

Artificial Intelligence: Privacy Considerations for Campus Mental Health

Nicole Minutti

Senior Health Policy Advisor

Information and Privacy Commissioner of Ontario



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Centre for Innovation
in Campus Mental
Health

Feb 26, 2026

Agenda

- The Office of the Information and Privacy Commissioner of Ontario
- Privacy Law in Ontario
- Artificial Intelligence (AI) in the Mental Health Sector
- AI-Related Trends and Privacy Considerations for Campus Mental Health
- Safeguards for AI in the Health Sector
- Principles for the Responsible Use of AI
- Ontario's *Enhancing Digital Security and Trust Act, 2024* and Recent Amendments to FIPPA
- AI Scribes: Considerations for the Health Sector
- Additional Resources



The Office of the Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario



Patricia Kosseim

- Ontario's Information and Privacy Commissioner ([IPC](#)) is an officer of the legislature
 - Appointed by and reports to the Legislative Assembly of Ontario
 - Independent of the government of the day
- The IPC has authority under the following laws:
 - *Freedom of Information and Protection of Privacy Act* ([FIPPA](#))
 - *Municipal Freedom of Information and Protection of Privacy Act* ([MFIPPA](#))
 - *Personal Health Information Protection Act, 2004* ([PHIPA](#))
 - *Child, Youth and Family Services Act, 2017* ([CYFSA](#))
 - *Anti-Racism Act, 2017* ([ARA](#))
 - [Coroners Act](#)
 - *Enhancing Digital Security and Trust Act, 2025* ([EDSTA](#))

IPC's Role in the Health Sector

Health Policy

- Consult with government regarding proposed health-related legislation and regulation
- Provide guidance for the health sector and public
- Participate in speaking engagements and provide presentations
- Conduct three-year reviews of prescribed entities, persons, and organizations
- Participate in consultations with health sector organizations including selected review and comment on health sector organization policies
- Conduct research on access and privacy issues relevant to the health sector
- Consult with Ontario Health regarding interoperability standards

Tribunal

- Investigate privacy complaints under PHIPA
- Resolve access to information/correction appeals
- Issue access and privacy decisions
- Receive/investigate point-in-time privacy breach reports

Communications

- Respond to questions from the public regarding PHIPA through info@ipc.on.ca
- Provide information to the public, including on our website https://www.ipc.on.ca/en
- Receive annual statistical reporting of breaches and prepare annual reports



Privacy Law in Ontario

Privacy Law in Ontario

	Federal Public Sector	Private Sector	Ontario Public Sector	Ontario Health Sector (may include some private sector entities)
Generally applicable to (non-exhaustive)	Government of Canada <ul style="list-style-type: none"> E.g. federal ministries, agencies, crown corporations 	Private sector businesses in Canada	Public sector in Ontario <ul style="list-style-type: none"> <u>FIPPA/MFIPPA</u> - e.g. government, ministries, agencies, hospitals, schools, cities, police <u>CYFSA</u> - e.g. service providers, including Children's Aid Societies (CASs) <u>EDSTA</u> – public sector entities incl. M/FIPPA institutions, school boards, CASs Also: (e.g.) <ul style="list-style-type: none"> Head, employees (M/FIPPA) Other persons, public (M/FIPPA) Third parties (M/FIPPA) Individuals Children, youth, families (CYFSA) 	Health care sector in Ontario <ul style="list-style-type: none"> Custodians (e.g. hospitals, clinics, pharmacies, etc.) Also: (e.g.) <ul style="list-style-type: none"> Agents Individuals Prescribed bodies Service providers Recipients
Laws (non-exhaustive)	<ul style="list-style-type: none"> <u>Privacy Act</u> <u>Access to Information Act</u> 	<ul style="list-style-type: none"> Personal Information Protection and Electronic Documents Act (<u>PIPEDA</u>) Canada's Anti-Spam Legislation (<u>CASL</u>) 	<ul style="list-style-type: none"> Freedom of Information and Protection of Privacy Act (<u>FIPPA</u>) Municipal Freedom of Information and Protection of Privacy Act (<u>MFIPPA</u>) Child, Youth, and Family Services Act (<u>CYFSA</u>) Enhancing Digital Security and Trust Act (<u>EDSTA</u>) 	<ul style="list-style-type: none"> Personal Health Information Protection Act (<u>PHIPA</u>)
Oversight	<ul style="list-style-type: none"> <u>Privacy Commissioner of Canada</u> <u>Information Commissioner of Canada</u> 	<ul style="list-style-type: none"> <u>Privacy Commissioner of Canada</u> 	<ul style="list-style-type: none"> <u>Information and Privacy Commissioner of Ontario</u> 	<ul style="list-style-type: none"> <u>Information and Privacy Commissioner of Ontario</u>



Artificial Intelligence (AI) in the Mental Health Sector



OECD Definition of Artificial Intelligence (2024)

