Privacy Considerations for AI in the Health Sector

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

aIPHa Workshop – Artificial Intelligence (AI) and Public Health

Nov 6, 2024

Agenda

- The Office of the Information and Privacy Commissioner of Ontario
- The Personal Health Information Protection Act, 2024 (PHIPA)
- Duties of Custodians and their Agents under PHIPA
- Bill 194: *Strengthening Cyber Security and Building Trust in the Public Sector Act*
- Privacy Considerations for AI in the Health Sector

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*

IPC's Overall Role & Mandate

In addition to overseeing provincial access and privacy laws, the IPC also serves the government, public institutions, and the public through its mandate to:

- Resolve appeals when access to information is refused
- Investigate privacy complaints related to personal information
- Ensure compliance with the province's access and privacy laws
- Review privacy policies and information management practices
- Conduct research on access and privacy issues and provide comment on proposed legislation and government programs
- Educate the public, media and other interested parties about Ontario's access and privacy laws and current issues affecting access and privacy

IPC'S VISION

Enhance Ontarians' trust that their access and privacy rights will be respected by ...

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

The Personal Health Information Protection Act, 2004

Application of PHIPA

- Ontario's *Personal Health Information Protection Act* (PHIPA) sets out rules for the collection, use and disclosure of personal health information (PHI) by health information custodians (custodians).
- PHIPA applies to PHI in the custody or control of:
  - Custodians
  - Agents of custodians

Personal Health Information

- PHI is identifying information about an individual in oral or recorded form that:
  - Relates to an individual's physical or mental health
  - Relates to the provision of health care to the individual
  - Is a plan that sets out the home and community care services to be provided by a funded health service provider or Ontario Health Team
  - Relates to payments or eligibility for health care
  - Relates to the donation of body parts or bodily substances
  - Is the individual's health number
  - Identifies an individual's substitute decision-maker

Health Information Custodians

- Custodians include:
  - Health care practitioners who provides health care
  - Group practices of health care practitioners who provide health care
  - Health service providers that are part of an Ontario Health Team and that provide a funded home and community care service
  - Hospitals, psychiatric facilities and independent health facilities
  - Long-term care homes, retirement homes and homes for special care
  - Pharmacies, ambulance services, labs and specimen collection centres
  - Centres, programs, or services for community health or mental health whose primary purpose is the provision of health care
  - Medical Officers of Health of a board of health *(public health units)*
  - Minister/Ministry of Health

Agents

- A person that, with the authorization of a custodian, acts for or on behalf of the custodian in respect of PHI.
- Custodians remain responsible for any PHI that is collected, used, disclosed, retained or disposed of by their agents.

Electronic Service Providers

- An electronic service provider (ESP) is a person who supplies services that enable a custodian to collect, use, modify, disclose, retain or dispose of PHI electronically.
- ESPs must comply with prescribed requirements.
- When the ESP is not an agent of the custodian:
  - It shall not use any PHI to which it has access, except as necessary in the course of providing the service.
  - It shall not disclose the PHI.
  - It shall not permit any person acting on its behalf to access the information unless the person complies with the restrictions that apply to the ESP.

Duties of Custodians and their Agents

Duties of Custodians and their Agents

- Custodians have a number of duties under PHIPA which generally fall into four categories:
  - Collection, use and disclosure
  - Access and correction
  - Transparency
  - Security
- These duties continue to apply when custodians develop, maintain, procure, implement, and use artificial intelligence (AI) technologies.

Collection, Use and Disclosure

Under PHIPA, custodians are not permitted to collect, use or disclose PHI unless:

- The individual consents, or
- The collection, use or disclosure is permitted or required by PHIPA.

Custodians are also responsible for taking steps to ensure that they have the authority to collect, use, and disclose PHI.

PHIPA's "Limiting Principles"

- Custodians are not permitted to collect, use or disclose PHI if other information will serve the purpose.
- Custodians are not permitted to collect, use or disclose more PHI than is reasonably necessary for the purpose.

Access and Correction

Access

- Individuals have a right of access to their health records with some exceptions.
- Custodians must respond within 30 days (with the possibility of a 30-day extension).

Correction

- Individuals may request correction of their health records.
- Custodians must respond within 30 days.
- If the individual shows it is not accurate, custodians must correct the record unless:
  - It was not originally created by the custodian, and they do not have sufficient expertise, knowledge or authority to correct the record; or
  - It consists of professional opinion or observation that was made in good faith.

Transparency

Contact Person

- Custodians must designate a contact person responsible for:
  - Facilitating their compliance with PHIPA
  - Ensuring all agents are appropriately informed of their duties under PHIPA
  - Responding to inquiries from the public about their information practices
  - Responding to requests for access to or correction of health records, and
  - Receiving complaints from the public about their compliance with PHIPA.

Cont'd

Transparency

Written Public Statement

- Custodians must make available to the public a written statement that:
  - Provides a general description of their information practices
  - Describes how to contact the contact person
  - Describes how to obtain access to or request correction of a health record, and
  - Describes how to make a complaint to the custodian and to the Commissioner.
- If a custodian uses or discloses PHI without consent, outside the scope of the information practices described in the written public statement, the custodian must inform affected individuals at the first reasonable opportunity.

Transparency

Breach Notification to Affected Individuals

- If PHI is stolen, lost, used or disclosed without authority, custodians must:
  - Notify individuals at the first reasonable opportunity, and
  - Inform the individuals, in the notice, that they are entitled to make a complaint to the IPC.

