

Responsible Use of Artificial Intelligence in Health and Health Research

Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners and Ombuds with responsibility for privacy oversight
("FPT Privacy Regulators")

Adopted in Ottawa (Ontario) on September 15, 2026

Context

Escalating costs, aging populations, and a shortage of healthcare workers are challenging Canada's health systems and causing delays in access to services. Governments and healthcare providers are looking for solutions, including Artificial Intelligence systems (AI systems), to deliver efficient and high-quality care with limited resources.¹ Strong legal, privacy, and ethical safeguards are needed to realize the benefits of AI systems in health while avoiding violation of the privacy and other fundamental rights of individuals.

AI systems are generally defined as machine-based systems that undertake activities typically performed by humans and make inferences from the input they receive to generate outputs such as predictions, content, and recommendations or decisions.² AI systems in health can include purpose-built diagnostic and classification tools, as well as generative AI tools, such as chatbots and AI scribes. The life cycle of AI systems can span from design and development to procurement, deployment, use and monitoring, and eventual decommissioning. Throughout their life cycle, AI systems may be designed to learn from collected information, adjust to new input data, simulate intelligent behaviour, or automate decision-making.³ The tools may also be used to support the detection and diagnoses of medical conditions,⁴ be integrated into the delivery of health services,⁵ or be used as part of healthcare system optimization.⁶

AI systems are being widely developed and implemented at an unprecedented rate across Canada. The health sector must act now to ensure the ongoing protection of individuals' personal information and maintain patient trust in the system as a whole. Delaying adequate protections, accountability, and oversight at each stage of an AI system's life cycle could lead to significant consequences for individuals and groups, including:

1. **Unauthorized collections, uses, and disclosures of information:** AI systems may lead to unauthorized collections, uses and disclosures of personal information, including personal health information. A violation of an individual's privacy rights may occur, for example, when AI systems combine de-identified datasets with other information in a way that can reidentify individuals. Alternatively, AI systems may be trained on illegally sourced data, or their outputs may be commercialized or disclosed without authority.

Processing large quantities of information without having the necessary security protections in place may also leave the information susceptible to malicious events, including cyberattacks.

2. **Algorithmic bias, systemic discrimination, and patient harms:** As datasets are applied to new areas of clinical practice, factors such as bias and noise in input data, and misclassifications, can influence the accuracy of predictions or decisions made by AI systems.⁷ Inaccuracies can lead to false diagnoses and the development of ineffective or inappropriate treatment plans, putting the safety and health outcomes of patients at risk. This is especially the case for diverse and vulnerable populations with unique characteristics, such as ethnic minorities and other marginalized groups, who may not be well represented in the input data used to train the AI systems. These risks increase when characteristics linked to marginalization (e.g., race, gender, sexual orientation) intersect.

Canada's health system spans federal, provincial, and territorial jurisdictions and involves a range of interested parties from public and private sectors, including governments, AI developers and service providers, healthcare providers, and the health research community. Parties who design, develop, procure, adopt, deploy, and use AI systems, or who leverage the outputs of AI systems, must comply with all relevant laws and regulations, including parties who play multiple roles, such as a healthcare provider who develops their own AI system, or an AI developer who conducts their own health research.

Recalling

Recent resolutions that recognize the significant risks AI systems can have on the protection of the privacy rights of Canadians and the policy responses emerging both internationally and nationally, including:

1. The Organization of Economic Cooperation and Development: [Scaling Artificial Intelligence in Health](#), and [Health Data Governance for the Digital Age](#);
2. The Global Privacy Assembly, including the: [Resolution on meaningful human oversight of decisions involving AI systems](#), [Resolution on the collection, use and disclosure of personal data to pre-train, train and fine-tune AI models](#), and [Resolution on Generative Artificial Intelligence Systems](#);
3. Joint resolutions of FPT [Privacy] Regulators, including [Principles for responsible, trustworthy and privacy-protective generative AI technologies](#); and

4. Recent guidance of several [privacy regulators] across Canada, including Alberta's [Artificial Intelligence \(AI\) Scribe Privacy Impact Assessment Guidance](#) and guidance on [Responsible AI Governance in Alberta](#), Ontario's [Principles for the responsible use of artificial intelligence](#) and guidance on [AI Scribes: Key Considerations for the Health Sector](#), British Columbia's [PIPA and AI scribes: best practices for healthcare organizations in BC](#), and [Getting Ahead of the Curve: Meeting the challenges to privacy and fairness arising from the use of artificial intelligence in the public sector](#), cowritten by British Columbia and the Yukon Territory.