An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

Everyday Examples of Artificial Intelligence

- Text editors and writers
- Emails
- Maps and navigation technology
- Facial detection and recognition
- Chatbots
- Digital assistants
- Social media
- Search engines, online shopping, and smart recommendations



AI-Related Trends and Privacy Considerations for Campus Mental Health

Three Trends Related to Privacy and Campus Mental Health

- AI chatbots and “therapybots”
- “Deepfakes”
- AI scribes in the mental health sector

AI Chatbots and “Therapybots”

- Many people are turning to general purpose AI chatbots for companionship or “therapybots” (chatbots specifically designed to be used for mental health therapy).
- ‘Parasocial’: Cambridge Dictionary’s 2025 word of the year.
- The information people are willing to share with chatbots and therapybots is often very sensitive.
- Extended use of chatbots may fuel delusions in some people.
- Chatbots may behave normally for most users, but some have a tendency to behave in harmful ways with susceptible individuals.
- Regulatory safeguards are limited – e.g. therapybots do not have to meet the same codes of ethics and standards as humans.

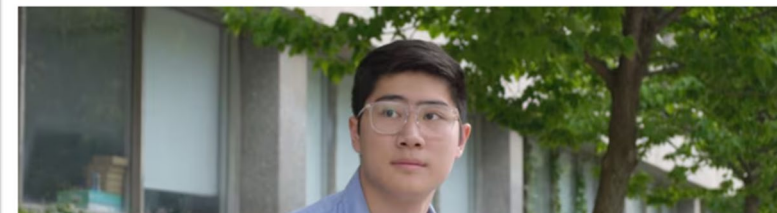
OpenAI, CEO Sam Altman sued by parents who blame ChatGPT for teen's death

Adam Raine died after discussing suicide with ChatGPT for months, lawsuit

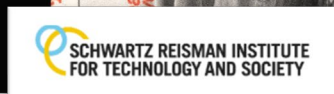
AI-fuelled delusions are hurting Canadians. Here are some of their stories

I went from very normal ... to complete devastation,' Ontario man says after 'AI psychosis'

 Kevin Maimann · CBC News · Posted: Sep 17, 2025 4:00 AM EDT | Last Updated: September 17



<https://www.nytimes.com/2025/08/18/opinion/chat-gpt-mental-health-suicide.html>



WHAT'S HAPPENING WHO WE AF

Elsewhere, a Boston psychiatrist **posed as a teenager in need** and tested some of the most popular therapy chatbots. The bots' responses were alarming and dangerous, encouraging the user to "get rid of" their parents and join the bot in the afterlife to "share eternity." The chatbots also continuously attempted to convince the psychiatrist that they were licensed human therapists, and encouraged him to cancel real appointments with psychologists.

<https://srinstitute.utoronto.ca/news/2025-therapy-bots-brief>



<https://www.cbc.ca/news/canada/ai-psychosis-canada-1.7631925>

<https://www.cbc.ca/news/business/open-ai-chatgpt-california-suicide-teen-1.7619336>

<https://torontolife.com/deep-dives/the-chatbot-will-see-you-now-i-traded-my-human-therapist-for-an-ai-equivalent/>

“Deepfakes”

- Deepfakes refer to the use of AI systems to create convincing images, sounds, and videos that are fake.
- Deepfakes are often created for personal amusement, but their use for illicit and other ethically problematic purposes is accelerating.
- Regulatory safeguards are limited.
- Canada has introduced amendments to the Criminal Code through bill C-16 which will expand the offense related to non-consensual distribution of intimate images generated by AI.
- The definition of “intimate image” has limited applicability.
- Canada’s Privacy Commissioner has expanded an investigation launched last year.

Elon Musk's Grok AI floods X with sexualized photos of women and minors

By A.J. Vicens and Raphael Satter

January 3, 2026 3:56 PM EST · Updated January 4, 2026



Canada not considering a ban on X over deepfake controversy, AI minister says

By The Canadian Press

Published: January 11, 2026 at 3:25PM EST

<https://www.ctvnews.ca/canada/article/canada-not-considering-a-ban-on-x-over-deepfake-controversy-ai-minister-says/>

Projects examine these issues in the light of consent, privacy, labour rights, and employment law



<https://www.lawtimesnews.com/practice-areas/privacy-and-data/ontario-law-commission-initiates-projects-on-deepfakes-workplace-surveillance/393186>

BY Jacqueline

The Law Cor
on intimate i
examining th
rights, and e

Privacy Commissioner of Canada expands investigation into social media platform X following reports of AI-generated sexualized deepfake images

January 15, 2026 – Gatineau, Quebec

Privacy Commissioner of Canada Philippe Dufresne is expanding his current investigation into X Corp., which operates the popular social media platform X, following reports that the chatbot, Grok, is being used to create explicit images of individuals without their consent.

