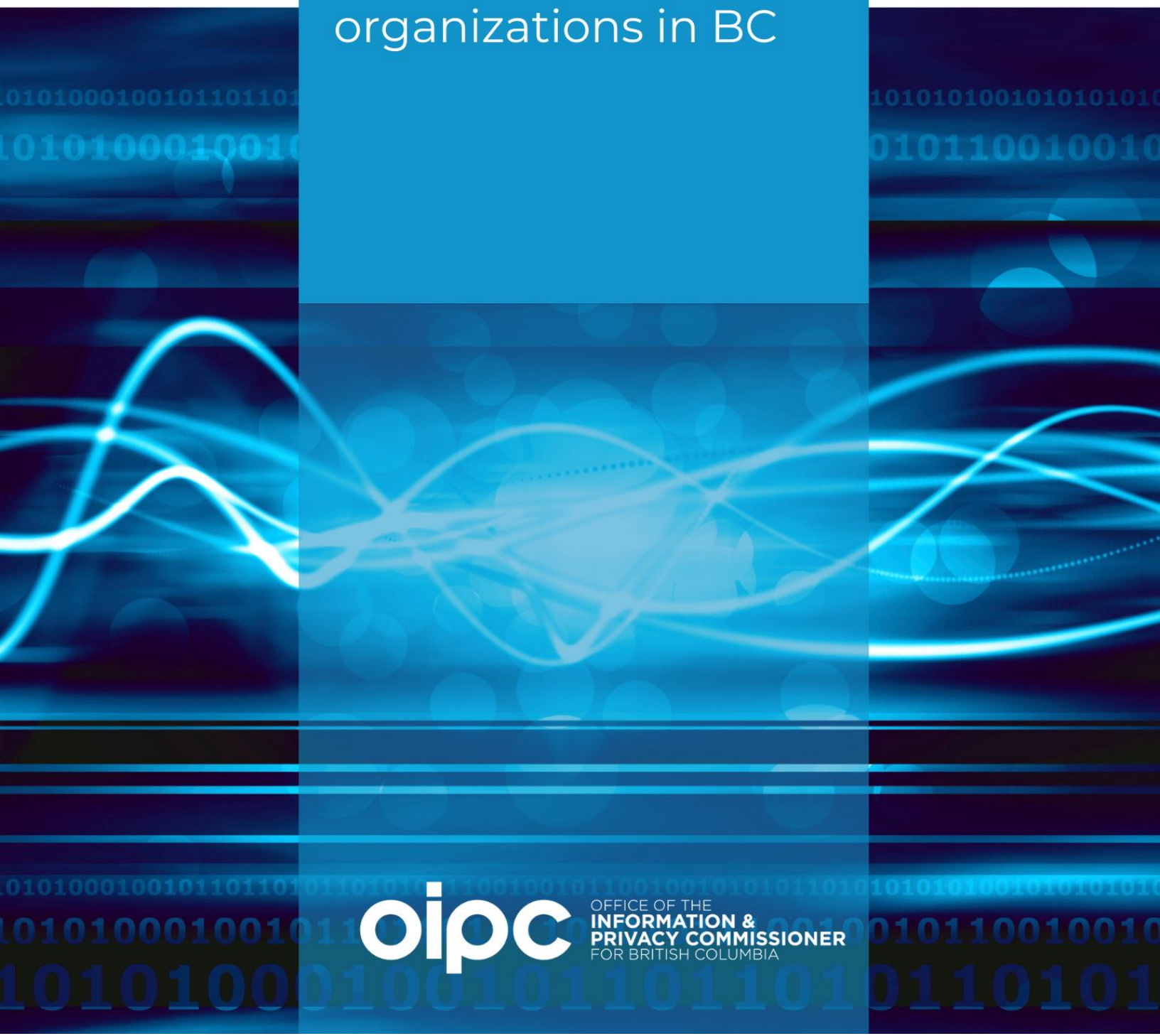
GENERAL

January 2026

PIPA and AI scribes: best practices for healthcare organizations in BC



OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

PURPOSE OF THIS GUIDANCE DOCUMENT

This document provides guidance to healthcare organizations subject to British Columbia's *Personal Information Protection Act* (PIPA) that are considering the use of artificial intelligence (AI) scribes in their practices. Examples of organizations under PIPA include healthcare providers running their own practices, most primary care clinics, and other entities providing health services outside of a public body.

Please note that this guide does not analyze other legal or regulatory requirements for using AI scribes that fall outside of BC's PIPA. For example, it does not cover the use of AI scribes by public bodies in BC, such as health authorities and most hospitals. Public bodies rely on separate legal authorization under the *Freedom of Information and Protection of Privacy Act* (FIPPA), which involves a different analysis that is not covered by this guide.

If you are uncertain whether PIPA or FIPPA applies to your practice (for example, if you are a healthcare organization operating under contract for a public body), we recommend that you refer to your contract and/or seek legal advice to clarify this before reading further.

Health professionals are advised to seek advice from their applicable regulatory body regarding any additional laws, bylaws, regulations, or practice standards that may apply to the use of AI scribes in their particular setting.

WHAT ARE AI SCRIBES?

