Office of the Information and Privacy Commissioner of Alberta

# Guidance for Small Custodians on the Use of Artificial Intelligence

November 2023

## Guidance for Small Custodians on the use of Artificial Intelligence

Alberta currently has no specific laws regulating the use of artificial intelligence (AI). However, Alberta's privacy laws apply when AI systems process health information (HI) or personal information (PI).

This guidance is to help small custodians (such as those designated under section 2(2) of the *Health Information Regulation*, or HIR[1]) comply with privacy laws when using AI systems in their practices. It will also help small custodians consider the risks and will suggest steps to meet due diligence and regulatory requirements.

### Some helpful definitions

**AI system** – A product or service used by an entity, which utilizes a form of AI to automate, enhance or otherwise improve or facilitate service delivery.

**Artificial intelligence (AI)** – an advanced form of information processing for the purpose of automating and/or enhancing the performance of human tasks.

***Health Information Act* (HIA)** – Alberta's HIA provides individuals with the right to request access to their own health information in the custody or under the control of health custodians while providing custodians with rules for the collection, use, disclosure, retention and protection of health information.

**HI** – health information about an individual as defined under HIA.

***Personal Information Protection Act* (PIPA)** - PIPA provides individuals with the right to request access to their own personal information while providing private sector organizations with rules for the collection, use, disclosure, retention and protection of personal information.

**PI** – personal information about an individual as defined under PIPA.

**Office of the Information and Privacy Commissioner (OIPC)** – The OIPC independently oversees Alberta's privacy and access laws, including HIA and PIPA.

[1] For more detail, see the regulation at https://kings-printer.alberta.ca/1266.cfm?page=2001_070.cfm&leg_type=Regs&isbncln=9780779840939&display=html Regulated professions include regulated members of professional associations i.e. physicians, dentists, optometrists, nurses, etc.

## More about AI and how it is used in healthcare

Artificial intelligence (AI) is a catch-all for various kinds of techniques to process information in a way that resembles human intelligence. AI always requires three ingredients, which are:

- hardware, to provide the infrastructure, storage and processing power;
- software, computer code to resemble intelligent interaction with whatever inputs are provided; and
- data, as an input to generate a useful output and to train the software in the first place.

AI is being used in healthcare to assist in endeavors such as drug discovery and development, enhancing medical devices, emergency triage, diagnosis of diseases, capacity planning, patient scheduling, note-taking, or medical simulations. A majority of AI applications in healthcare involve the processing of HI or sometimes PI, e.g. employee information.

## Which privacy laws apply?

The collection, use, disclosure and retention of health information (HI) in Alberta is governed by the *Health Information Act* (HIA)[2]. The *Personal Information Protection Act* (PIPA) applies to personal information (PI) in the custody or control of organizations and includes employee information. So, the personal employee information of a small custodian's employees is subject to PIPA. There currently is no specific legislation to govern the use of AI in Alberta.

## As a custodian under HIA and an employer under PIPA, how can the use of AI impact my privacy compliance?

When AI systems interact with PI and HI, there are requirements for using these systems. You should ensure you have legal authority for the purpose for which you want to use the PI or HI in the AI system, and that its use complies with the requirements under applicable legislation, which is, for now, HIA and PIPA.

### Legal authority to process

It is important to familiarize yourself with how the AI technology works. Is HI or PI being processed solely to provide care and plan staffing, or are there *secondary purposes* such as reinforcing the learning of the AI system, system technical diagnostics and performance of the AI, identifying sales or marketing opportunities, etc.? You may not have legal authority for some of these purposes proposed by the system's service provider. Once this information about purposes is known, you must ensure that you have the authority to collect, use and disclose PI and HI for each of the identified purposes. If you do not have authority for a purpose, you need to work with the technology provider to customize the service delivered or limit the use or disclosure of information for secondary purposes, to ensure you meet your obligations under HIA and PIPA.

### Compliance risk

AI systems carry compliance risks, which are inherent to all information and communications technology (ICT) systems, and also carry their own specific risks. You need to ensure you meet your obligations under HIA and PIPA by having reasonable physical, administrative and technical controls in place on the use of all your ICT

[2] For more information about HIA and PIPA see the OIPC's resources at https://oipc.ab.ca/wp-content/uploads/2022/02/HIA-Guide-2010.pdf and https://oipc.ab.ca/wp-content/uploads/2022/02/PIPA-Guide-2008.pdf. For further detail, see the Acts at https://kings-printer.alberta.ca/Laws_Online.cfm.

systems[3]. You also need to consider how you will comply with requirements for providing access to information and for responding to an individual who requests correction of their information. Some examples of specific risks when using AI systems are:

- AI systems often operate like black boxes[4]. It is not always clear how an AI system reaches a specific conclusion or decision for a given output. There is, for such systems, a risk of using incorrect PI or HI, using data with inherent bias, or having errors built into the logic that produces the outcomes. These issues may be present but not easily detected. This is not just a privacy risk but may result in harms to patients. Transparency of AI decision-making and supervision by humans are required for important processes.
    - *Example: Consider an AI-based scheduling system, which is used by a clinic for analysing various sources of data (e.g. past workload data, weather information, public holidays, events and real-time public health surveillance data) for staff scheduling purposes. If such a system uses inaccurate data, this may lead to staffing issues at the clinic.*

- There is a risk of breaches through exploitable vulnerabilities in the AI system. This is similar to the risk faced by regular ICT systems, but there is an additional risk related to opening an AI system up to public access.
    - *Example: A public-facing AI system used for self-intake, if improperly tested or configured, may be vulnerable to compromise by means of such things as logical attacks[5] to extract patient information.*