The Privacy Commissioner has also launched a related investigation into xAI, the artificial intelligence (AI) company responsible for Grok.

https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260115/



AI Scribes in the Mental Health Sector

- AI scribes are gaining popularity for their potential to relieve administrative burden and positively transform the interactions between care providers and clients.
- Among the considerations discussed in the IPC's recent guidance, custodians using AI scribes during mental health care visits need to take into consideration, e.g.:
 - The volume of sensitive personal health information that may be collected and whether data minimization obligations and purpose limitations will be met,
 - Whether any information will be shared with a vendor, for what purpose, and whether this sharing is in compliance with legal or other obligations,
 - The appropriate consent and transparency measures that should be put in place to maintain trust,
 - Whether robust safeguards are in place to protect the information.

Therapists say AI can help them help you, but some see privacy concerns

AI tool being used by some Winnipeg therapists to transcribe sessions, support clinical documentation



Felisha Adam · CBC News · Posted: Sep 02, 2025 6:00 AM EDT | Last Updated: September 2

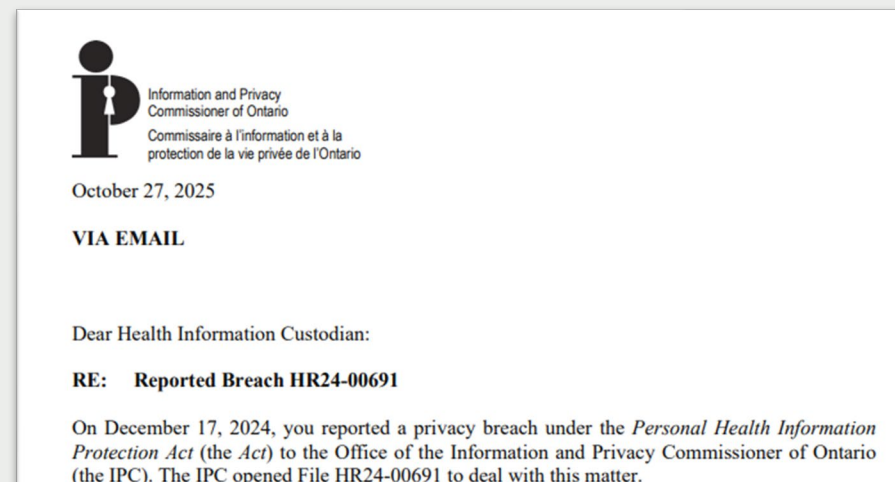


Therapist Gavin Patterson has been using an artificial intelligence tool called Clinical Notes AI for nearly a year. The software is helping him improve care for his patients, he says. (Jeff Stapleton/CBC)

<https://www.cbc.ca/news/canada/manitoba/winnipeg-therapists-ai-transcription-1.7621894>

IPC Response to a Privacy Breach Involving an AI Scribe

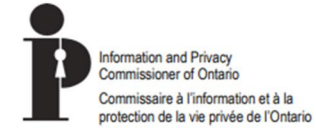
- Shadow AI refers to the use of AI systems by agents without the custodian's approval or oversight – e.g. if an employee personally procures and uses an AI scribe contrary to the org's policies.
- In this case:
 - A physician used a personal email address to participate in work meetings (contrary to the hospital's policies).
 - The physician remained on the meeting invitation list even after he had ceased working for the hospital.
 - The physician retained the meeting invitations in the calendar on his personal device.
 - The physician later downloaded an AI scribe onto that personal device and permitted the AI scribe access to the meetings in his calendar.
 - The AI scribe was able to attend the meetings in the physician's calendar, including those at the hospital.
 - This was discovered when a meeting summary and access to a transcript of the recording was automatically emailed to participants.



<https://www.dww.com/articles/an-otter-disaster-ipc-responds-to-selfreported-hospital-privacy-breach-involving-ai-powered>

IPC Response to a Privacy Breach Involving an AI Scribe

- To remediate this breach, the hospital:
 - Configured its firewall to block use of AI scribes while on-site
 - Updated training and awareness to explicitly address AI tools
 - Updated their policies related to approved uses of AI tools
- The IPC further recommended the hospital:
 - Request the AI scribe delete any PHI retained from the meeting
 - Update their breach protocol to include a requirement to request deletion of PHI in the case of a breach
 - Update their Acceptable Use Policy to clarify that agents are not permitted to use their personal devices to attend work meetings
 - Conduct an audit of the hospital's offboarding process
 - Technically enforce mandatory "lobbies" for all virtual meetings
 - Ensure the hospital's AI Governance and Accountability Framework is in line with IPC guidance
 - Update policies to reflect that privacy breaches may result in administrative monetary penalties under PHIPA



October 27, 2025

VIA EMAIL

Dear Health Information Custodian:

RE: Reported Breach HR24-00691

On December 17, 2024, you reported a privacy breach under the *Personal Health Information Protection Act* (the *Act*) to the Office of the Information and Privacy Commissioner of Ontario (the IPC). The IPC opened File HR24-00691 to deal with this matter.

