AI Reception Agent Trust Pack

Privacy, security, clinical safety, and operational assurance for Australian healthcare practices

Document owner	Quantum Digital Pty Limited
Version	Ver 1.10
Issue date	23 August 2026
Review date	14 Sept 2026
Applies to	AI Reception
Classification	Confidential — customer due diligence

Prepared for healthcare practices evaluating or using an AI-enabled telephone receptionist. This pack explains the intended operating model and provides the schedules needed to record the actual deployment configuration.

How to Use This Pack

This pack should be completed jointly by the service provider and the clinic. It is not a substitute for a privacy impact assessment, legal advice, a data processing agreement, or the clinic's own policies. State and territory health-record and surveillance laws may impose additional requirements.

Assurance at a Glance

Control area	Minimum position before go-live	Evidence
Data minimisation	Only request the information needed for the approved call purpose.	Approved scripts; field map
Transparency	Caller is told they are speaking with an AI agent and whether the call is recorded.	Opening script; privacy notice
Purpose limitation	No advertising, profiling or unrelated model training without a separate lawful basis and clear approval.	DPA; vendor terms
Security	Least privilege, MFA for administrators, encryption and audited access.	Access matrix; security reports
Human oversight	Defined transfer, callback and failure pathways.	Escalation matrix; test results
Clinical safety	No diagnosis, triage or emergency service; urgent warning signs trigger a safe script.	Risk register; conversation tests
Lifecycle	Retention is configured, reviewed, and deletion is verifiable.	Retention schedule; deletion logs
Incidents	24/7 intake and an NDB assessment workflow are assigned.	Incident plan; contact list

Roles and Accountability

Role	Typical accountability
Clinic/healthcare provider	Determines why patient information is collected; approves scripts, workflows and access; maintains the clinical record; handles patient rights and clinical follow-up.
AI reception service provider	Operates the agent under contract; implements agreed security, retention, support, deletion and incident controls; assists the clinic with privacy requests and investigations.
Subprocessors	Provide telephony, speech recognition, language model, hosting, messaging, monitoring or support services only for contracted purposes.
Authorised clinic staff	Review and act on bookings, messages and escalations within their role.
Caller/patient	Receives notice, chooses whether to continue where applicable, and provides information voluntarily.

1. Information the Agent Collects

The agent must collect only the minimum information needed for the approved interaction. Depending on the clinic configuration, this may include:

- Identity and contact details: name, date of birth or another verification attribute, telephone number, email address and preferred contact method.
- Appointment information: requested clinician, service, location, date, time, referral status and booking preferences.
- Administrative health information: reason for the appointment in the caller's own words, relevant referral details, accessibility or communication needs, and limited information required by an approved booking rule.
- Call content and technical data: audio recording if enabled, transcript, call summary, time, duration, caller number, routing events, consent response, transfer outcome and system logs.
- Payment or insurance information only if expressly enabled. Full card details must not enter recordings, transcripts or general logs; use a compliant payment channel.
- Share information about another person only when the caller is authorised to act for them and the workflow records that relationship.

Data-field Register — Complete Before Issue

Field/artefact	Required?	Purpose	System of record	Retention
Caller number	Y	Return call/identity context	TBA	-
Audio	Y	[QA / evidence / disabled]	Retell	12 months
Transcript	Y	Summarisation/task completion	Retell	12 months
Call summary	Y	Clinic follow-up	TBA	12 months
Booking fields	N	Create or change appointment	TBA	Per record law/policy
Logs and metadata	Y	Security, reliability, support	Retell	12 months

2. Why the information is collected

Purpose	Information normally used	Boundary
Answer administrative questions	Question, clinic-approved knowledge, call metadata	No personalised clinical advice.
Book, change or cancel appointments	Identity, contact, booking preferences	Rules approved via scheduling system.
Take and route a message	Contact details, message, recipient or service	Sensitive details kept to the minimum needed.
Verify the caller	Agreed verification attributes	No knowledge-based questions beyond policy.
Transfer or arrange callback	Call context, routing reason, contact details	Human receives a concise, relevant handover.
Quality, security & troubleshooting	Recording/transcript if enabled, logs, outcomes	Access restricted; sampling and retention documented.
Legal and complaint handling	Relevant records and audit logs	Preserved only when required or subject to a legal hold.