- The AI system will likely be provided by an external service provider, where there is additional risk of improper data handling practices, breach or outage.
    - *Example: The service provider you use for a virtual assistant that schedules patient visits and makes notes of all your consultations has been hit by malware such as a ransomware attack[6], which causes the system to become inaccessible. Because you rely on this system for automatic note-taking and patient file maintenance, appointments now take you nearly twice as long because you need to deal with these administrative tasks yourself. The quality of care suffers accordingly. In addition, you may need to manage and report the privacy breach caused by such an attack to the OIPC, as required under applicable legislation.*

---

[3] A good start to bring this into practice is the Canadian Centre for Cyber Security's resource for healthcare providers at https://www.cyber.gc.ca/en/guidance/cyber-security-healthcare-organizations-protecting-yourself-against-common-cyber-attacks

[4] A system or device which produces useful information or other outputs, without revealing much information about its internal workings.

[5] Logical attacks use functionality of a system in a way unintended or unforeseen by the developer, so as to circumvent security controls. A good example of a logical attack against language based AI systems is something called "jailbreaking". Jailbreaking uses AI's understanding of language together with its tendency to want to comply with requests made to it by users. Simple jailbreaks include asking the AI to forget its ethical rules or pretend it is an unethical fictional character to circumvent controls on outputs put in place by its developers.

[6] Ransomware is a form of malicious software (malware) that installs itself on an electronic device or system, including smartphones, tablets and computers, and encrypts the entire hard drive, or specific files. It then prompts the victim to pay a ransom, before the information is decrypted. Ransomware may also attempt to encrypt files that are located on network/cloud drives connected to an infected device or system. More importantly, attackers may access and steal information stored on a device or system during the course of an attack.

**Privacy and security risk assessment**

If a custodian is planning to use an AI system to process HI, they must assess their duties under HIA to collect, use and disclose HI in accordance with the law. They must also ensure their practices are in compliance with requirements regarding security of, access to, and retention of HI. A privacy impact assessment (PIA) is useful and, when operating under HIA, is a mandatory tool to ensure potential privacy and security risks are identified and addressed prior to the implementation of AI systems that process HI. Under Section 64 of HIA, custodians are required to submit PIAs to the OIPC prior to implementing a new system or administrative practices that collect, use or disclose identifying health information.

If the AI system interacts with, or is a part of your electronic health records (EHR) system, custodians should take into account HIA requirements regarding EHR systems, as set out in the Act and Regulations. The OIPC has guidance available that sets out these requirements[7].

## What questions should I consider before acquiring AI-based products or services for my practice?

There are benefits that can result from the use of AI, including improved productivity, enhanced delivery of traditional healthcare, and optimization of the clinical services being provided. Clinics and physicians can do their part to prevent adverse effects by asking questions and gathering the right information before implementing an AI system. These questions include the following.

- What is the purpose of the AI system I want to obtain?
    - Is this process better done by AI, by a human or by a combination of both?
    - What is the balance of costs, risks and benefits?
    - What is the impact of using AI for this process for me, my staff and my patients?

- What data will be used by the AI system? Will this data include PI or HI?

- Do I have authority under HIA and/or PIPA to process HI and/or PI with this AI system?

- What are the guarantees, certifications, policies and contractual obligations of the service provider that offers the AI system?
    - Are adequate physical, administrative and technical safeguards in place?
    - Do the certifications, policies and contractual obligations meet or exceed the compliance requirements?
    - Do I have a clear idea of the risks of the product or service, and are there contingency plans in place for any risks?
    - If the service provider of the AI system claims that only anonymized or non-identifying personal information is used for secondary purposes, what standard for anonymization or de-identification is being used and do the service provider's practices guarantee that there is no risk of re-identification?
    - Has the service provider assessed and taken proper steps to assure the accuracy and fairness of the product or service (e.g. bias of training data and bias of outcomes).

[7] https://oipc.ab.ca/wp-content/uploads/2022/02/Electronic-Health-Record-Systems-2016.pdf

- Is the HI and/or PI processed outside of Alberta or Canada[8]?

- How is the HI and/or PI secured when used by the AI system?
    - Where is the HI and/or PI stored? Is it stored in a cloud-based service?
    - Are HI and/or PI encrypted in transit and in storage using industry standard algorithms? Are the encryption keys securely managed and by whom?
    - Was the AI system reasonably tested prior to and after your implementation? Are both the AI software and the infrastructure it runs on continuously monitored for security issues?

- Will HI and/or PI be used to train the AI system I use?

- How do I prepare for the use of an AI system in my practice?
    - What additional AI-specific training, policies and procedures do I need to implement?
    - Is it transparent to patients that AI is or will be used, and how it is used?
    - Can patients opt out of having their information processed by AI and can they request a second opinion, if they disagree with results?

## Related OIPC guidance materials

The OIPC regularly publishes guidance to help custodian comply with HIA. All resources can be found at https://oipc.ab.ca/resources/hia/.

### *Health Information Act* Guide

This guide is intended to give custodians a basic understanding of the *Health Information Act*. https://oipc.ab.ca/wp-content/uploads/2022/02/HIA-Guide-2010.pdf

### Electronic Health Records System Guidance

This document is meant for custodians and their information managers (service providers) to assess the safeguards in electronic health records systems. https://oipc.ab.ca/resource/electronic-health-record-systems/



[8] Additional requirements apply under HIA s.60(b) and HIR s.8(4) when outside Alberta and PIPA s.6(2) and s.13.1 when outside Canada in such cases.