AI scribes are tools that use generative AI[1] to listen to, transcribe, and summarize real-time conversations between patients and healthcare providers. Currently, they primarily function as transcription tools that produce notes for integration into the patient's medical record. However, these technologies are evolving rapidly, and their capabilities vary significantly from one tool to the next. For example:

- Some AI scribes automatically populate information about the patient visit directly into the healthcare provider's Electronic Medical Record (EMR) or Electronic Health Record (EHR).
- Others generate referral letters, patient handouts, and physician reminders for ordering lab work and writing prescriptions for medications.

[1] "Generative AI is a subset of machine learning in which systems are trained on massive data sets – often including personal information – to generate new content such as text, computer code, images, video, or audio in response to a user prompt. This content is probabilistic, and may vary even in response to the same or similar prompts." Canadian federal, provincial and territorial privacy regulators, Principles for responsible, trustworthy and privacy-protective generative AI technologies, December 7, 2023: https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/

- Some AI scribes even act as a medical "co-pilot" by suggesting medical diagnoses, medical investigations, referrals, and treatment options.

This guide focuses on AI scribes that function as a transcription tool, rather than those that offer broader capabilities, such as clinical decision-making support. However, there are reminders throughout this document to remain alert to function creep, where a tool that originally operated solely as a transcription tool may add additional functions over time, leading to new privacy and access implications.

HOW DOES PIPA APPLY?

In BC, PIPA governs the collection, use, and disclosure of personal information[2] by organizations,[3] including healthcare providers and medical clinics that are not public bodies.[4] Organizations can only collect, use, or disclose personal information if PIPA authorizes it. This applies to personal information that healthcare organizations collect using AI scribes.

1. Collection, use and disclosure of personal information

Before using an AI scribe to collect, use or disclose personal information, a healthcare organization must establish that it has the appropriate legal authority under the following sections of PIPA:

- **Collection** of personal information (from patients and others present) – Part 4
- **Use** of the personal information (within the organization) – Part 5; and
- **Disclosure** of the personal information (to other entities) – Part 6.

When a clinician uses an AI scribe to meet with a patient, several flows of personal information are happening simultaneously. First, the clinician is collecting personal information from the patient for the purpose of providing healthcare. Second, the AI scribe tool is using personal information from the patient for multiple purposes, such as transcribing, summarizing, and potentially making healthcare recommendations. In addition, the AI scribe company (vendor) may be collecting, using, and/or disclosing personal information for its own purposes, such as quality assurance, developing new products or services, training the AI model, marketing, or selling to third parties.

---

[2] Under s. 1 of PIPA, personal information means "information about an identifiable individual and includes employee personal information but does not include a) contact information, or b) work product information." Contact information refers to business contact information.

[3] The definition of organization under s. 1 of PIPA "includes a person, an unincorporated association, a trade union, a trust or a not for profit organization…" In the healthcare context, this includes healthcare providers running their own practices, most primary care clinics, and other entities providing health services outside of a public body.

[4] The definition of public bodies under Schedule 1 of FIPPA includes government ministries and other various bodies designated in Schedule 2 of FIPPA, and local public bodies. In the healthcare context, this includes the Ministry of Health, health authorities, as well as most hospitals and government-funded and operated clinics.

Therefore, evaluating an AI scribe tool requires examining both the healthcare organization's and AI scribe vendor's collections, uses, and disclosures of personal information. An organization cannot avoid its obligations under PIPA by contracting with another organization to store or use personal information on its behalf. Under PIPA, an organization remains responsible for personal information under its control, even when the personal information is not in its custody.[5]

Even if an organization's initial assessment suggests that the use of an AI scribe is PIPA compliant, the organization must remain alert to function creep, where shifts in the tool's capabilities or the vendor's policies over time may fundamentally change how the AI scribe collects, uses, or discloses personal information. For example, an AI scribe that originally functioned as a transcription tool may be updated to make diagnostic and treatment recommendations. These changes may raise new privacy and access implications, and the healthcare organization needs to evaluate these new capabilities to make sure they do not enable the AI scribe to collect, use, disclose or store personal information in a manner that would contravene PIPA.

The best way for any organization to protect itself from privacy risks resulting from vendor software updates is to require the vendor to obtain permission before performing updates. If an update changes how personal information is collected, used, disclosed or stored, then we strongly recommend that the healthcare organization require the vendor to explain those changes and give the organization a choice to accept or reject the update.

Although not required under PIPA, a privacy impact assessment (PIA)[6] is a helpful compliance tool that organizations are recommended to complete to help them decide if PIPA authorizes the collection, use and disclosure of personal information using an AI scribe. The best practice is to conduct an initial PIA before adopting an AI scribe, and then update the PIA whenever there are changes to the tool's functions or the vendor's policies that impact how personal information is handled.

If a healthcare organization cannot identify an authority under PIPA for the collection, use, or disclosure of personal information, then it must not collect, use or disclose it.

2. Reasonable person test

An overarching principle of PIPA is that an organization's collection, use, or disclosure of personal information must be for "purposes that a reasonable person would consider appropriate in the circumstances."[7]

---

[5] See s. 4(2) of PIPA.

[6] See OIPC guidance document *PIAs for the private sector* and *PIA template for organizations*. OIPC staff are also available to review and provide feedback on PIAs, if requested. Please see OIPC contact information at the end of this guide.