Therefore

Canada's FPT Privacy Regulators are committed to work together to raise awareness of the potential impacts of AI systems and to advance consistent principles for protecting the privacy and fundamental rights of Canadians. We call on all interested parties to play their part to enable the use of AI systems in a way that is privacy-protective, valid and reliable, safe, human rights affirming, transparent, and accountable throughout their entire life cycle.⁸ Accounting for these six principles is critical to maintaining public trust in the health sector and ensuring Canadians can benefit from innovation while continuing to receive trustworthy healthcare.

As FPT Privacy Regulators, we urge the following calls to action:

Federal, provincial, and territorial governments should:

1. Review, amend, or adopt relevant legislation and regulations that balances support for innovation with the need to ensure that AI systems in health are developed, procured, deployed, used, and decommissioned in a manner that meets the six core principles (privacy protective, valid and reliable, safe, human rights affirming, transparent, and accountable).
2. Consult meaningfully with the privacy regulator within their jurisdiction when developing legislative and regulatory frameworks to help ensure they enable the responsible collection, use, disclosure, and retention of personal information throughout the life cycle of AI systems in health.
3. Engage with the public frequently and transparently, including patient and family committees and impacted individuals and groups—particularly vulnerable persons from marginalized populations—to ensure that their rights and interests are accounted for in the development of trustworthy regulatory frameworks governing AI systems in health.
4. Legally require all relevant parties who develop, procure, and use AI systems in health to establish effective AI governance and accountability frameworks, based on robust risk assessments and commensurate mitigation measures.

AI system developers and service providers in health should:

1. Take a privacy-by-design approach when designing AI systems, which includes:
 - a) following data minimization principles;
 - b) using de-identified or synthetic data instead of directly or indirectly identifiable personal information, wherever possible, for any purpose that involves an AI system.
 - c) ensuring that they know the provenance of the information used to train each AI system and that the information is lawfully sourced;
 - d) building in appropriate controls to ensure each AI system only collects, uses, discloses, and retains personal information as permitted by privacy laws;
 - e) ensuring that the safeguards applied are proportionate to the quantity and sensitivity of information collected, used, disclosed, or retained by each AI system;
 - f) avoiding design practices that would influence, manipulate, or coerce users into making decisions that are contrary to their privacy interests;
 - g) ensuring privacy settings are the most protective by default and that security safeguards are established to proportionately protect the personal information that AI systems collect, use, disclose, or retain; and
 - h) enabling auditing capabilities and the ability to perform routine real-world testing to ensure that each AI system performs as intended.
 - i) reducing the potential of unfair bias and inaccurate outputs by ensuring that training data is accurate, representative, and complete, and by continually validating the AI system to prevent the adoption of biased computational models, enable mistake detection, and protect the safety of patients.⁹
 - j) Adopt a robust AI governance and accountability framework to cover the entire life cycle of the AI system, including human-in-the-loop oversight and a mechanism for clients and their end-users to be able to challenge AI outputs.
2. Conduct ongoing privacy, security, and AI-specific assessments throughout the life cycle of each AI system to identify and mitigate risks as they emerge, and ensure these mitigation measures are commensurate with the levels and severity of the risks identified.
3. Provide clients with evidence of how the AI system is trained and a general explanation of how the AI system works and uses information, including the factors, sources, and assessments it relied upon to inform its decision or approach.
4. Demonstrate to the client that the use of the AI system complies with the relevant privacy law.

5. Share ongoing risk assessment findings with clients and inform them of any mitigations they should apply downstream to prevent outputs that undermine the six core principles.