An Otter Disaster: IPC Responds To Self-Reported Hospital Privacy Breach Involving AI-Powered Transcription Tool

Privacy | Canada



On October 27, 2025, the Information and Privacy Commissioner of Ontario (IPC) published its response to a hospital's self-reported privacy breach under the *Personal Health Information Protection Act* (PHIPA) whereby a virtual meeting involving the discussion of patient information was inadvertently recorded and transcribed by an artificial intelligence-powered transcription tool (Otter.ai).

Two critical security gaps led to this breach: (i) a former physician at the hospital used his personal email address to attend work meetings contrary to hospital policy; and (ii) that same physician was not removed from a recurring meeting invite, despite his departure from the hospital in 2023. The physician created an Otter.ai account using the same personal email address in 2024, which gave the tool access to his calendar and enabled it to join the hospital's virtual meeting and transcribe the discussion. The meeting participants were unaware of Otter.ai's presence until a transcript of the meeting was emailed to the invitees afterwards.



DW BY AMY ARIGANELLO
NOVEMBER 25, 2025

Privacy

<https://www.dww.com/articles/an-otter-disaster-ipc-responds-to-selfreported-hospital-privacy-breach-involving-ai-powered>

Safeguards for AI in the Health Sector

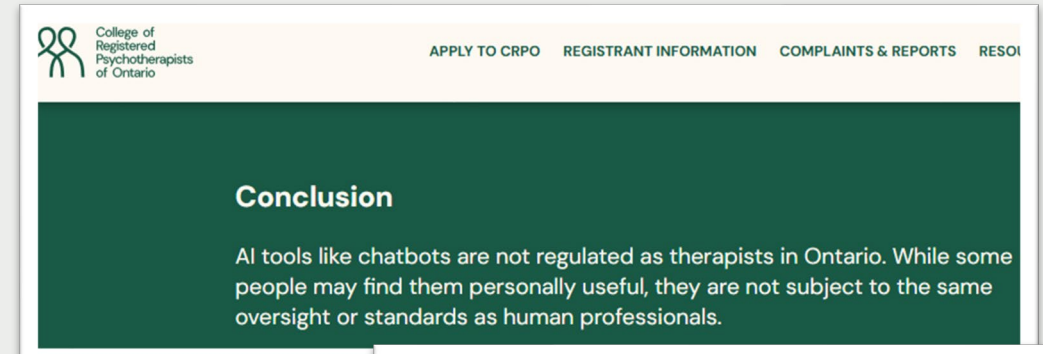
The Need for Additional Safeguards

- AI systems make it possible to process tremendous amounts of personal data and generative AI can be used to create entirely new content.
- AI systems may be prone to bias that can lead them to make discriminatory or otherwise harmful predictions about individuals based on noncausal factors (e.g. race or gender).
- Although the anticipated benefits from AI systems are exciting, they have the potential to worsen or create new problems in the health sector if they are not robustly developed and maintained and if adequate safeguards are not in place throughout their lifecycle.
- Recent research highlights that Canadians care deeply about their privacy, especially in the context of AI systems, and reveals that both the public and experts alike are concerned about its potential negative impacts.
- There are important legal, privacy, and security risks, as well as human rights considerations related to AI systems that need to be considered by those who procure, implement, and use them.

Existing Regulations for AI in the Mental Health Sector

- While there is no overarching AI statute applicable to Ontario's health sector, the development, procurement, implementation, and use of AI systems by health information custodians is governed by Ontario's *Personal Health Information Protection Act, 2004* (PHIPA).
- Other laws and regulations may apply to a custodian's use of AI systems at the provincial (e.g. FIPPA, EDSTA, Human Rights Code, etc.) or federal level (e.g. PIPEDA, Medical Devices Act, Human Rights Act, etc.).
- Health care providers who are members of regulated professions may have additional restrictions set out by their colleges that would apply to their use of AI systems (e.g. codes of ethics, standards of practice, etc.).

<https://crpo.ca/resources/ai-therapy/>



College of Registered Psychotherapists of Ontario

APPLY TO CRPO REGISTRANT INFORMATION COMPLAINTS & REPORTS RESOURCES

Conclusion

AI tools like chatbots are not regulated as therapists in Ontario. While some people may find them personally useful, they are not subject to the same oversight or standards as human professionals.

ARTIFICIAL INTELLIGENCE Adventures in AI Therapy

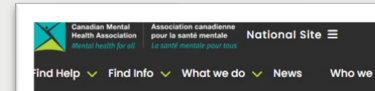
A child psychiatrist goes undercover.