[7] See ss. 11, 14 and 17 of PIPA.

This means that a healthcare organization wishing to implement an AI scribe must first assess whether a hypothetical reasonable person, knowing all the purposes for the collection, use and disclosure of personal information by the AI scribe and the surrounding circumstances, would consider those purposes to be appropriate. Even if patients consent to the use of an AI scribe, an organization must still be able to demonstrate that its collection, use and disclosure of personal information meets this reasonable person standard. Both are required: a person cannot consent to something that isn't appropriate; and an organization can't proceed with something that is considered appropriate if a person hasn't consented to it.[8]

What constitutes "reasonable" and "appropriate" will vary according to the particular circumstances of each organization and the kind of healthcare the organization provides. Considerations may include:

- the sensitivity of the personal information involved;
- whether the organization is collecting or using the minimum amount of information reasonably required to achieve its purposes;
- the relevance or usefulness of the information in fulfilling the organization's purposes (not the AI scribe vendor's purposes);
- the manner of collecting and using the personal information; and
- whether there are less privacy-invasive alternatives that achieve the same purposes.[9]

What distinguishes an AI scribe's collection of personal information from traditional notetaking with a pen and notepad is that there are many processes taking place with an AI scribe that are more complex, potentially more privacy invasive, and less obvious to the average person. For example, the amount and sensitivity of personal information being collected by an AI scribe exceeds that of traditional notetaking (e.g., extensive biometric data[10] are captured through voice recordings, as well as extraneous personal details that would normally be omitted from handwritten notes), and it will not be obvious to the average person how their personal information is flowing through the tool. This is why it is so important for healthcare organizations to carefully assess an AI scribe against the requirements in PIPA.

[8] There are limited circumstances where PIPA permits the collection, use and disclosure of personal information without consent. Please refer to the consent section of this document, including footnote 12, for more details.
[9] See, for example, OIPC-BC Orders P12-01 (2012 BCIPC No. 25), P13-02 (2013 BCIPC No. 24), P20-04 (2020 BCIPC No. 24), and P25-01 (2025 BCIPC No. 13).
[10] Biometric data captured by an AI scribe include the distinct characteristics of an individual's voice (accent, pitch, tone, cadence, speech patterns, etc.), which can identify a person and also be used to infer other features about them such as gender, age, ethnicity, and even their emotional state. These data are extremely difficult to anonymise, even when other identifiers are removed.

3. Consent

Under PIPA, an organization cannot collect, use or disclose an individual's personal information unless it is only for a purpose that a reasonable person would consider appropriate in the circumstances and:

- the individual the information is about has consented to the collection, use, or disclosure of their personal information; or
- PIPA authorizes the collection, use, or disclosure of their personal information *without* consent.

Patient consent

In the majority of clinical scenarios, consent is required from a patient (or their authorized *representative*[11]) prior to using an AI scribe, given that there will be no legal authority under PIPA for the collection, use, or disclosure of personal information without consent. There may be limited situations where consent is not required under PIPA, such as in certain emergencies where a patient is unable to consent.[12]

Healthcare organizations must get express consent from patients, rather than implicit consent. Express consent may be obtained verbally or in writing (e.g. using a hard copy or online consent form), but either way, written documentation in the patient's file is highly recommended so there is a clear record of their decision.

It is not appropriate to rely on implicit consent,[13] given:

- the novelty, complexity, and rapid pace of change of AI scribe technologies. It will not be obvious to a reasonable person what an AI scribe is, how much personal information it is collecting, and how it will use their personal information;[14]
- the varying functionality of AI scribes. The types of collections, uses, and disclosures of personal information can vary significantly from one tool to another and require explanation; and

[11] See s. 2 of the PIPA Regulation for details about who can act as a representative for others to give or refuse consent to the collection, use and disclosure of their personal information under PIPA.

[12] Sections 12, 15, and 18 of PIPA establish the limited circumstances in which the collection, use and disclosure of personal information may be permitted without consent. However, none of these circumstances will apply to the use of AI scribes in typical clinical scenarios. There may be some unique cases where patient consent is not required – for example, certain emergency situations where collection of personal information without consent may be authorized under ss. 12(1)(a) or (b) of PIPA. This determination would require an assessment of the specific circumstances.

[13] Section 8 of PIPA describes two types of implicit consent – "deemed" and "consent by not opting-out" – which are not appropriate forms of patient consent in the AI scribes context.

[14] See the "obvious to a reasonable person" requirement for deemed implicit consent under s. 8(1)(a) of PIPA.

- the sensitivity of the personal information involved.[15]

If a patient is accompanied to the appointment by other individuals whose voices may be captured by the scribe, then express consent should be obtained from them as well.[16]

If a minor is present during the appointment, their capacity to consent for themselves needs to be assessed. Section 2(2)(c) of the PIPA Regulation holds that the guardian of a minor can only give or refuse consent to the collection, use and disclosure of personal information on behalf of the minor "if the minor is incapable of exercising that right." PIPA does not specify an age at which a minor becomes capable of exercising their own rights under the Act, given that the ability of children and youth to provide meaningful consent depends greatly on their cognitive and emotional maturity, as well as the specific context and nature of personal information involved.[17]

Consent is only valid where the individual truly understands what they are consenting to. Healthcare organizations must consider the content and accessibility of the information they provide to their unique patient population. This includes using clear explanations, a level of language suitable to a diverse audience, and a comprehensible means of displaying and/or communicating information.[18]

The consent process must include notice to individuals of all the purposes for which the healthcare organization and AI scribe vendor are collecting their personal information. The purposes must be specific: "healthcare" is not specific enough to meet the collection notice requirement under s. 10(1) of PIPA.