Healthcare providers who procure, adopt, and use AI systems should:

1. Ensure that their governance and institutional policies and procedures for the collection, use, disclosure, and retention of personal information in connection with AI systems comply with the privacy laws applicable to the jurisdiction within which they operate.
2. When consent is required by applicable privacy laws, ensure that individuals receive clear and meaningful communications about how their personal information would be collected, used, and disclosed in connection with the AI systems; and where practicable, offer the choice to opt out prior to the deployment of an AI system.
3. Designate a contact person with whom individuals or groups can discuss their concerns pertaining to the use of their information by AI systems, or raise objections to such use, and enable a practical and accessible means by which they can challenge any consequential decisions or inferences made.
4. Limit the amount of personal information collected, used, disclosed, and retained in connection with AI systems to that which is necessary for their designated purpose and as may otherwise be permitted by law.
5. Consider the results of privacy, security, and AI-specific assessments of prospective AI system developers or service providers. The potential for an AI system to result in breaches, inaccuracies, bias, discrimination, and other harms observed in the outputs should inform the decision of whether an AI system is adopted.
6. Adopt and keep up-to-date an AI system risk management framework, ensuring ongoing monitoring and assessment of risks across an organization's AI systems throughout their life cycles, and integrate this framework within broader risk management frameworks. AI system risks should be considered with other related program risks, and may also inform other governance instruments such as privacy impact assessments, threat risk assessments, or other types of assessments.
7. Exercise utmost diligence when contracting and sub-contracting with third parties for AI systems and ensure the contracts executed include provisions that enable compliance with all applicable laws, regulations, and policies. Contracts should address obligations for privacy and security training, record keeping, auditing, and limits imposed on the particular uses and disclosures of information, including prohibiting a contractor or sub-contractor's unauthorized commercialization or disclosure of information.

8. Provide clear and easy-to-comprehend explanations for individuals on how their information is collected, used, disclosed, and retained in connection with an AI system and how they may exercise their privacy and access rights associated with this activity.
9. Train staff on the appropriate use of AI systems and take the necessary measures to prevent the use of AI systems without approval or oversight (“shadow AI”), for example, a hospital employee who uses their own personally procured AI system that does not comply with the policies and procedures of the hospital.¹⁰
10. Ensure appropriate human oversight and verification of AI-enabled systems’ outputs, including through human-in-the-loop review, to assess the validity and reliability of outputs throughout an AI system’s life cycle, prevent the occurrence of outputs that are inaccurate, discriminatory, unfairly biased, or harmful, and to mitigate where necessary.

Canada's health research community should consider the following:

1. The Panel on Research Ethics and Canada’s three federal research funding agencies – the Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council, should update their guidelines and policies, including the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (TCPS 2) to reflect the new realities of AI and AI-assisted research in health, and provide health researchers with clear guidance on how to assess and navigate AI-specific challenges or complexities in a manner fit for purpose. This may include providing more granular guidance on how to mitigate the risks of re-identifying an individual when de-identified, anonymized, and/or synthetic data is used by an AI system; or how to reduce bias that may result from the absence of research participants who demonstrate unique characteristics or are part of diverse and vulnerable populations.
2. The Panel on Research Ethics, Canada’s three federal research funding agencies, the Canadian Association of Research Ethics Boards, and institutions that establish, fund, and directly oversee research ethics boards (REBs) such as universities, hospitals, and public agencies, should strengthen the governance, support, and capacity of REBs across the country through appropriate levels of resources and education for REB members to effectively oversee the ethics of AI and AI-assisted research, including privacy and confidentiality aspects, in the context of health.

3. In assessing AI research or AI assisted research projects in health, Research Ethics Boards should ensure that they have the requisite capacity to address the legal, social, and ethical dimensions of AI research and technologies, including on privacy. REBs should also carry out the necessary due diligence by requiring persuasive demonstration that the expected benefits to study participants, their communities, or society as a whole outweigh risks to participants' and how these risks will be mitigated.
4. Researchers should:
 - a) Refine their assessments of risks and benefits to individuals and groups whose personal information is being used as part of the AI system or AI-assisted research or will be otherwise impacted by the research.
 - b) Be transparent and publicly share the outcomes of AI research or AI-assisted research in the health context.