Point-in-Time Breach Reporting to IPC

- Custodians must notify the IPC of a breach, when it is discovered, in certain circumstances (e.g. when PHI has been used or disclosed without authority, PHI has been stolen, etc).

Annual Statistical Reporting to IPC

- In addition to the point-in-time reporting requirements, custodians are required to report breaches to the IPC on an annual basis.

Security

- Custodians must take reasonable steps to ensure that PHI is protected against theft, loss and unauthorized collection, use or disclosure, unauthorized copying, modification, or disposal.
- Custodians are also required to ensure that records of PHI in their custody or control are retained, transferred, and disposed of in a secure manner.

Selected IPC Guidance

- Safeguarding Personal Health Information
- The Secure Transfer of Personal Health Information
- Secure Destruction of Personal Health Information
- Encrypting Personal Health Information on Mobile Devices
- Privacy and Security Considerations for Virtual Health Visits
- Health Requirements for Strong Encryption
- Communicating Personal Health Information by Email
- Detecting and Deterring Unauthorized Access to Personal Health Information
- What to Do When Faced with a Privacy Breach: Guidelines for the Health Sector
- Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act

Bill 194: “*Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*”

Bill 194

- The Ontario government has introduced Bill 194, the "*Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*" aimed at strengthening digital infrastructure and data privacy protections within public entities and services in Ontario.
- The draft legislation includes provisions and regulation making authority related to:
  - The development and implementation of cyber security programs and reports that would 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.
  - Increasing the authority of the IPC to investigate and respond to privacy breaches and inappropriate use of personal data.

IPC's Submission on Bill 194

"The legislation, as drafted, would establish significant regulation-making powers in respect of cyber security, AI systems, and digital technologies affecting individuals under the age of 18.

The IPC agrees that these areas of societal activity pose high risk to Ontarians' privacy and human rights and require urgent government intervention.

However, as currently worded, Schedule 1 of Bill 194 lacks the statutory protections needed to protect with privacy and human rights and fails to provide the level of transparency and accountability that are necessary to secure Ontarians' trust in how the government will effectively govern these high-risk areas."

https://www.ipc.on.ca/en/resources/ipc-comments-bill-194-strengthening-cyber-security-and-building-trust-public-sector-act

IPC's Recommendations in its Submission on Bill 194

General recommendations for Schedule 1 *(Enhancing Digital Security and Trust Act, 2024)*

1. Include a purpose clause at the outset of the Act.
2. Make the act subject to independent oversight and enforcement.
3. Make the production of regulations under the act subject to public consultations.
4. Require the minister to consult with the IPC prior to making (or proposing) regulations or issuing directives that may impact privacy or access rights.
5. Make ministerial directives transparent to the public.
6. Include a whistleblower protection provision.

Recommendations specific to the cyber security portion of Schedule 1

7. Explicitly set out the core elements of a cyber security program.
8. Require notification of the IPC when cyber security incidents affect personal information.
9. Require the Minister to prepare an annual report on its cyber related responsibilities.

Cont'd

IPC's Recommendations in its submission on Bill 194

Recommendations specific to the AI portion of Schedule 1

10. Codify fundamental AI principles and guardrails into the statute.
11. Adopt a risk-based regulatory approach for AI.
12. Specify no-go zones.

Recommendations specific to digital technologies affecting children

13. Strengthen protections for children under existing privacy laws (instead of under Bill 194).
14. Expand the application of ministerial directives and regulations related to technical standards to cover all service providers under the Child Youth and Family Services Act.

“No-Go Zones”

Article 5: Prohibited AI Practices within the EU AI Act

Subliminal techniques

AI systems should not be made available that would use subliminal techniques to influence user consciousness or distort their ability to make an informed decision.

Exploitation of a vulnerability

AI systems should not be made available to exploit the vulnerability of a person or groups of people (e.g. by age, disability, socio-economic situation) or association with a group in a way that may cause harm to those people or groups.

Social evaluation

AI systems should not be made available whose purpose is to evaluate or classify a person or group of people (e.g. produce a social score), based on real, inferred or predicted behaviour or characteristics, that would lead to unfavourable treatment unrelated to the contexts in which the data was originally generated or disproportionate to their social behaviour.

Risk assessment

AI systems should not be made available whose purpose is to make risk assessments related to the likelihood that a person will commit a criminal offense based solely on the AI system’s profiling.

https://artificialintelligenceact.eu/article/5/

“No-Go Zones”

Article 5: Prohibited AI Practices within the EU AI Act

Facial recognition

AI systems should not be made available whose purpose is to create and expand facial recognition databases through the untargeted scraping of facial images using the internet or CCTV footage.

Employee emotions

AI systems should not be made available whose purpose is to assess the emotions of people in a workplace or educational institutions.

Biometric categorization

AI systems should not be made available whose purpose is to use biometric information to categorize people in order to determine their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation.

