), the fair evaluation of manuscripts, and the publication of manuscripts that meet the journal's standards of excellence.

Évaluation/Peer-Review: Nicholson Price & Jay Shaw

Les recommandations des évaluateurs externes sont prises en considération de façon sérieuse par les éditeurs et les auteurs dans la préparation des manuscrits pour publication. Toutefois, être nommé comme évaluateurs n'indique pas nécessairement l'approbation de ce manuscrit. Les éditeurs de la *Revue canadienne de bioéthique* assument la responsabilité entière de l'acceptation finale et de la publication d'un article.

Reviewer evaluations are given serious consideration by the editors and authors in the preparation of manuscripts for publication. Nonetheless, being named as a reviewer does not necessarily denote approval of a manuscript; the editors of *Canadian Journal of Bioethics* take full responsibility for final acceptance and publication of an article.

REFERENCES

1. Hamid S. The Opportunities and Risks of Artificial Intelligence in Medicine and Healthcare. CUSPE Communications. 2016.
2. Price Nicholson II W. Artificial intelligence in the medical system: four roles for potential transformation. Yale Journal of Law & Technology. 2019;21:122-32.
3. Tschider CA. AI's legitimate interest: towards a public benefit privacy model. Houston Journal of Health Law & Policy. 2021;21:101-61.
4. Jiang F, Jiang Y, Zhi H, et al. Artificial intelligence in healthcare: past, present and future. Stroke and Vascular Neurology. 2017;2(4):230-43.
5. Johnson KW, Soto JT, Glicksberg BS, et al. Artificial intelligence in cardiology. Journal of the American College of Cardiology. 2018;71(23):2668-79.
6. Thompson RF, Valdes G, Fuller CD, et al. Artificial intelligence in radiation oncology: a specialty-wide disruptive transformation? Radiotherapy and Oncology. 2018;129(3):421-6.
7. Canadian Blood Services. Kidney Paired Donation (KPD) Program. 2019.
8. 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;48(4):e12901.
9. O'Sullivan S, Nevejans N, Allen C, et al. 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;15(1):e1968.
10. Hashimoto DA, Rosman G, Rus D, Meireles OR. Artificial intelligence in surgery: promises and perils. Annals of surgery. 2018;268(1):70-6.
11. Dietterich T. Overfitting and undercomputing in machine learning. ACM Computing Surveys. 1995;27(3):326-7.
12. Mukherjee S. A.I. versus M.D. The New Yorker. Annals of Medicine. 3 Apr 2017.
13. Cuttler M. Transforming health care: How artificial intelligence is reshaping the medical landscape. CBC News. 26 Apr 2019.
14. Char DS, Shah NH, Magnus D. Implementing machine learning in health care—addressing ethical challenges. The NEJM. 2018;378(11):981-3.
15. United Nations. Universal Declaration of Human Rights. 10 Dec 1948.
16. Reddy S, Allan S, Coghlan S, Cooper P. A governance model for the application of AI in health care. Journal of the American Medical Informatics Association. 2020;27(3):491-7.
17. Nicholson Price II W, Cohen IG. Privacy in the age of medical big data. Nature Medicine. 2019;25(1):37-43.
18. 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):338-52.
19. 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.
20. Powles J, Hodson H. Google DeepMind and healthcare in an age of algorithms. Health and Technology. 2017;7(4):351-67.
21. Skopek JM. Untangling privacy: Losses versus violations. Iowa Law Review. 2019;105(5):2169-2231.
22. Crawford K, Schultz J. Big data and due process: Toward a framework to redress predictive privacy harms. Boston College Law Review. 2014;55:93-128.
23. Nicholson Price II W. Problematic interactions between AI and health privacy. Utah Law Review. 2021;4:925-36.
24. Tschider CA. Regulating the internet of things: discrimination, privacy, and cybersecurity in the artificial intelligence age. Denver Law Review. 2018;96:87-143.
25. Winter JS, Davidson E. Governance of artificial intelligence and personal health information. Digital Policy Regulation and Governance. 2019;21(3):280-90.

26. Lacobucci 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. 14 Nov 2018.
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;25(1):30-6.
29. CBC News. LifeLabs pays ransom after cyberattack exposes information of 15 million customers in B.C. and Ontario. 17 Dec 2019.
30. Hunter J. Privacy breach in B.C. health ministry led to freeze on medical research data. The Globe and Mail. 26 Apr 2016.
31. Solomon H. Cost of Canadian data breaches continues to rise, says study. IT World Canada. 11 Jul 2018.
32. University of California - Berkeley. Artificial intelligence advances threaten privacy of health data. EurekAlert! 3 Jan 2019.
33. Kolata G. Your data were ‘anonymized’? these scientists can still identify you. New York Times. 23 Jul 2019.
34. Hayden EC. Privacy loophole found in genetic databases. Nature News. 17 Jan 2013.
35. Z Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y. Identifying personal genomes by surname inference. Science. 2013; 339(6117):321-4.
36. 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;1(8):e186040.
37. Erlich Y, Shor T, Pe’er I, Carmi S. Identity inference of genomic data using long-range familial searches. Science. 2018;362(6415):690-4.
38. Ji S, Gu Q, Weng H, et al. De-health: all your online health information are belong to us. arXiv preprint arXiv:1902.00717. 2019.
39. Lubarsky B. Re-identification of “anonymized data”. Georgetown Law Technology Review. 2017;202-13.
40. McIntyre E. Health care professionals and the privacy rights of patients. Advocates’ Quarterly. 2015;43(4):428-47.
41. General Data Protection Regulation. 2016 0.J.
42. Health Insurance Portability and Accountability Act, 1996 Pub. L., c.104-191.
43. Personal Information Protection and Electronic Documents Act, SC 2000, c 5.
44. Office of the Privacy Commissioner of Canada. Provincial and territorial privacy laws and oversight. 2020.
45. Office of the Privacy Commissioner of Canada. Processing Personal Data Across Borders: Guidelines. 2009.
46. 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;8:85-98.
47. Minssen T, Gerke S, Aboy M, Price N, Cohen G. Regulatory responses to medical machine learning. Journal of Law and the Biosciences. 2020;7(1):lsaa002.
48. R v Dyment, 1988 2 SCR 417 at 428-429, aff’d R v Spencer 2014 SCC 43.
49. R v Tessling, 2004 SCC 67, citing A. F. Westin, Privacy and Freedom (1970).
50. 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.
51. Jones v Tsige, 2012 ONCA 32.
52. Oliveira v. Aviva Canada Inc. et al, 2017 ONSC 6161.
53. Hopkins v. Kay, 2015 ONCA 112
54. Jaremko JL, Azar M, Bromwich R, 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.
55. McInerney v. MacDonald, 1992 CanLII 57 (SCC), [1992] 2 SCR 138.
56. Nicholson Price II W, Gerke S, Cohen IG. Potential liability for physicians using artificial intelligence. JAMA. 2019;322(18):1765-6.
57. Nicholson Price II W. Medical malpractice and black-box medicine. In: Cohen IG, et al., editors. Big Data, Health Law, and Bioethics. Cambridge University Press; 2018.
58. Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council. Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS2); Dec 2018.
59. 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):164-71.