As FPT Privacy Regulators we will continue to take the following actions, within the scope of our respective mandates:

1. Call for trustworthy AI governance frameworks in the form of clear legislation and regulations across the country, which are robust and account for the need to enable innovation in health while respecting privacy and other fundamental rights.
2. Take steps to ensure governments, health AI system developers and service providers, health providers and the health research community comply with relevant privacy laws, regulations and policies in our respective jurisdictions.
3. Coordinate, to the extent possible, regulatory action across federal, provincial and territorial jurisdictions, to ensure fair, consistent and equitable privacy protections of individuals and groups across Canada.
4. Educate the health sector, through guidance and awareness activities, about the privacy principles needed to ensure a responsible approach is taken to mitigate the risks and potential harms associated with the collection, use, disclosure, and retention of personal information throughout the entire life cycle of an AI system.
5. Inform the public how to exercise their privacy rights respecting the manner in which their personal information is collected, used, disclosed, and retained in connection with AI systems in health.

¹ "The Role of AI in Hospitals and Clinics: Transforming Healthcare in the 21st Century" (March 29, 2024): <https://pmc.ncbi.nlm.nih.gov/articles/PMC11047988/>

² OECD Definition: <https://oecd.ai/en/work/ai-system-definition-update>; Office of the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission. "Principles for the responsible use of artificial intelligence" (January 21, 2026): <https://www.ipc.on.ca/en/resources/principles-responsible-use-artificial-intelligence>; and Ontario's *Enhancing Digital Security and Trust Act* (EDSTA): <https://www.ontario.ca/laws/statute/24e24>

³ IAPP Definition: <https://iapp.org/resources/ai-governance-glossary>

⁴ “The Impact of Artificial Intelligence in the Medical Field” (November 10, 2025):

<https://scienceinsights.org/the-impact-of-artificial-intelligence-in-the-medical-field/>

⁵ “Artificial intelligence in healthcare: transforming the practice of medicine” (July 2021):

<https://pmc.ncbi.nlm.nih.gov/articles/PMC8285156/>; and “The Role of AI in Hospitals and Clinics:

Transforming Healthcare in the 21st Century” (March 29, 2024):

<https://pmc.ncbi.nlm.nih.gov/articles/PMC11047988/>

⁶ The UK Health Security Agency. “How we are pioneering artificial intelligence applications in public health”

(March 14, 2025): [https://ukhsa.blog.gov.uk/2025/03/14/how-we-are-pioneering-artificial-intelligence-](https://ukhsa.blog.gov.uk/2025/03/14/how-we-are-pioneering-artificial-intelligence-applications-in-public-health/)

[applications-in-public-health/](https://ukhsa.blog.gov.uk/2025/03/14/how-we-are-pioneering-artificial-intelligence-applications-in-public-health/); and

⁷ “Harnessing Artificial Intelligence for Health”: [https://www.who.int/teams/digital-health-and-](https://www.who.int/teams/digital-health-and-innovation/harnessing-artificial-intelligence-for-health)

[innovation/harnessing-artificial-intelligence-for-health](https://www.who.int/teams/digital-health-and-innovation/harnessing-artificial-intelligence-for-health) .

⁸ “Office of the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission.

“Principles for the responsible use of artificial intelligence” (January 21, 2026):

<https://www.ipc.on.ca/en/resources/principles-responsible-use-artificial-intelligence> .

⁹ “Bias in AI: What It Is, How It Happens & What to Do About It” (November 10, 2025):

<https://www.sciencenewstoday.org/bias-in-ai-what-it-is-how-it-happens-what-to-do-about-it>

¹⁰ Office of the Information and Privacy Commissioner of Ontario. “AI Scribes: Key Considerations for the

Health Sector” (January 28, 2026): [https://www.ipc.on.ca/en/resources/ai-scribes-key-considerations-health-](https://www.ipc.on.ca/en/resources/ai-scribes-key-considerations-health-sector)
[sector](https://www.ipc.on.ca/en/resources/ai-scribes-key-considerations-health-sector).