Real-time remote biometric identification by law enforcement

AI systems should not be made available whose purpose is to put real-time remote biometric identification systems in use for law enforcement, with some exceptions and conditions.

https://artificialintelligenceact.eu/article/5/

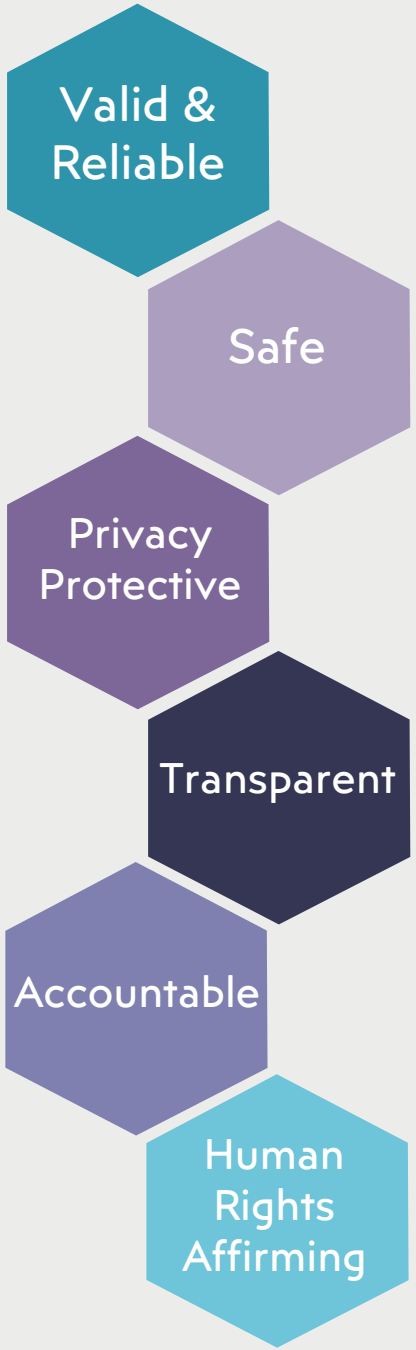
Cont'd

IPC's Recommendations in its submission on Bill 194

Recommendations specific to Schedule 2 *(FIPPA)*

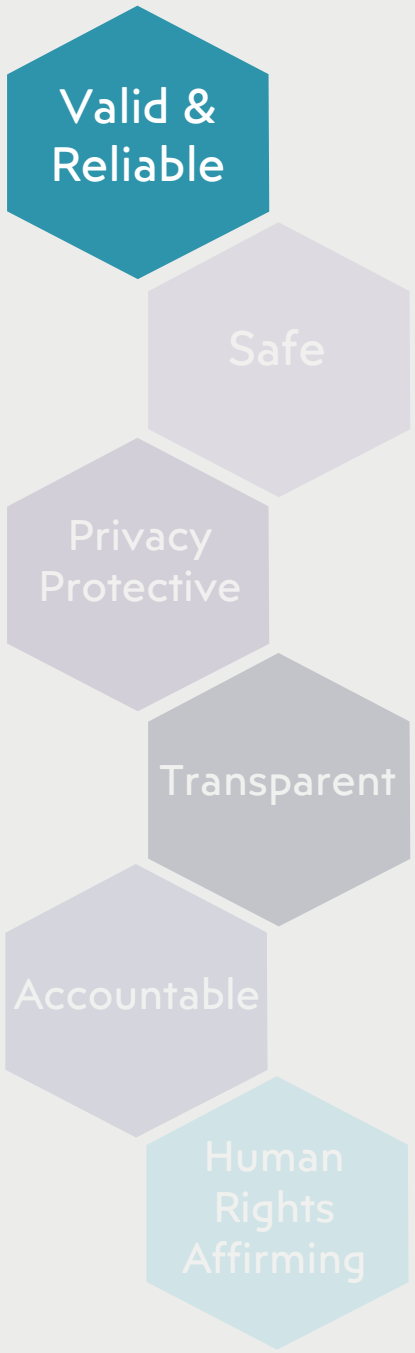
15. Introduce data minimization principles.
16. and 17. Strengthen privacy impact assessment requirements.
18. Broaden the grounds for individuals to bring complaints to the IPC.
19. Broaden scope of IPC's investigative powers.
20. Enable IPC to disclose information, as necessary.
21. Include a recipient rule.
22. and 23. Deem children's information as sensitive.
24. and 25. Protect whistleblowers from employer reprisal.
26. Remove expanded powers for ServiceOntario from FIPPA.
27. Include a mandatory statutory review period.
28. Make equivalent amendments to MFIPPA.

Privacy Considerations for AI in the Health Sector



Principles for the Development and Deployment of AI Technologies

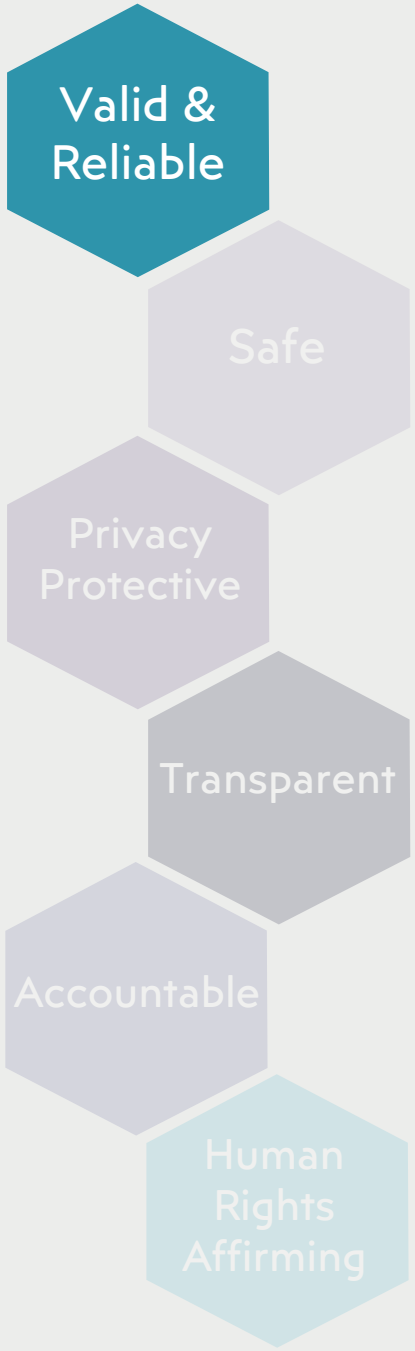
- *From the IPC's submission on Bill 194*
- There are many sets of principles related to AI that have been developed worldwide - across these we can see universal principles emerging.
- At a fundamental level, public sector entities developing or deploying AI systems must ensure that such systems are:
    - Valid and reliable
    - Safe
    - Privacy protective
    - Transparent
    - Accountable
    - Human rights affirming



Valid and Reliable

- Before AI technologies are adopted by public sector entities, the technologies should have to meet independent testing standards for validity and reliability.
- Any tested technologies should demonstrably work as intended in the environments in which they will be used.