After providing adequate information, healthcare organizations must give individuals a clear option to say "yes" or "no" to the use of an AI scribe.[19] Healthcare organizations must also inform patients that they can withdraw their consent at any time, with no change to the level of care they receive from their clinician.[20] If a patient declines consent to an AI scribe, or initially consents and then later withdraws consent, the clinician must be prepared to collect their personal information using another method.

---

[15] The sensitivity of the personal information is one of the factors to consider when assessing the reasonableness of using "consent by not opting out" implicit consent under s. 8(3) of PIPA.

[16] If a patient consents, but another individual accompanying the patient does not consent to their voice being captured by the AI scribe, then that individual has the option to not participate in the conversation, or the clinician will need to switch to another method of notetaking.

[17] See p.10 of *Obtaining meaningful consent* for further guidance on consent and children.

[18] See *Obtaining meaningful consent* for further guidance on best practices for obtaining informed consent.

[19] Under s. 7(2) of PIPA, an organization must not require an individual to consent to the collection, use, or disclosure of personal information beyond what is necessary to provide the product or service.

[20] Under s. 9 of PIPA, individuals have the right to withdraw their consent at any time (with limited exceptions, which do not apply to the context of AI scribes).

Finally, consent should be considered a dynamic and ongoing process. As previously mentioned, organizations need to remain alert to function creep and notify patients if there are changes in the AI scribe's capabilities or privacy practices over time that impact the handling of their personal information, so they can re-evaluate their consent choices. For example, an organization cannot rely on a patient's previous consent for an AI scribe to transcribe chart notes if software updates have changed the tool's function into a medical "co-pilot" that uses patients' personal information to make diagnostic and treatment recommendations.

Employee consent

Using an AI scribe to record clinician-patient interactions involves the collection of information about employees as well as patients.

Whether organizations under PIPA are required to get consent from employees before they use an AI scribe to engage with patients is a complex question. The reason it is so complex is that different types of information (with different consent requirements) may be collected from employees using an AI scribe, depending on what information the employee discloses during the patient interaction, and the specific practices and policies of the healthcare organization and AI scribe vendor involved.

It is possible that an AI scribe may collect a combination of the following types of information from an employee, even during a single patient interaction:

- **Work product information**, which is not personal information under PIPA, and means information prepared or collected by an individual or group of individuals as a part of their employment or business responsibilities or activities, but does not include personal information about an individual who did not prepare or collect the personal information;
- **Employee personal information**, which is a type of personal information under PIPA, and means "personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual's employment"; and
- **Personal information** that is not employee personal information.[21]

An organization does not need to get consent for an AI scribe to collect, use or disclose work product information, since it is not personal information under PIPA. Consent is also not required for the collection, use or disclosure of employee personal information if the collection, use or disclosure is "reasonable for the purposes of establishing, managing or terminating an

[21] See s. 1 of PIPA for definitions of personal information, employee personal information, and work product information. Further guidance is provided in section 6 of *A Guide to B.C.'s PIPA*, and leading OIPC order P12-01 (2012 BCIPC No. 25), which provides an analysis of these terms.

employment relationship between the organization and the individual," and the employee is provided with notice beforehand.[22]

However, consent is required from employees if the AI scribe is collecting personal information about them that falls outside of employee personal information. Examples of what may be considered personal information about an employee include extraneous personal information shared about their family or recent vacation, and biometric data embedded in the employee's voice recording.

Given that at least some information collected from employees is likely to be personal information, the best practice is to obtain employee consent prior to the use of an AI scribe. The consent process must include notification of all of the purposes for which the AI scribe will collect the employee's personal information, prior to use.[23]

Organizations need to consider whether express consent or implicit consent (the "consent by not opting out" type**,** as detailed in s. 8(3) of PIPA) is the most appropriate form of employee consent, depending on the specific circumstances and the sensitivity of the personal information involved.[24] Note that "deemed" implicit consent under s. 8(1) of PIPA is not appropriate, given that all of the collection purposes may not be obvious to employees, especially if the AI scribe vendor is collecting personal information for its own purposes.[25]

If "consent by not opting out" implicit consent is chosen instead of express consent, an organization must evaluate s. 8(3) of PIPA carefully to make sure all the requirements are met.

4. Accuracy

Section 33 of PIPA ("Accuracy of Personal Information") requires organizations to make a reasonable effort to ensure that personal information collected by or on behalf of the organization is accurate and complete, if the personal information is:

- likely to be used to make a decision that affects the individual; or
- likely to be disclosed to another organization.