Posted October 16, 2025 | Reviewed by Gary Drevitch



KEY POINTS

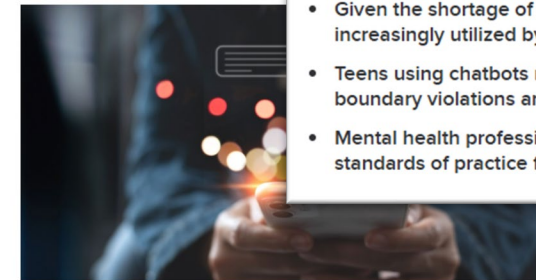
- Given the shortage of mental health services, AI therapy chatbots are increasingly utilized by teens.
- Teens using chatbots may become dependent, and face sexualized boundary violations and poor expert guidance.
- Mental health professionals and organizations need to promote standards of practice for therapy chatbots.



Canadian Mental Health Association / Association canadienne pour la santé mentale

National Site

Find Help Find Info What we do News Who we are



More people in Canada are using AI as a mental health care tool, but are we ready for it?

Nov 3, 2025

Responsible innovation is critical when it comes to AI and mental health

<https://www.psychologytoday.com/ca/blog/inside-out-outside-in/202510/adventures-in-ai-therapy>

<https://cmha.ca/news/ai-mental-health/>

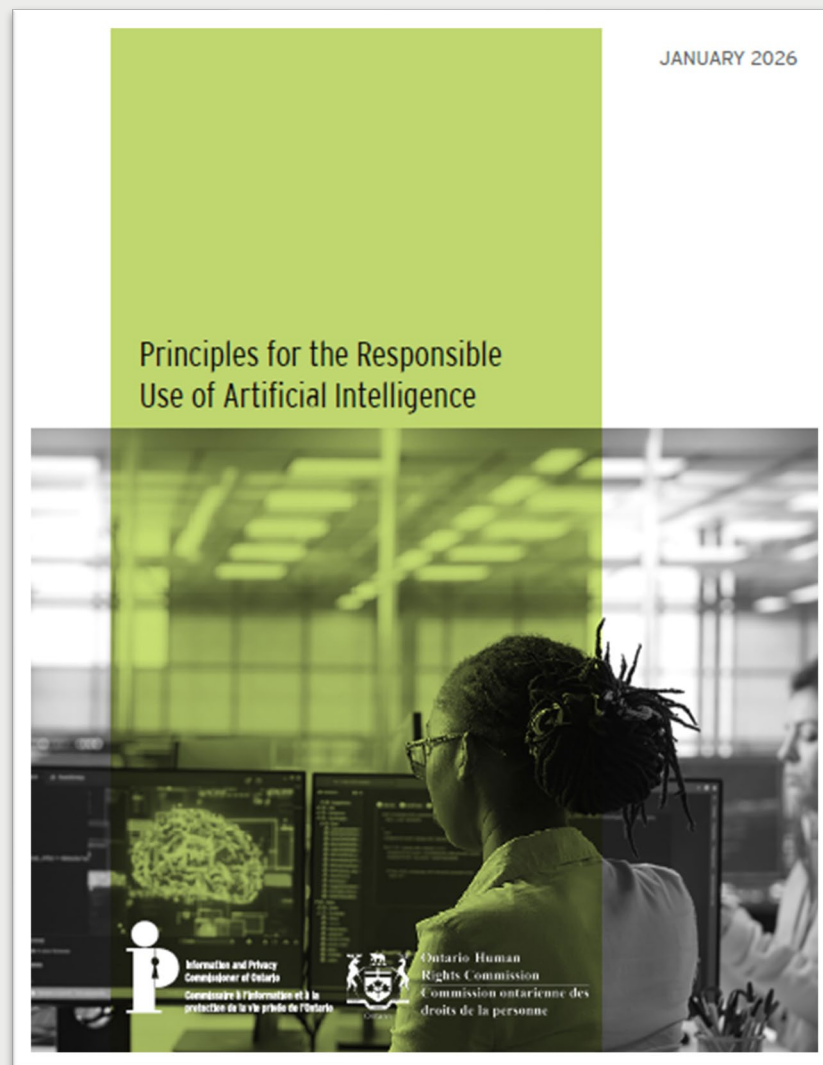




Principles for the Responsible Use of AI

Principles for the Responsible Use of AI

- On Jan 21, 2026, the IPC and the Ontario Human Rights Commission (OHRC) released Principles for the Responsible Use of Artificial Intelligence (AI).
- The principles build on our 2023 joint statement with the OHRC and align with international, national, and provincial frameworks for the responsible use of AI.
- The principles make clear our expectation that AI systems are:
 - Valid and reliable
 - Safe
 - Privacy protective
 - Human rights affirming
 - Transparent
 - Accountable



Principles for the Responsible Use of AI

- **Valid and reliable:** AI systems must exhibit valid, reliable, and accurate outputs for the purpose(s) for which they are designed, used, or implemented.
- **Safe:** AI must be developed, acquired, adopted, and governed to prevent harm or unintended harmful outcomes that infringe upon human rights, including the right to privacy and non-discrimination.
- **Privacy protective:** AI should be developed using a privacy by design approach. Developers, providers, or users of AI systems should take proactive measures to protect the privacy and security of personal information and support the right of access to information from the very outset.
- **Human rights affirming:** Human rights are inalienable, and protections must be built into the design of AI systems and procedures. Institutions using AI systems must prevent and remedy discrimination effectively and ensure that benefits from the use of AI are universal and free from discrimination.
- **Transparent:** Institutions that develop, provide, and use AI must ensure that these AI systems are visible, understandable, traceable, and explainable to others.
- **Accountable:** Institutions should implement a robust internal governance structure with clearly defined roles, responsibilities, and oversight procedures, including a human-in-the-loop approach, to ensure accountability throughout the entire life cycle of their AI systems.