From the IPC's submission on Bill 194

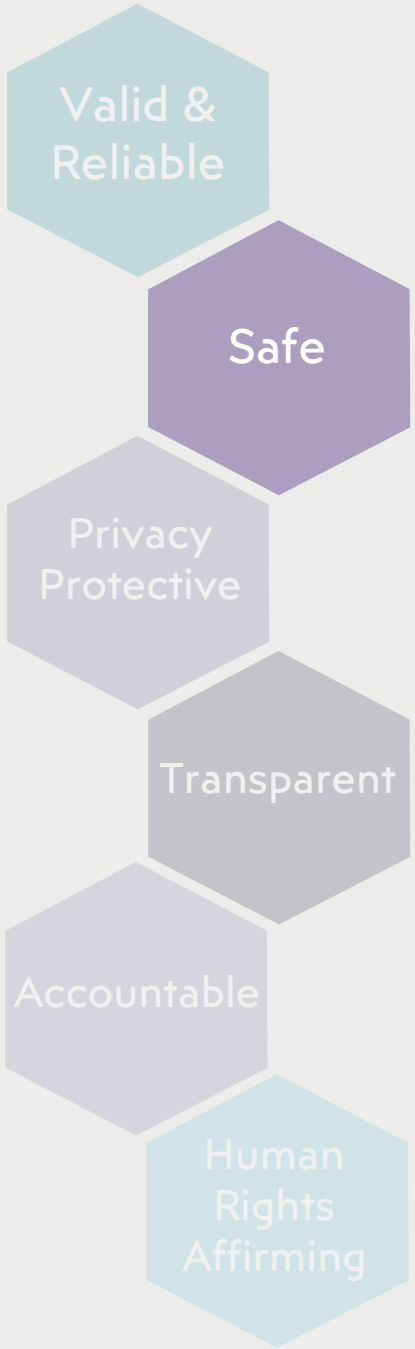


Valid and Reliable

Some considerations for the health sector

Cont'd

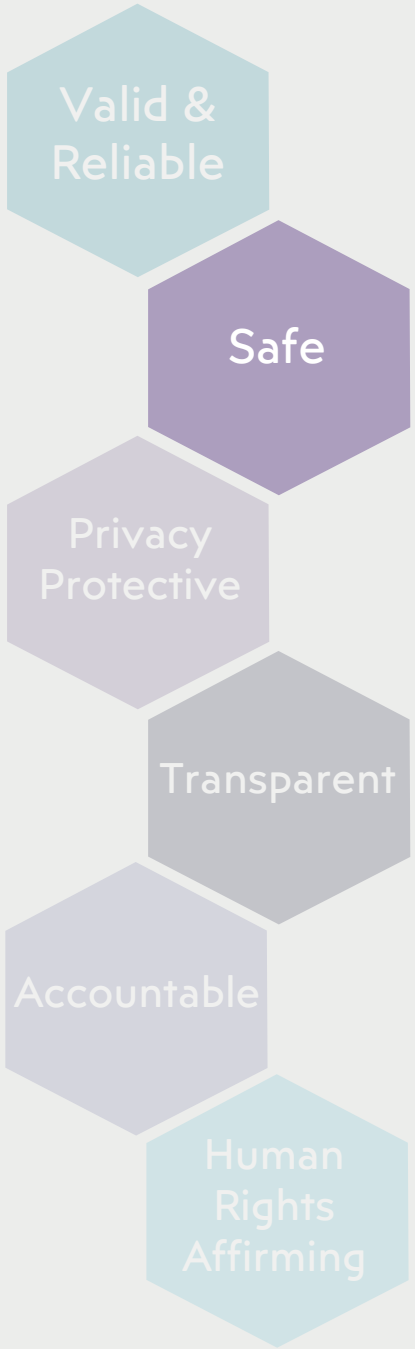
- What testing has been conducted to ensure the validity and reliability of the AI model?
- Was the testing conducted by a trusted third-party?
- How often will the model be re-evaluated?
- How accurate, up-to-date, and relevant is the AI model and the data it was trained on?
- What steps has the custodian taken to ensure that the AI model's outputs are regularly checked for accuracy?
- How will custodians be notified when the AI model's performance falls below certain thresholds?
- What policies, procedures, and practices does the custodian have in place to ensure that the AI model's outputs are checked for accuracy before any records of PHI created or altered by an AI model are used or disclosed?



Safe

- AI technologies should be configured to support human life, physical and mental health, economic security, and the environment.
- They should be monitored and evaluated throughout their lifespan to confirm they continue to support these objectives and can withstand unexpected events or deliberate efforts that cause them to behave in harmful ways not intended or anticipated by the developers, operators, or users of these AI systems.