Accuracy is a concern with generative AI technologies, including AI scribes. The bottom line is that these technologies generate outputs that are probabilistic (based on analysis of massive data sets), and not always factual. A variety of errors can occur, including:

[22] See ss. 13, 16, and 19 of PIPA.
[23] See collection notice requirement under s. 10(1) of PIPA.
[24] See requirement under s. 8(3)(d) of PIPA for "the sensitivity of the personal information in the circumstances" to be factored into the evaluation of whether "consent by not opting-out" is appropriate.
[25] See the "obvious to a reasonable person" requirement for deemed implicit consent under s. 8(1)(a) of PIPA.

- **Hallucinations** (making up content that isn't correct to fill gaps in the data);
- **Omissions** (leaving out relevant information);
- **Misinterpretations and misspellings** (e.g., names, diseases, medications); and
- **Biases** (due to biases in the underlying data the tool was trained on).

Furthermore, many factors that are known to increase the error rates of AI scribes, such as background noise, complex conversations, and variations in speech (e.g., accents and medical conditions affecting speech) are common in clinical settings.

Accuracy of AI scribes: key questions

Healthcare organizations must assess accuracy rates when choosing an AI scribe, as accuracy can vary widely between tools.

Good questions to ask vendors when assessing an AI scribe's accuracy include:

- What is the frequency of the different types of errors?
- Were the accuracy and error rates evaluated in a realistic clinical setting that included individuals with a diversity of language and speech patterns?
- Was the evaluation done by a third party (to reduce the risk of bias)?
- Does the vendor perform ongoing assessments and monitoring of accuracy and performance (preferably by a third party)?
- Is there a clear mechanism for your healthcare organization to report inaccuracies back to the vendor, and how will these reports be addressed?
- If information is transmitted from the AI scribe tool to the EMR, what technical controls are in place to ensure that the information is matched to the correct patient profile within the EMR?

Healthcare organizations must expect inaccuracies, and they need to plan strategies to identify and correct them. Even if an AI scribe hypothetically produces transcriptions that are 99% accurate, a 1% error rate may still be catastrophic in the medical setting – for example, if an AI scribe gets the name of an individual's medical condition or prescription medication wrong.

It is essential that healthcare organizations have well-communicated policies in place requiring active and continuous human oversight of the AI scribe's outputs. Keeping a human-in-the-loop is critical for validating the outputs, and correcting any mistakes before the information is used to guide clinical care. For example, any transcripts, summaries, or reports generated by the AI

scribe must be reviewed and edited by the responsible medical professional prior to being integrated into the patient's medical record, or being used or disclosed for any purpose. Introducing an AI tool into clinical practice does not shift accountability – the organization still remains responsible for what is entered into the patient's record.

Despite having policies in place requiring human oversight, employees can still develop complacency over time. Once clinicians become comfortable with an AI scribe, and if they find it to be accurate most of the time, there is a risk that the quality of their reviews may decline, leading to increased errors. Numerous studies have demonstrated that humans (including experts) are susceptible to automation bias, meaning that we have a tendency to over-rely on the outputs of automated systems, even when they are incorrect, or go against our better judgement.[26]

Organizations also need to be aware that the AI tool itself may become more error prone over time due to phenomena such as data drift and model drift, where the performance or accuracy of an AI model deteriorates over time due to exposure to real-world data that diverges significantly from the data set on which it was originally trained.

Healthcare organizations need to take steps to prevent and detect complacency, automation bias, and shifts in the AI scribe's performance, including conducting regular audits of the accuracy of the AI scribe's outputs as well as the staff's adherence to human-in-the-loop policies. We also recommend that organizations have a clear mechanism to report clinicians' observations about inaccuracies, biases, or any other potential harms back to the AI scribe vendor for ongoing evaluation and improvement.

5. Security requirements

Section 34 of PIPA (*Protection of Personal Information*) requires organizations to make reasonable security arrangements to protect personal information in their custody or under their control from risks such as unauthorized access, collection, use, disclosure, copying, modification, or disposal.

What is considered "reasonable" varies depending on the circumstance, taking into account a number of factors, including:

- the sensitivity of the personal information;
- the foreseeable risks;
- the likelihood of damage occurring;
- the medium and format of the record containing the personal information;

[26] See: Hoffman, B. Automation bias: what it is and how to overcome it. *Forbes*. March 10, 2024.

- the harm that could be caused by an incident; and
- industry standards.

Given that AI scribes collect, use, and disclose some of the most highly sensitive personal information there is about individuals, healthcare organizations are expected to implement a high level of security with respect to all of the personal information under their control. While PIPA does not prescribe specific security measures, the OIPC would expect to see personal information protected with multiple layers of physical, technical, and administrative safeguards, as outlined in *Securing personal information: A self-assessment for public bodies and organizations*.

Examples of commonly expected security measures for protecting health information include restricting physical access to AI scribe devices; having controls and protocols in place to prevent inadvertent recording;[27] requiring multifactor authentication[28] and robust passwords[29] for all users; encrypting data in transit and at rest; having controls and procedures in place to promptly detect and respond to privacy and security incidents; and implementing regular privacy and security training for any employees who come into contact with the AI scribe (or its outputs).

[27] Privacy breaches may occur due to poor handling of the tool, not just the tool itself. For example, see this decision from the Information and Privacy Commissioner of Ontario (October 27, 2025) about a hospital privacy breach caused by the inadvertent activation of an AI transcription tool during clinical rounds where patients' personal information was discussed.
[28] See the BC government's webpage: *An Introduction to Multi-Factor Authentication*.
[29] See the BC government's guidance on *Password Best Practices*.

