Using Virtual AI Assistants Safely in General Practice

A practical checklist for GP practices

phn CENTRAL AND EASTERN SYDNEY

An Australian Government Initiative

What is a virtual AI assistant?

- A tool that can respond to patients or staff by text or voice. It may support bookings, intake questions, FAQs and simple navigation.
- If it asks symptom questions or suggests next steps, the practice needs stronger governance, clear escalation rules and confirmation of any Therapeutics Goods Administration (TGA) regulatory requirements.

Before you start

- Confirm what the tool will and will not do, how patient information is handled, how patients can reach a person, and who will oversee safe use.
- Staff should be trained before implementation, and the practice should have clear processes for consent, complaints, urgent issues and ongoing review.

1. Vendor assessment and intended use

- ☐ Confirm whether the tool is patient-facing, staff-facing or both.
- ☐ Define what the tool is allowed to do, such as bookings, intake questions, FAQs, recalls or symptom questions.
- ☐ Ask the vendor to confirm whether the tool gives advice about urgency, diagnosis or treatment and whether TGA medical device requirements apply.
- ☐ If the tool is regulated, confirm whether it is included in the Australian Register of Therapeutic Goods or ask the vendor to provide a written reason why this is not required.
- ☐ The vendor clearly discloses whether patient information is used to train AI models or shared with other organisations, and identifies the legal basis for doing so, including whether patient consent is required.
- ☐ Confirm where data is stored, whether any overseas access or storage occurs, how long records are kept and how records can be deleted.
- ☐ Review data encryption, access controls, audit logs and available security certifications, such as SOC 2 or ISO 27001.
- ☐ Confirm the vendor has a privacy and security incident process, including how and when the practice will be notified.

2. Patient consent and transparency

- ☐ Patients are told clearly when they are using AI rather than communicating with a person.
- ☐ Patients are given an explanation of what the tool does, what information it collects, how the information is used and where their information will be stored.
- ☐ Consent is recorded when the tool collects, uses or stores patient information.
- ☐ Patients can choose not to use the AI assistant and can reach a person through a clear alternative pathway.
- ☐ Patient-facing information, such as a website notice, script or poster, explains the tool and its limits.
- ☐ The practice has a workflow to provide a clear human alternative for children, people with intellectual disability or cognitive impairment, people requiring an interpreter, and others who may need additional support.
- ☐ Patients know how to raise a concern or complaint about the tool.

3. Clinical governance and escalation

- ☐ A named lead oversees safe use, quality review and incident management.
- ☐ The practice has clear rules for what the AI assistant can answer and what must be escalated to practice staff.
- ☐ The tool has clear red-flag escalation rules for urgent symptoms, safety concerns and situations where the AI cannot safely respond.
- ☐ The AI assistant does not replace emergency instructions or urgent care pathways.
- ☐ Patient-facing responses and any advice to seek care are regularly reviewed for accuracy, safety, tone and suitability.
- ☐ Incorrect, unsafe, incomplete or concerning responses are logged, reviewed and raised with the vendor when needed.
- ☐ The practice seeks advice from its Medical Defence Organisation (MDO) or insurer, particularly if the tool is patient-facing or gives advice about urgency, diagnosis or treatment.

4. Privacy and cybersecurity

- ☐ A privacy impact assessment is completed before use. For solo practices or practices with up to 5 clinicians, use the CESPHN simplified privacy impact assessment template. Larger or corporate practices may use the Office of the Australian Information Commissioner (OAIC) Privacy Impact Assessment Tool
- ☐ The practice privacy policy and patient notices are updated to reflect use of the AI assistant where required.
- ☐ Staff understand their privacy responsibilities under the Privacy Act 1988 (Cth) and the Health Records and Information Privacy Act 2002 (NSW).
- ☐ Access to chat logs, transcripts and reports is limited to authorised staff.
- ☐ The IT provider or relevant technical lead reviews cybersecurity settings before implementation, including access control, device security, patching and incident response.
- ☐ The data breach response process covers the AI assistant and vendor-related incidents.

5. Staff training and readiness

- ☐ Staff are trained on what the tool can and cannot do before implementation.
- ☐ Staff understand key risks, including incorrect or incomplete responses, bias, over-reliance and failure to escalate.
- ☐ Reception and administration staff can explain the tool, the alternative human pathway and how to handle concerns or complaints.
- ☐ Staff know what to do if the tool fails, gives a concerning response or a patient needs urgent help.
- ☐ Staff do not enter patient information into general-purpose AI tools unless the practice has specifically assessed and approved that use.

6. Implementation and ongoing review

- ☐ The tool has been tested with relevant practice systems and workflows, such as appointment books, phone systems, websites or clinical software.
- ☐ The practice pilots the tool in a limited way before wider rollout.
- ☐ Success measures are agreed before rollout, such as call handling, booking accuracy, patient experience, staff workload and safety incidents.
- ☐ A sample of conversations is reviewed regularly to check that responses are accurate, safe, respectful and suitable for patients.
- ☐ Performance, complaints, incidents, patient feedback and staff feedback are reviewed regularly.
- ☐ Changes to the tool, including new functions or model updates, trigger a review of risk, privacy and governance arrangements.

Caution

Do not use a virtual AI assistant as an emergency response pathway. Do not allow the tool to give clinical advice outside its assessed purpose. Do not hide AI use from patients. Do not enter patient information into publicly available AI tools. Do not assume vendor claims are enough, check privacy, security and data handling arrangements by asking the vendor to provide documentation/proof.

Key message

Virtual AI assistants can support access, navigation and administration, but they do not replace clinical judgement, practice staff or urgent care pathways. Practices should have clear arrangements for transparency, consent, escalation, privacy, incident reporting and ongoing review.

Key resources

- RACGP: **Conversational artificial intelligence (AI)**
- AHPRA: **Meeting your professional obligations when using AI in healthcare**
- OAIC: **Guidance on privacy and the use of commercially available AI products**
- TGA: **Artificial intelligence and medical device software regulation**
- ACSQHC: **AI Clinical Use Guide for Clinicians**
- AMA: **Artificial Intelligence in Healthcare**

Questions

Contact the CESPHN AI Project Officer (digitalhealth@cesphn.com.au), or seek advice from the practice's MDO, indemnity insurer or relevant professional adviser.