From the IPC's submission on Bill 194

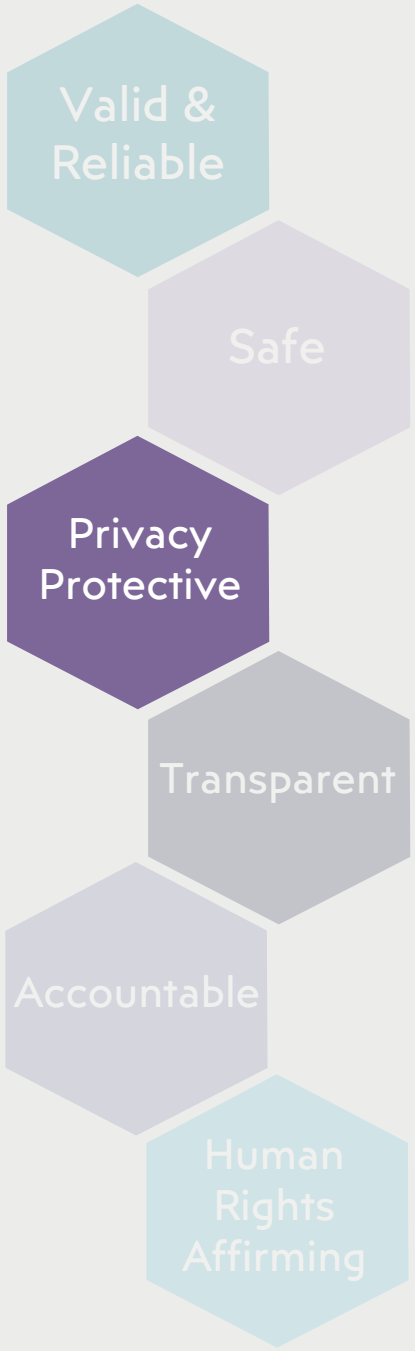


Safe

Some considerations for the health sector

Cont'd

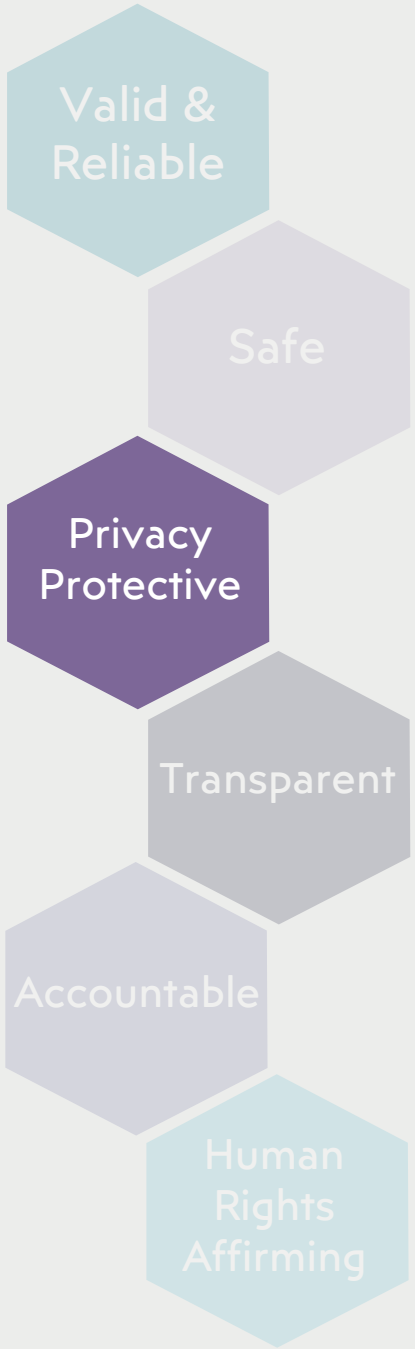
- What policies, procedures, and practices are in place to ensure ongoing monitoring and testing of the AI model to ensure ongoing safety?
- What mechanisms are in place to flag inaccuracies (including hallucinations) and potential biases to the custodian and developer?
- What sort of "circuit breaker" mechanisms are in place that would stop the AI model from operating and/or flag when it is producing unexpected and potentially harmful outputs?
- What steps has the custodian taken to ensure that sufficient security protections are in place to prevent unauthorized collection, use, or disclosure of PHI?
- What steps has the custodian taken to ensure that sufficient protections are in place to ensure that records of PHI are securely retained, transferred and disposed of when using AI technologies?
- What steps has the custodian taken to protect PHI from unauthorized collection, use, or disclosure through the use of the AI technology?



Privacy Protective

- AI technologies should be developed or adopted using a privacy by design approach that anticipates and mitigates privacy risks to individuals and groups.
- This means, among other things, requiring clear lawful authority to collect, process, retain, and use personal data in relation to AI systems, including training data.
- Systems must build in measures to ensure the accuracy of AI outputs and protect all inferences about individuals resulting from these outputs that are about individuals as personal information.
- AI systems must also be designed to protect the security of personal information from unauthorized access or cyber security threats.
- Individuals should be informed of the intended use of AI technology to process their personal information and, where appropriate, have an opportunity to opt-out of an automated decision in preference for a human decision maker.