Disclosures of personal information outside of Canada

PIPA does not contain any specific provisions related to the disclosure of personal information outside of Canada. However, organizations must assess the potential risks of any cross-border disclosures as part of their security assessment. Organizations can only disclose personal information outside of Canada if they are satisfied that their obligations under s. 34 of PIPA will be met.

In the context of AI scribes, organizations are unlikely to meet s. 34 requirements if they choose to use an AI scribe vendor that processes or stores patients' sensitive personal information in a jurisdiction that does not respect the rule of law, or has inadequate privacy laws.

Although not required under PIPA, the best practice for initiatives involving disclosures outside of Canada is to conduct a PIA including an additional cross-border risk assessment component.

6. Access to, correction, and retention of personal information

Section 23 of PIPA requires organizations to respond to requests from individuals for:

- access to their own personal information,
- information about the ways in which their personal information has been and is being used by the organization, and
- information about who their personal information has been disclosed to.

In addition, s. 24 of PIPA gives individuals the right to request correction of errors or omissions in their personal information.

Therefore, healthcare organizations must establish policies and processes for how any retained personal information (including voice recordings or transcripts) will be safely provided back to individuals who request access to their own information, and how any errors or omissions will be corrected, upon request.

Under s. 35, organizations must destroy documents containing personal information or remove the means by which the personal information can be associated with particular individuals as soon as it is reasonable to assume that:

- the purpose for which the personal information was collected is no longer being served by keeping the personal information; and

- it is no longer necessary to keep the personal information for legal or business purposes.

However, if an organization uses an individual's personal information to make a decision that directly affects the individual (for example, a healthcare decision), it must keep that information for at least one year after using it so the individual has a reasonable opportunity to access it.

What this means is that any personal information collected or generated by the AI scribe can only be retained for as long as is needed to fulfill the healthcare organization's original collection purposes and applicable legal requirements, and then must be securely disposed of or destroyed. Voice recordings that contain embedded biometric data are particularly sensitive, and must not be kept after transcription is complete, unless the healthcare organization has a clear and reasonable purpose for doing so. -If the AI scribe vendor or any other third-party is contracted to store personal information on behalf of the healthcare organization, they must follow the records retention and destruction instructions of the healthcare organization they have contracted with.

7. Other considerations for PIPA compliance

Updating policies and practices

Section 5 of PIPA requires organizations to develop and follow policies and practices to meet their obligations under the Act.[30] Before adopting an AI scribe, healthcare organizations should update policies, practices, and procedures to account for the privacy and access implications associated with using an AI scribe.

Addressing complaints

Sections 46 and 47 of PIPA give individuals the right to complain to our office if they think that an organization has failed to fulfil their obligations under PIPA.[31]

Organizations must have a process for responding to access to information and privacy complaints. To encourage transparency and trust between healthcare organizations and their patients, we recommend that organizations proactively inform patients that they have a right to request their personal information and that they have a right to complain to the OIPC if they think the organization has not fulfilled an obligation under PIPA.

Staff training and education

Organizations must train their employees on how the AI scribe works. Employees need to know what their responsibilities are for protecting personal information when using an AI scribe. This will help employees understand how personal information is being collected, used and disclosed through the AI scribe, and it will help employees to meet the organization's PIPA

[30] See *Developing a privacy policy under PIPA* for best practices on developing privacy policies and practices.
[31] See the OIPC's step-by-step guidance on *How do I make a complaint?*.

obligations and to answer questions from patients. As much as possible, the AI scribe should not be a mystery to anyone coming into contact with it.

Organizations can find further guidance on meeting their obligations under PIPA in *A Guide to BC's PIPA*.

WHAT SHOULD I LOOK FOR IN AN AI SCRIBE VENDOR'S PRIVACY POLICY AND SERVICE AGREEMENT?

It is often difficult for healthcare providers, let alone patients, to understand the privacy policies and terms of service put forward by tech companies.

However, it is imperative that healthcare organizations understand the terms in these documents so they know what they are agreeing to when they use an AI scribe. Healthcare organizations must be capable of explaining information from the AI scribe vendor's policies to patients during the consent process. Without an understanding of the vendor's privacy policy and service agreement, healthcare organizations will not be equipped with the information they need to seek consent from patients.