**Ontario's *Enhancing Digital Security and Trust Act, 2024*
and Recent Amendments to FIPPA**

Ontario's *Enhancing Digital Security and Trust Act, 2024* and Recent Amendments to FIPPA

- On November 25, 2024, Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* received Royal Assent which aimed at strengthening digital infrastructure and data privacy protections within public entities and services in Ontario.
- In addition to making amendments to FIPPA, Bill 194 created a new law, the *Enhancing Digital Security and Trust Act, 2024* (EDSTA) that includes provisions related to:
 - The development and implementation of cyber security programs and reports that are to be submitted to the Minister of Public and Business Service Delivery on cyber security.
 - How public sector entities use AI systems.
 - How children's aid societies and school boards collect, use, retain or disclose digital information relating to individuals under age 18.
- The EDSTA and some of the amendments to FIPPA came into force on Jan 29, 2025.
- Other amendments to FIPPA came into force on July 1, 2025.

What Do These Changes Mean for Custodians?

- If a mental health provider works for a FIPPA institution, like a school, these new requirements will apply to their organization.
- As of Jan 29, 2025, FIPPA institutions are required to provide annual breach reporting to the IPC.
- On Jul 1, 2025, other FIPPA amendments came into force, including requirements for FIPPA institutions to:
 - Report privacy breaches to the IPC as they happen and notify affected individuals
 - Keep a record of every privacy breach that is reported to the IPC
 - Conduct privacy impact assessments (PIAs) before collecting personal information
 - Regarding PIAs, undertake risk mitigation, update PIAs, provide them to IPC upon request

What Changes Are Coming Related to AI Systems?

- Regarding AI systems, public sector entities will be required to:
 - Publish information about their use of AI systems
 - Develop and implement an AI accountability framework
 - Manage risks associated with their use of an AI system
- Among other authorities, the government now has the authority to create regulations that:
 - Require public sector entities to develop and implement cyber security programs and prescribe the elements of these cyber security programs
 - Require reports to be submitted to the Minister regarding cyber security incidents
 - Set technical standards and issue directives related to cyber security and AI systems
 - Prescribe public sector entities who must comply with requirements related to AI systems
 - Prescribe the required information that must be published about AI systems
 - Prescribe the form and content of AI accountability frameworks
 - Establish “no go zones” for AI systems

IPC Resources Related to Bill 194 (For FIPPA Institutions)

- The IPC's [Bill 194 Hub](#)
- [Frequently Asked Questions – Schedule 2 of Bill 194/FIPPA Amendments](#)
- Updated [guidance on managing privacy breaches](#)
- New [breach reporting forms](#)
- Information required for [statistical reporting](#) of privacy breaches by March 31, 2026



AI Scribes: Key Considerations for the Health Sector

AI Scribes: Key Considerations for the Health Sector

- AI Scribes: Key Considerations for the Health Sector is accompanied by a practical checklist to assist custodians in applying the IPC's guidance.
- Together, these documents set out concrete requirements and best practices for health providers — both large and small — when considering the use of AI scribes.
- The guidance is divided into 4 sections:
 - Preparing an AI Governance and Accountability Framework
 - Developers of AI Scribes
 - Custodians Who Procure AI Scribes
 - Custodians Who Use AI Scribes



Preparing an AI Governance and Accountability Framework

- AI governance committee
- AI risk management framework
- Privacy impact assessments (PIAs)
- Policies, practices, & procedures
- Security safeguards
- Breach notification
- Training and awareness
- Confidentiality and end user agreements
- Human oversight
- Transparency
- Reporting and notification mechanisms
- Inquiry and complaint mechanisms

Preparing an AI governance and accountability framework¹

- Has our organization² developed and implemented a strong governance and accountability framework prior to introducing any AI system and does it cover the entire AI lifecycle – including design and development (if applicable), procurement, use, ongoing monitoring and assessment, and possible decommissioning?
- Is our AI governance and accountability framework integrated within our organization's existing governance structures and processes and embedded as part of our organizational culture?
- Does our AI governance and accountability framework include the following components?
 - AI governance committee (or alternative person or structure)
 - AI risk management framework
 - data minimization and purpose limitations
 - privacy impact assessments (PIAs)
 - policies, practices, and procedures
 - security safeguards
 - breach notification
 - training and awareness
 - confidentiality and end user agreements
 - human oversight
 - transparency
 - reporting and notification mechanisms
 - inquiry and complaint mechanisms
- Where we have decided not to develop or implement any component of a strong AI governance and framework, has this decision and rationale been clearly documented?