From the IPC's submission on Bill 194

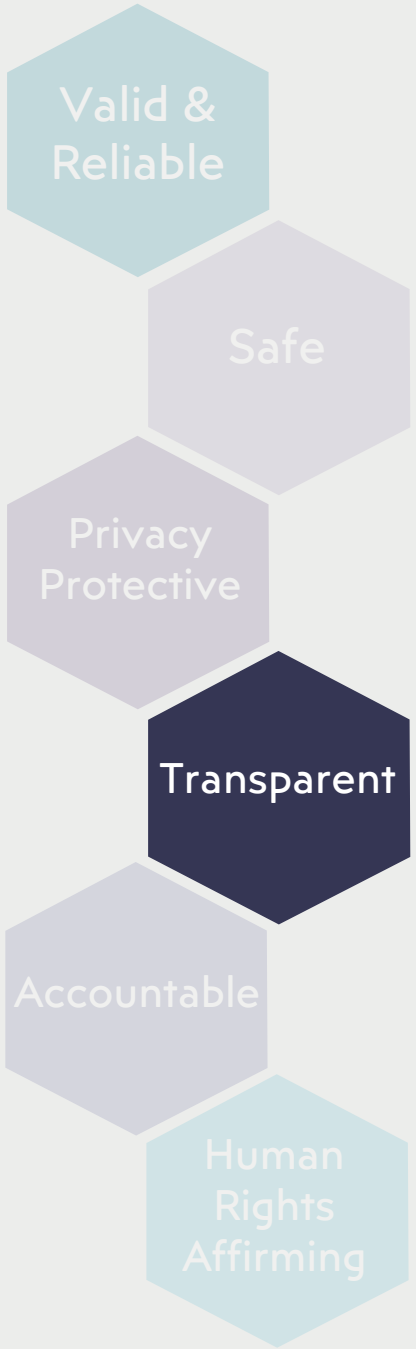


Privacy Protective

Some considerations for the health sector

Cont'd

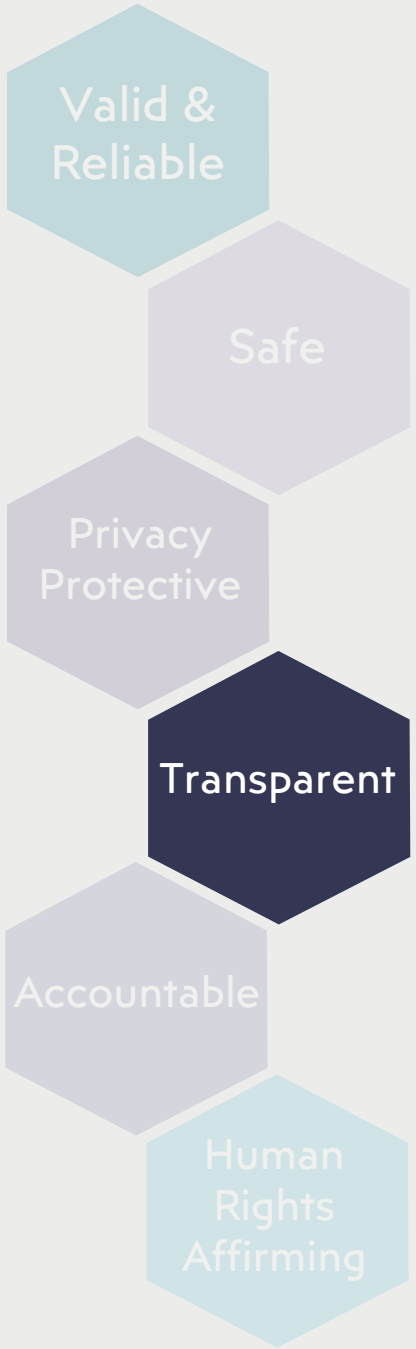
- What steps has the custodian taken to ensure that they have the authority to collect, use, and disclose PHI through the AI technology?
- What steps has the custodian taken to ensure that the underlying data used to develop and train the AI model has been obtained lawfully?
- What steps has the custodian taken to ensure that they are adhering to PHIPA's limiting principles when developing, maintaining, procuring, implementing and using an AI technology?
- What policies, procedures, and practices are in place to ensure that individuals are meaningfully informed of the use of an AI technology by the custodian and are given an opportunity to withhold or withdraw their consent prior to the collection, use, or disclosure of their PHI through the use of an AI technology?
- What technical and administrative measures are in place to ensure that the custodian is able to fulfill their obligations in providing individuals with access to and correction of records of their PHI that are generated or altered by an AI technology?



Transparent

- Public sector entities should adopt policies and practices that make visible, explainable, and understandable how AI technologies work.
- As part of this, public sector entities should retain sufficient technical information about the AI technologies they use so they can provide a full accounting of how decisions are reached.
- Individuals should be informed of decisions that have been made about them using AI.
- They should be told when they are interacting with an AI technology and when information presented to them has been generated by AI systems.
- The level of transparency by public sector entities may vary depending on whether it is directed to the public, individuals or groups directly impacted by AI systems, or regulators charged with overseeing them.