AI scribe vendors: key questions for PIPA compliance

- What personal information elements about patients, clinicians, and/or other employees will be collected, used, and disclosed by the vendor?
- Will the vendor use the collected personal information, or derived "de-identified" information, for any secondary purposes (e.g., for non-health related purposes such as training the AI model)?
- Will any personal information, or derived de-identified information, be disclosed to third parties (e.g., sold to third parties for commercial purposes)?
- Will any information be sent outside of Canada, to be processed or stored in other jurisdictions? (if so, where, and what privacy protections exist in the other jurisdictions?)
- What is the vendor's retention policy for the collected personal information and any derived "de-identified" information? Is it adjustable?
- Will the vendor store voice recordings or delete them as soon as a transcript has been generated?
- Does the vendor perform ongoing assessments and monitoring of accuracy and performance (preferably by a third party)?
- Is the vendor contractually obligated to send the healthcare organization timely updates about any new software updates, AI capabilities/practices, declining AI performance, or other changes that may impact the handling of personal information or have other privacy implications?
- Is there a clear mechanism for the healthcare organization to report inaccuracies, biases, non-compliance, or other potential harms back to the vendor? Does the vendor have a contractual obligation to take action in response to such reports?
- What will happen to the personal information and any derived de-identified information when the contract ends, or if the vendor's business structure changes? (e.g., sale of the company, merger with another company, or bankruptcy)
- Does the vendor have reasonable security measures in place to protect the personal information it stores?
- Does the vendor perform industry-standard security assessments and audits, and is it willing to provide the healthcare organization with information about the outcome of these assessments and audits?
- Is the vendor contractually obligated to report any privacy breaches on their end to the healthcare organization?
- Does the healthcare organization retain the contractual right to control, modify and delete the records generated by the AI scribe?
- How will the vendor train its employees on the contractual requirements?

Don't take a vendor's word for it that they are PIPA compliant, and don't accept claims of compliance with other legislation to be good enough. Be aware that there is no accreditation program in Canada that assesses or approves companies' claims of legal compliance. Many vendors claim to be compliant with other laws, such as the Federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) or the U.S. *Health Insurance Portability and Accountability Act* (HIPPA), but it is PIPA that applies to the use of AI scribes in BC. If data flows outside of BC, PIPA still applies to the personal information involved.

"De-identified" data

Be careful to assess what a vendor means if they refer to "de-identified data." There is no standard definition of what constitutes "de-identified," and it doesn't always mean that the information can be widely collected, used, and disclosed. PIPA does not include the concept of de-identified data. Instead, information is either personal information or it is not under the Act. In many cases, what a vendor calls de-identified data is still personal information under PIPA because it is capable of being combined with other information to identify an individual. A vendor cannot use de-identified data that is personal information for a specified purpose unless PIPA authorizes the use and disclosure of that information from the healthcare organization to the vendor for that purpose.

CONCLUSION

AI scribes hold the promise of improving the patient-provider relationship and reducing administrative burden in the healthcare system by automating transcription and other administrative tasks traditionally performed by the healthcare provider. However, before adopting this technology, healthcare organizations must carefully assess the AI scribe and the vendor offering the product against the legal requirements in PIPA.

For further information, please visit our website at www.oipc.bc.ca or contact:

Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038 Stn Prov Govt
Victoria BC, V8W 9A4
Email: info@oipc.bc.ca
Phone: (250) 387-5629

Callers outside Victoria can contact the office toll-free by calling Service BC and requesting a transfer to (250) 387-5629.

Service BC: Vancouver: (604) 660-2421; Elsewhere in BC: (800) 663-7867

APPENDIX: CHECKLIST FOR HEALTHCARE ORGANIZATIONS CONSIDERING USE OF AN AI SCRIBE

This checklist guides healthcare organizations through a privacy and security self-assessment to determine readiness for AI scribe implementation. We recommend checking off each task as it is completed.

1. Assessing your organization's purposes for implementing an AI scribe

☐ Have you carefully considered your intended purposes for implementing an AI scribe?

☐ Have you decided what capabilities/features you want (and don't want) in an AI scribe before selecting one?

2. Assessing collection, use and disclosure of personal information

☐ Do you have a good understanding of how your chosen AI scribe works, and all the capabilities/features it offers? (Consider scheduling a product demonstration with the vendor to observe the tool in action and ask questions.)

☐ Have you determined how to limit the use of the AI scribe to your intended purposes (e.g., can you disable any of the tool's features that are not required)?

☐ Do you understand all the personal information elements that your organization will be collecting, using, and disclosing when using the AI scribe?

☐ Do you understand all the personal information elements that the AI scribe vendor (company) will be collecting, using, and disclosing?

☐ Have you identified a legal authority under PIPA for each of the planned collections, uses and disclosures of personal information?

☐ Have you assessed whether each of the planned collections, uses and disclosures of personal information would be "reasonable" under PIPA?

If you cannot identify a PIPA authority for each of the collections, uses, or disclosures of personal information involved in your initiative, don't go ahead with it!

3. Assessing accuracy of the AI scribe's outputs

☐ Do you understand the frequency of errors (hallucinations, omissions, misspellings) produced by the AI scribe?

☐ Have you checked whether the tool's accuracy was evaluated in a realistic clinical setting that included individuals with a diversity of language and speech patterns?

☐ Do you know whether the AI scribe's accuracy/error rate was assessed by a third party (to reduce the risk of bias)?

- ☐ Are you satisfied that the vendor performs sufficient ongoing assessments and monitoring of accuracy (preferably by a third party)?
- ☐ Have you determined if there is a clear mechanism for reporting inaccuracies back to the vendor, and how these reports will be addressed?
- ☐ If information is transmitted from the AI scribe tool to the EMR/EHR, have you obtained sufficient information about the technical controls that are in place to ensure that the information is matched to the correct patient profile?

