Putting the "Informed" in Informed Consent:
Outlining the risks of AI to your patients

Artificial Intelligence Learning Centre
CHEAT SHEET
CEP

OMA's recommendations for patient consent with AI scribes:

- ✓ Obtain express consent from each patient **the first time** an AI scribe is used.
- ✓ Clearly provide patients the **option to opt-out** of AI scribe use, and make it clear this will not impact their care.

For full guidance, including practitioner obligations and tips on implementation, see AI Scribes Guidance Tips (OMA, 2024).

For information on safeguarding patient data, security for virtual visits, and more, see Privacy & Security Tips (OntarioMD, 2024).

Step 1 Outline **potential risks** from AI scribe use → **Step 2** Describe steps taken to **mitigate** these risks

RISK Unknowns about AI scribes.

This risk is unique to AI products.
While AI scribes offer a lot of promise, they are still very new, and there may be issues with safety and efficacy that have not emerged yet, or are not fully understood. Medical scribes are not regulated in Canada, whether AI, digital, or human.

Practitioners should describe:

- Steps taken to determine appropriateness, safety, and value for the clinic.
- That opting out will not affect patient care.

RISK Secondary use of patient data.

This risk can be unique to AI products.
Secondary use of de-identified patient health information from EMRs is not uncommon. But only AI-powered products are trained to improve based on detecting and fine-tuning patterns from data sets. AI companies actively seek new data to continuously improve their models over time.

Practitioners should confirm:

- The vendor does not use personal health information to train its model or fine-tune its algorithms.
- Personal health information is properly de-identified for any secondary use. This needs to be clearly stated in the clinic's privacy policy.

Putting the "Informed" in Informed Consent:
Outlining the risks of AI to your patients

Artificial Intelligence Learning Centre
CHEAT SHEET
CEP

RISK Sale of patient data to third-parties.

This risk is <u>not</u> unique to AI products. Many private health care technology companies have a commercial interest in selling patient data to third-parties who wish to market additional products to patients.

Practitioners should confirm:

- The vendor does not share patient health information with third parties.

RISK Data stored outside of Canada is no longer protected by Canadian privacy laws.

This risk is <u>not</u> unique to AI products. It is not uncommon for digital healthcare products to store data outside of Canada. Storage in Canada is not required for compliance with PHIPA or PIPEDA.

Practitioners should explain:

- Whether data will be stored only in Canada or will be stored for some period of time outside of Canada in the clinic's privacy policy.
- Steps taken by the vendor to ensure data is protected to a similar standard required by PHIPA/PIPEDA.

RISK Data breach caused by interception or unauthorized access to text transcripts, audio recordings, or clinical documentation.

This risk is <u>not</u> unique to AI products. Electronic medical records or non-AI transcription services hold similar risks for data breaches.

Practitioners should confirm:

- Any strategies already in place that the clinic uses to protect patient data (multi-factor authentication, etc).
- The specific product being used and confirm the product is PHIPA compliant.
- Specifics of vendor practices regarding data encryption, storage, and deletion.

RISK Incomplete health record.

This risk is <u>not</u> unique to AI products. Many different information sources are used to create a health record. Under PHIPA, healthcare practitioners are responsible for ensuring that records are complete and accurate.

Practitioners should describe:

- Practices already in use to ensure a complete and accurate medical record.
- Any new practices put in place to prevent over-reliance on AI tools.