From the IPC's submission on Bill 194

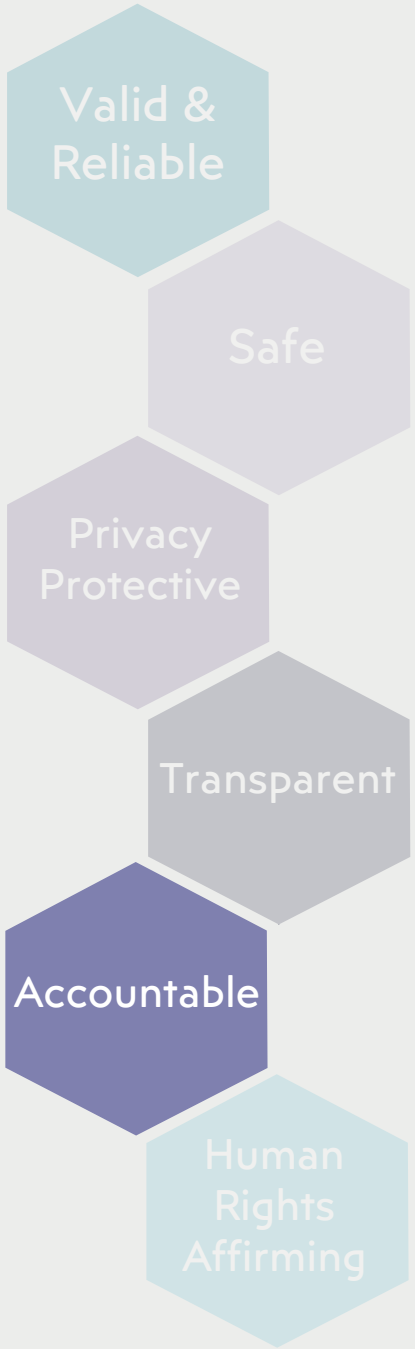


Transparent

Some considerations for the health sector

Cont'd

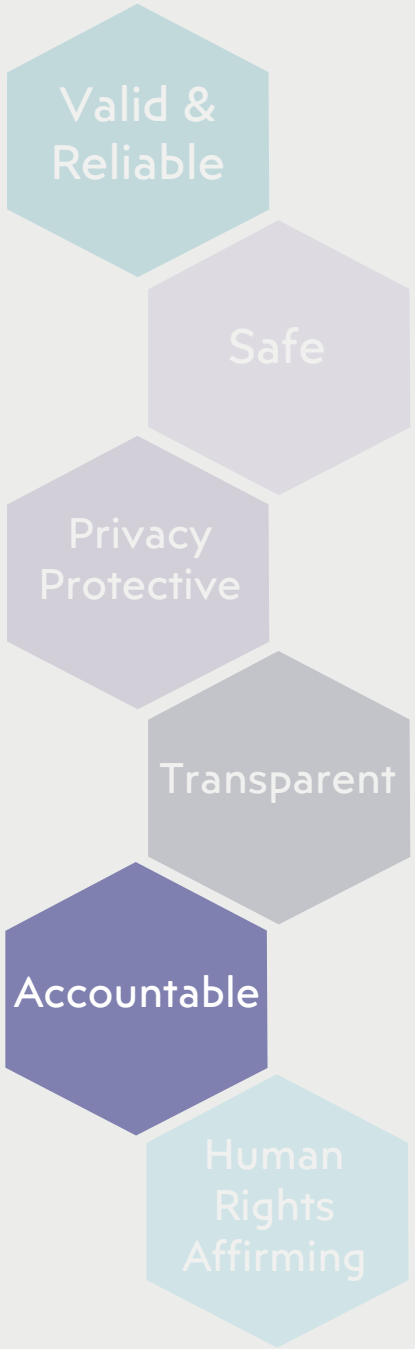
- What policies, procedures and practices does the custodian have in place to make visible, explainable, and understandable how the AI technology works?
- What mechanisms are in place to ensure that individuals are able to understand when and what records of their PHI have been generated or altered by an AI technology or what decisions have been made about them using an AI technology?
- Is the custodian's contact person adequately prepared to meet their responsibilities under PHIPA with regard to the AI technology?
- Does the custodian's description of its information practices, contained within its written public statement, adequately address the custodian's use of the AI technology?
- What steps has the custodian taken to ensure it is able to meet its breach notification and reporting obligations under PHIPA if PHI is stolen, lost, used or disclosed without authority through the use of the AI technology?



Accountable

- Public sector entities must develop a robust governance structure for the development, deployment, use, repurpose, or decommissioning of AI systems, with clearly defined roles and responsibilities.
- They should have to conduct algorithmic impact assessments including PIAs to identify the risks of algorithms and how to mitigate against such risks.
- They should identify and document design and application choices they make in respect of their AI systems, and consequential decisions they make about groups or individuals made using AI outputs.
- Individuals must be able to challenge the accuracy of decisions made about them and seek recourse when they believe they have been negatively impacted by them.
- Public sector entities should be subject to review by an independent oversight body with authority to enforce these principles and require the organization to undertake remedial or corrective actions.