4. Securing personal information

- ☐ Are you satisfied that your healthcare organization and the AI scribe vendor have "reasonable security arrangements" in place to protect the personal information flowing through the AI scribe, as required under s. 34 of PIPA?[32]
- ☐ Have you determined whether the vendor performs industry-standard security assessments and audits? Is it willing to provide your organization with information about the outcome of these assessments and audits?
- ☐ If information will be disclosed outside of Canada (e.g., for processing or storage), are you satisfied that the handling of personal information in other jurisdiction(s) will meet reasonable security requirements?
- ☐ Have you checked that the vendor is contractually obligated to report any privacy breaches on their end to your healthcare organization?

5. Additional considerations when reviewing the AI scribe vendor's privacy policy and service agreement

- ☐ Has the vendor agreed in writing to comply with PIPA?
- ☐ Have you checked for any red flags regarding the vendor's collections, uses, or disclosures of personal information? (e.g., will the vendor use personal information or derived de-identified information for unreasonable secondary purposes, or disclose it to third parties?)
- ☐ If the vendor plans to use or disclose de-identified information, have you clarified what they mean by de-identified and assessed whether the information might still be considered personal information under PIPA?
- ☐ Are you satisfied with the vendor's retention policy for the collected personal information and any derived de-identified information? If not, is it adjustable?

[32] See *Securing personal information: A self-assessment for public bodies and organizations* for guidance on assessing your security measures.

- ☐ Have you examined what will happen to the personal information when the contract ends, or if the vendor's business structure changes (e.g., sale of the company, merger with another company, or bankruptcy)?
- ☐ Are you satisfied that the vendor performs sufficient ongoing assessments and monitoring of performance (preferably by a third party)?
- ☐ Have you checked that the vendor is obligated to provide timely notification to your organization of any software updates, new AI capabilities, declining AI performance, or other changes that may impact the handling of personal information or have other privacy implications?
- ☐ Have you determined if there is a clear mechanism for your organization to report back any observed inaccuracies, biases, non-compliance, or other potential harms? Does the vendor have a contractual obligation to take action in response to these reports?
- ☐ Have you confirmed that your organization retains the contractual right to control, modify and delete the records generated by the AI scribe?
- ☐ Are you satisfied with how the vendor will train its employees on the contractual requirements?
- ☐ Have you considered consulting with your organization's privacy officer or seeking legal advice before entering into a contract with the vendor?

6. Conducting a privacy impact assessment (PIA)

- ☐ Have you completed a privacy impact assessment for your AI scribe initiative?[33]
- ☐ Have you identified risks and developed appropriate mitigation strategies to address those risks?
- ☐ Is there a policy in place to update the PIA whenever there are changes to the AI scribe tool or vendor policies that impact how personal information is handled?

7. Implementing privacy policies and practices

- ☐ Have you updated existing policies and procedures to reflect your use of an AI scribe?
- ☐ Have you incorporated AI scribe best practices into mandatory privacy training for all employees?
- ☐ Have you established policies and practices as required under s. 5 of PIPA to respond to privacy complaints and requests for access to and correction of personal information?
- ☐ Have you established policies concerning the retention and destruction of personal information (e.g., voice recordings and transcripts) generated by the AI scribe and stored by your organization?

[33] See OIPC guidance document *PIAs for the private sector* and suggested *PIA template for organizations*.

- ☐ Have you developed policies requiring active and continuous human oversight of the AI scribe's outputs before they are used in clinical care (i.e. human-in-the-loop)?
- ☐ Have you developed policies and procedures for conducting regular audits to assess the accuracy of the AI scribe's outputs and staff compliance with human-in-the-loop policies?
- ☐ Have you developed a clear mechanism to report observations about inaccuracies, biases, or any other potential harms back to the AI scribe vendor for evaluation and improvement?
- ☐ Will you conduct regular reviews of your policies and practices, given the potential for function creep and evolving privacy implications associated with AI scribes over time?

8. Obtaining patient consent

- ☐ Have you developed a protocol for obtaining and documenting express consent from individuals prior to using the AI scribe?
- ☐ If using a consent form, is the content consistent with BC's PIPA and the language at an appropriate level for patients to understand? (Forms supplied by AI scribe vendors will likely need to be amended.)
- ☐ Will you provide the following information to patients during the consent process?
    - ☐ Clear explanations about what the AI scribe is, and how it works;
    - ☐ Details about how and why their personal information will be collected, used, and disclosed (by both your organization and the AI scribe vendor);
    - ☐ Details about the use or disclosure of any de-identified information by the vendor;
    - ☐ Open and transparent information about any potential risks to their privacy;
    - ☐ Open and transparent information about the extent to which the tool will assist in making decisions about them;
    - ☐ They have a right to decline the use of an AI scribe during their visits, and may also withdraw their consent at any time, without it changing the quality of the health care they'll receive (include details of how they can withdraw);
    - ☐ They have a right to make a complaint to your organization and the OIPC; and
    - ☐ The required information listed under s. 10(1) of PIPA (i.e. "collection notice").
- ☐ Is there a standard and well-communicated protocol in place for clinicians to take notes by other methods if a patient declines use of the AI scribe or withdraws their previous consent?
- ☐ Is there a policy in place to re-evaluate the consent protocol regularly?

    Reminder: Consent must be dynamic. Updated consent is required when changes in the tool's capabilities or vendor practices impact the handling of personal information or create other new privacy implications.