

Simplified Privacy Impact Assessment

For new AI tools in solo and small healthcare practices

Purpose

A Privacy Impact Assessment (PIA) helps you think through how a new AI tool will handle patient and practice information and what to do about any risks before you start using it. It does not replace specialist privacy, legal, cyber security or medico-legal advice.

This tool is built around the federal Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs) and the Health Records and Information Privacy Act 2002 (NSW) (HRIP Act).

Practice name	
AI tool and vendor	
What will the tool do?	<i>Example: draft consultation notes, answer calls, support triage, identify recalls or assist billing.</i>
Assessment completed by	
Date and proposed go-live	
Practice person responsible for the tool	

How to complete this PIA

1

Describe the tool

Write what it does, who will use it and what information it handles.

2

Privacy assessment

Check the tool against the Privacy Act, APPs & HRIP Act

3

Rate the risk

Low: acceptable with routine controls.
Medium: action needed before use. **High:** do not proceed until reviewed.

4

Record actions and sign off

Assign an owner and due date. Review again after major changes or incidents.

Stop and seek advice if:

The tool makes or strongly influences clinical recommendations; patient information is used to train a model; overseas storage or recipients are unclear; subcontractors are not disclosed; the vendor will not provide written answers; a serious data breach could occur; or any risk remains High.

STEP 1. DESCRIBE THE TOOL, PURPOSE AND INFORMATION FLOW

Q1. What is the tool, and what does it do?

e.g. an ambient scribe drafting consult notes, a chatbot triaging patient queries, a predictive tool flagging high-risk patients, or a clinical decision support tool suggesting a diagnosis or treatment. Name the vendor too.

Q2. What personal or health information does it access, use or produce?

e.g. consultation audio or transcripts, patient names and Medicare numbers, clinical notes, appointment or referral history. Health information is always "sensitive information" under the Privacy Act, so extra care applies.

Q3. Where does that information go, and who else can see it?

Is it processed or stored on the vendor's servers, in Australia or overseas? Could it be used to train the vendor's own AI models? Ask the vendor directly if their privacy policy doesn't say.

☐ Pending — need to contact vendor for details

Get written answers

Do not rely only on a sales demonstration. Ask the vendor to provide clear written answers and supporting documents.

Vendor evidence collected

Documents reviewed	☐ Privacy policy ☐ Data processing agreement ☐ Contract ☐ Security report/certification ☐ Breach process
Outstanding questions	
Vendor contact and date	

STEP 2. PRIVACY ANALYSIS – CHECK THE TOOL AGAINST THE PRIVACY ACT

Q4. Have patients been told the tool is in use, and does your Privacy Policy cover it? (APP 1 & 5)

e.g. signage or a verbal notice at check-in, a line in your website Privacy Policy or patient information sheet. Patients should know before, or at the point of, their information being collected by the tool.

Q5. Is what the tool collects and uses limited to its stated purpose and could it be used for anything else? (APP 3 & 6)

e.g. check the vendor's terms for secondary use such as model training; confirm whether data shared is identifiable or de-identified.

☐ Pending — need to contact vendor for details

Q6. If information leaves Australia, what safeguards apply? (APP 8)

e.g. a written guarantee the overseas recipient handles it consistently with the APPs, or hosting limited to a specific country. Ask the vendor for this in writing if it isn't published.

☐ Pending — need to contact vendor for details

Q7. What security measures protect the information, at the practice and the vendor? (APP 11)

e.g. encryption in transit and at rest, staff access controls and multi-factor authentication, vendor security certification such as SOC 2 Type II or ISO 27001:2022.

☐ Pending — need to contact vendor for details

Q8. Does the practice take reasonable steps to ensure information provided to the tool is accurate, complete and up to date? (APP 10)

e.g. patient demographic details, medical history, or other clinical data used by the tool should come from current records and be checked for obvious errors where appropriate. AI outputs may be less reliable if inaccurate or outdated information is provided to the tool.

Q9. Does a clinician always check the tool's output before it goes into the patient record? (APP 10)

e.g. review and correct AI-generated notes, summaries or suggestions before filing. Never let AI output go straight into the record unchecked.

Q10. Can the practice provide patients with access to, and correction of, information generated by the tool? (APP 12 & 13)

e.g. patients should be able to access and request correction of AI-generated information through the practice's usual health record process.

STEP 3. PRIVACY RISK ASSESSMENT - FLAG THE RISKS

Use this rating scale and guide to rate each risk area below.

Rating	Meaning	Required response
LOW	Unlikely to cause meaningful harm, or effective safeguards are in place.	Document and monitor.
MEDIUM	Could cause meaningful harm, or an important control or fact is missing.	Complete action before go-live and consider specialist review.
HIGH	Serious harm is possible, key facts are unknown, or safeguards are inadequate.	Do not proceed until the risk is reduced and appropriately reviewed.

* No AI tool is risk free. The goal is to reduce risk to a level that is reasonable and acceptable for your practice, not to remove it entirely. Where risk remains, record what it is, why it is acceptable and who accepted it.

Rating	Apply this rating when
LOW <i>If ALL apply</i>	■ The vendor has provided written answers and documentation. ■ Security and privacy controls are in place. ■ The practice can meet its privacy obligations. ■ Reasonable safeguards are in place and any risk that remains is unlikely to cause meaningful harm.
MEDIUM <i>If ANY apply</i>	■ Important information is still being confirmed. ■ A privacy or security control needs improvement. ■ Additional actions are required before go-live. ■ There is potential for meaningful harm if something goes wrong.
HIGH <i>If ANY apply</i>	■ Serious harm to patients or the practice could occur. ■ The vendor cannot explain how information is handled. ■ Data location, overseas recipients or subcontractors are unclear. ■ Patient data may be used for AI model training without appropriate safeguards. ■ Significant privacy, security or governance controls are missing.

Risk area	Rating	What you'll do about it
Patient information seen, used or shared beyond what patients would reasonably expect		
A data breach or security incident involving information in the tool		
Errors or "hallucinations" in AI output relied on without being checked by a clinician		
Patients not realising they're interacting with, or being assessed by AI		
Other risk specific to this tool:		

Do not go-live if:

- A high risk remains
- The tool influences clinical decisions
- Patient data may train a model
- Overseas recipients are unclear
- Vendor evidence is inadequate
- The practice cannot meet access, correction, deletion or breach obligations

Selected overall rating ☐ Low ☐ Medium ☐ High

Why this rating was selected

Who reviewed the rating

STEP 4. DECIDE & SIGN OFF

Decision

- ☐ Proceed as planned
- ☐ Proceed with the changes noted below
- ☐ Pause: seek further advice before proceeding

If proceeding with changes, list the actions needed before implementation:

Action	Who	By when

Completed & risk accepted by
(name & role):

Date:

Reviewed by
(name & role):

Date:

Next review date:

e.g. if vendor terms change, or annually