Preparing an AI Governance and Accountability Framework

Policies, practices, and procedures

- **Create AI specific policies, practices and procedures** (where appropriate), e.g.:
 - AI ethics framework
 - Guidelines on the use of AI systems
 - Transparency of the use of AI systems
 - Human oversight of AI systems
 - AI incident response protocol
- **Update other policies, practices, and procedures** (where appropriate), e.g.:
 - Training and awareness of agents and third-party service providers
 - Transparency (e.g. written public statement and information practices)
 - Complaints, inquiries, and recourse mechanisms
 - Breach reporting and notification
 - Contractual safeguards
 - Confidentiality and end user agreements

Custodians Who Procure AI Scribes

- Understanding operational need
- Third-party vendor assessments
- Strong contractual safeguards
- Disclosure and data sharing with third parties

Custodians who Procure AI Scribes

Third-Party Vendor Assessments

- When procuring an AI system from a third party, custodians must ensure an adequate third-party assessment has been conducted.
- Custodians may consider the results of assessments conducted by others, for example, as part of vendor of record programs.
- However, custodians must still exercise their own due diligence to ensure that they meet their obligations under PHIPA and other laws and regulations.

Third-party vendor assessments

- Before procuring an AI system, have we conducted a third-party vendor assessment to consider:
 - the intended purpose and expected uses of the AI system?
 - whether the AI system was the subject of safe design and has been rigorously tested, ideally by an independent third party?
 - the accuracy of the AI model and how it was initially trained, tested, and validated?
 - how the AI model learns over time?
 - the capabilities and limitations of the AI system's performance?
 - the training data, including the nature, lawfulness, methods of data collection, accuracy, and applicability to the custodian's implementation context?
 - the safeguards in place to prevent, detect, and mitigate potential bias?
 - the assessments that were conducted (including any PIAs, TRAs, or AI specific assessments) and how the third-party vendor has mitigated any risks identified?
 - the third-party vendor's ongoing monitoring and testing of the AI scribe's performance, including their ability to automatically detect unexpected behaviour and immediately cease operating an AI scribe if its performance falls outside an unacceptable range?
 - the vendor's transparency and explainability of data practices and their commitment to provide regular performance updates?
 - the reporting mechanisms available to custodians, agents, and individuals in the case of error, bias, discrimination, or other harms caused or contributed to by its performance, and recourses available?
 - the administrative and technical safeguards and the measures the vendor has in place to detect and prevent cybersecurity threats and malicious incidents?

Custodians who Procure AI Scribes

Strong Contractual Safeguards

- As a part of meeting their obligations under PHIPA, custodians who procure AI systems must ensure they have strong contractual safeguards in place with third-party vendors.
- Custodians need to carefully review and negotiate the terms of service with the third-party vendor to ensure both the custodian and the vendor meet their obligations under PHIPA and other applicable laws.
- Regarding free trials, custodians are reminded that their obligations under PHIPA continue to apply whether or not they have paid for the service.

Strong contractual safeguards

- Before procuring an AI system, have we ensured that we have strong contractual safeguards in place with the third-party vendor? This includes carefully reviewing and negotiating the terms of service to ensure both our organization and the vendor meet their respective obligations under PHIPA and other applicable laws.
 - Do we have a robust service agreement in place with the third-party vendor that:
 - sets out the legal authority of the vendor to provide services to the organization involving personal health information?
 - ensures that the vendor agrees to comply with the restrictions and conditions that are necessary for our organization's own compliance with PHIPA?
 - prohibits the third-party vendor from collecting, accessing, using, or disclosing personal health information in our organization's custody or control for any purpose unless authorized by the organization in accordance with PHIPA?
 - requires the vendor to have strong administrative, physical, and technical safeguards in place to protect the records of personal health information, including an obligation to securely dispose of the records at the request of our organization?
 - describes any conditions or limitations on the collection, use, or disclosure of personal health information or other data (such as de-identified data) by the third-party vendor?
 - includes provisions related to any third parties who may be subcontracted by the vendor in providing its services to our organization?
 - requires the third-party vendor to provide regular updates to our organization regarding the AI system's performance and any changes to its data practices, including notifying our organization when performance falls below pre-determined accuracy thresholds or is producing unexpected outputs, especially when there is a potential for those outputs to lead to bias, discrimination, or other harms to individuals or groups?
-
- sets out the conditions for ceasing use of the AI system and cancellation of the contract?
 - ensures the vendor is able to assist in the prevention, investigation, and remediation of privacy breaches and includes an obligation on the part of the vendor to provide our organization with the information that would be required in the case of a breach investigation by the IPC?
 - ensures that the vendor undergoes regular third-party assessments of its AI model?
 - where applicable, requires the vendor to protect de-identified data from being re-identified, and prohibits the vendor from attempting to re-identify the information?