From the IPC's submission on Bill 194

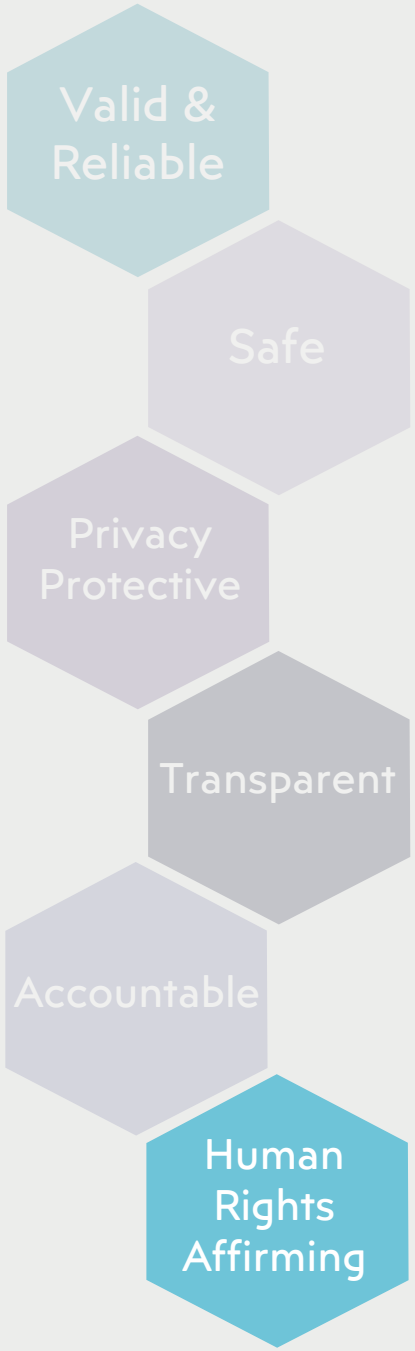


Accountable

Some considerations for the health sector

Cont'd

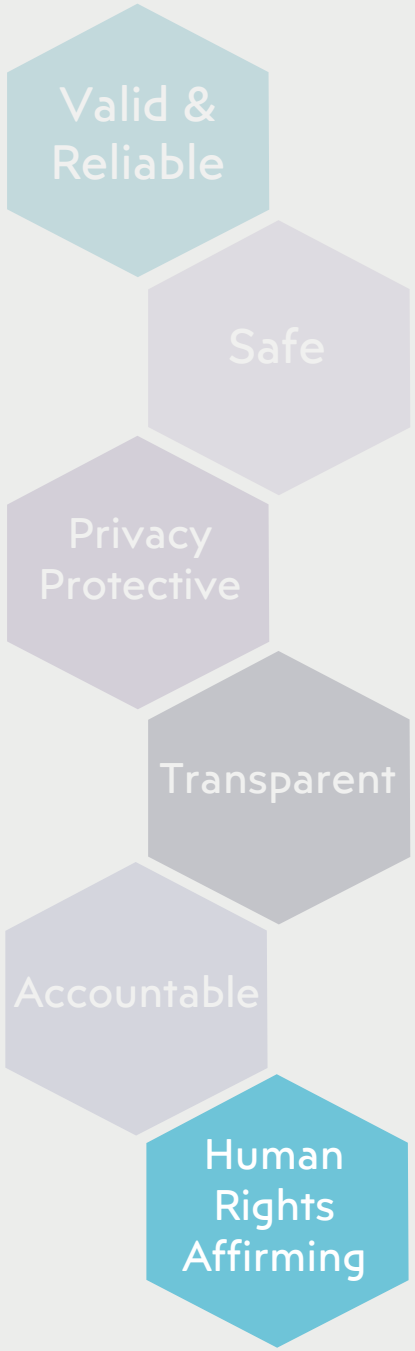
- Do the policies, procedures and practices of the custodian address the custodian's compliance with PHIPA in the context of the AI technology?
- Do the policies, procedures and practices of the custodian include a clear AI governance framework that sets out the custodian's accountabilities and its agents?
- What assessments have been conducted prior to developing, maintaining, procuring, implementing and using an AI technology - e.g. privacy impact assessment (PIA), threat risk assessment (TRA), AI specific assessment such as an algorithmic impact assessment (AIA), or vendor assessment?
- What recourse options are available to individuals to enable them to challenge the decisions made about them through the use of an AI technology including the accuracy of any PHI that is generated or altered by the AI technology?
- What training is in place for custodians and their agents to ensure they understand their obligations?



Human Rights Affirming

- AI technologies should be designed to be fair and equitable.
- They must respect and affirm human rights for individuals and communities.
- AI technologies should also be purposefully designed to address and redress historical discrimination and bias so that individuals and communities affected by AI systems do not experience ongoing discrimination based on equal application of logics of a given AI technology or its outputs.

From the IPC's submission on Bill 194



Human Rights Affirming

Some considerations for the health sector

Cont'd

- What steps has the custodian taken to ensure that the AI technology "*benefits the people of Ontario while protecting fundamental rights and freedoms guaranteed by the Canadian Charter of Rights and Freedoms and the Human Rights Code*?"*
- What steps have been taken to help ensure that the AI technology will provide a net benefit to society and produce fair and equitable outputs?
- What bias or other assessments have been conducted to help ensure that the AI technology has adequately mitigated the risk of bias in the model? How often will this assessment be repeated?
- What steps have been taken to ensure that the AI technology has not been designed, (inadvertently or not) to produce biased outputs?
- What steps have been taken by the custodian to ensure that appropriate methods and techniques are in place to minimize the potential impacts of biased data used to train the AI model?

* OHRC Submission on Bill 194

IPC-Related References

- Principles for Responsible, Trustworthy and Privacy Protective Generative AI Technologies (Joint resolution of the federal, provincial, and territorial information and privacy commissioners and ombudspersons)
- Resolution on Generative Artificial Intelligence Systems (Joint resolution of the Global Privacy Assembly)
- Resolution on Artificial Intelligence and Employment (Joint resolution of the Global Privacy Assembly)
- Joint statement on the use of AI technologies (Ontario IPC and Ontario Human Rights Commission)
- Statement on Generative AI (Roundtable of G7 Data Protection and Privacy Authorities)
- Written Submission on Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024
- IPC Ontario Comments on Ontario's Trustworthy AI Framework
- Artificial intelligence in health care: Balancing innovation with privacy (IPC Podcast)

Additional References

- Bill 194: *"Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024"*
- Ontario's Trustworthy AI Framework
- Ontario Human Rights Commission written submission on Bill 194
- Bill C-27, the Digital Charter Implementation Act
- The Artificial Intelligence and Data Act (AIDA) Companion Document
- Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems
- Health Canada draft guidance: "Pre-market guidance for machine learning-enabled medical devices"
- Guidance for the responsible use of AI by government

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