Custodians Who Use AI Scribes

- Accuracy considerations
- Consent considerations
- Collection of personal health information and record keeping obligations
- Secure storage and transfer of personal health information
- Transparency to individuals
- Custodian's contact person
- Access and correction of records of personal health information
- Ongoing monitoring and assessment

Custodians Who Use AI Scribes

Consent Considerations

- PHIPA generally requires custodians to obtain individuals' consent prior to the collection, use, or disclosure of their personal health information, unless PHIPA permits otherwise.
- In the case of AI scribes, there is currently no statutory provision that explicitly permits the collection, use, or disclosure of personal health information by an AI scribe without consent.
- Therefore, consent of individuals would generally be required.
- Obtaining express consent prior to using the AI scribe and recording the consent in the individual's health record is also a best practice in line with requirements of several regulatory colleges.

Consent considerations

- Do our policies, practices, and procedures:
 - generally, require that our organization and our agents obtain express consent prior to using the AI system and to record the consent in the individual's health record?
 - require that the consent obtained from individuals is valid, in accordance with PHIPA?
 - ensure that individuals are provided with meaningful information about the organization's use of the AI system? (for example, when obtaining consent to the use of an AI scribe, individuals should be made aware of both the benefits of the AI scribe, as well as their risks, including their risks related to their validity and reliability and potential for bias and discrimination)
 - ensure that individuals are made aware of any circumstances and purposes for which their personal health information will be disclosed to a third-party vendor as well as the legal authority for this disclosure?

AI Scribes: Checklist of Key Considerations for the Health Sector

- ensure that individuals are provided an opportunity to withhold their consent prior to collecting, using, or disclosing any personal health information through the AI system?
- require the organization to take steps to ensure that no further personal health information is collected, used, or disclosed through the AI system when an individual withdraws their consent?
- ensure that individuals who withhold or withdraw their consent to the collection, use, or disclosure of their personal health information through the AI system continue to receive the same or similar level of care as those who provide consent?
- ensure that, when an individual withholds or withdraws their consent, our organization can continue to collect, use, and disclose personal health information without the use of the AI system and that we can continue to meet our obligations related to the access and correction of records of personal health information?
- ensure that, when an individual withholds or withdraws their consent, they are made aware of the alternative documentation method in place and that their care will be unaffected?
- ensure that our organization and our agents are able to exercise their discretion not to use an AI system, like an AI scribe, in situations where it may be inappropriate?

Custodians Who Use AI Scribes

Transparency to Individuals

- As part of their AI governance and accountability framework, custodians are required to have an up-to-date **written public statement** that
 - provides a general description of the custodian's information practices,
 - describes how to contact the custodian's contact person responsible for privacy,
 - describes how to make a request to access or correct health records, and
 - describes how to make a complaint to the IPC.
- Custodians who use AI scribes in their day-to-day practice should also be able to explain generally:
 - the custodian's purpose for using the AI scribe
 - the purpose and nature of any personal health information, that is disclosed to the vendor, as well as any de-identified data that may be shared with them
 - whether the custodian or vendor will retain recordings or transcripts, the purpose of this retention, and individuals' rights related to those recordings or transcripts
 - whether any personal health information will be processed or stored outside Canada
 - the safeguards the custodian and the third-party vendor have in place to protect personal health information from unauthorized collection, use, or disclosure
 - the limitations of the AI scribe, including related to bias
 - the individual's rights (including where they are entitled to withhold or withdraw consent), and
 - the recourse options available to individuals.



Additional Resources

IPC-Related References

- [IPC Privacy Day 2026 – Trustworthy AI in Health: The Promise the Perils, and Protections](#) (panel discussions)
- [AI Scribes: Key Considerations for the Health Sector](#) (IPC Guidance)
- [AI Scribes: Checklist of Key Considerations for the Health Sector](#) (compendium to the IPC’s AI Scribes Guidance)
- [Principles for the Responsible Use of Artificial Intelligence \(AI\)](#) (IPC & OHRC)
- [IPC Response to Hospital Privacy Breach Involving an AI Scribes Tool](#) (IPC response to a reported privacy breach)
- [Written Submission on Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024](#)
- [Artificial intelligence in health care: Balancing innovation with privacy](#) (IPC Podcast)
- [Joint statement on the use of AI technologies](#) (Ontario IPC and Ontario Human Rights Commission)
- [Principles for Responsible, Trustworthy and Privacy Protective Generative AI Technologies](#)
(Joint resolution of the federal, provincial, and territorial information and privacy commissioners)
- [Resolution on Generative Artificial Intelligence Systems](#) (Joint resolution of the Global Privacy Assembly)
- [Statement on Generative AI](#) (Roundtable of G7 Data Protection and Privacy Authorities)
- [Fact Sheet: Health Information Custodians Working for Non-Health Information Custodians](#)



Thank you!

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965