Do not use information for unrelated marketing, sale, behavioural profiling, or training a general-purpose model unless the clinic has expressly approved the use and all legal, notice, and consent requirements have been addressed.

3. Where data is processed and stored

Complete the following schedule using vendor documentation and the deployed configuration—not a vendor's general marketing statement. "Region" must cover primary storage, backups, logs, support access and transient processing.

Data stage	Provider/system	Country/region	At rest?	Support access from	Evidence
Call carriage	TBA	Australia	Y	Australia	Clients Telco
Speech-to-text	Retell	US	Y	US	Std Agreement
Agent/language model	TBA	US	Y	US	TBA
Orchestration	TBA	US	Y	US	Std Agreement
PMS / booking	TBA	Australia	Y	Australia	TBA
Recordings/transcripts	Retell	US	Y	US	Std Agreement
Monitoring/support	Quantum	Australia	Y	Australia	Std Agreement
Backups	Retell	US	Y	US	Std Agreement

If personal information is disclosed to an overseas recipient, the clinic and provider must address APP 8 and make the relevant countries visible in the privacy notice. Remote support access may itself be relevant and must be assessed.

4. Third parties that receive data

List every recipient or subprocessor with access to personal information below, including any enabled optional features. The schedule should describe the service, information received, purpose, location and contractual safeguards.

Recipient	Service	Data received	Purpose	Location	Safeguards
Twillio	Telephony	Audio, number, metadata	Connect and route calls	US	DPA; security schedule
Retell	Speech recognition	Audio/transcript	Convert speech to text	US	No-training term; retention setting
Retell	Language model	Transcript/prompt	Understand and respond	US	Enterprise terms; data-use restriction
Retell	Messaging	Name, number, message	Send confirmations/alerts	US	DPA; minimised content
Retell	Cloud/logs	Encrypted data/metadata	Hosting, backup, monitoring	US	Encryption; access logs
Clinic systems	PMS / CRM / email	Booking or message data	Complete requested task	US	Clinic access controls

Communicate subprocessor changes under the contract, with a reasonable objection or termination process where the change materially affects risk.

5. Call-Recording Arrangements

Recording must be an explicit deployment decision. Surveillance and listening-device laws differ across Australia; seek specific legal advice.

Setting	Approved configuration
Recording status	Enabled
Announcement timing	TBA

Setting	Approved configuration
Caller choice	Request human
Pause/redaction	Not required
Access	Client Specified
Transcript treatment	Enabled

Possible Opening Script

INITIAL CALLER NOTICE "Hello, you've reached [Clinic]. I'm [Agent name]. How can I help?"

IF CHALLENGED CALLER NOTICE "This call is recorded and transcribed for {purpose}.] Please do not share payment card details. If this is an emergency, hang up and call Triple Zero (000). You can ask for a person at any time."

If recording can be declined: "Would you like to continue with recording, continue without recording, or speak with our team?" The system should log the response without coercion and honour the selected path.

6. Patient Notification & Consent

Transparency should be layered: a short spoken notice at the start of the call, an accessible privacy collection notice online, and a fuller privacy policy. Notice and consent are related but are not interchangeable. The lawful basis and consent requirement depend on the collection, purpose and applicable law.

Notice element	What to state
Identity	AI Agent's Name.
Collection	Categories of information, including audio and transcripts if applicable.
Purpose	Answer FAQs, booking requests, messaging, transferring
Consequences	What may happen if you do not provide information, including alternative contact methods.
Disclosure	Ask the clinic staff or refer to the Privacy Policy on the clinic's website
Rights	How to request access, correction, deletion where available, or make a complaint.
Choices	Human transfer, callback, non-recorded path if offered, and accessible alternatives.
Clinical limitation	No diagnosis or emergency response; urgent instructions.

Consent should be voluntary, informed, current and specific, and provided by a person with capacity. If the caller is a parent, guardian, carer or representative, the workflow must follow the clinic's authority and identity-verification policy.

7. Access Controls

Control	Required position
Role-based access	Access matches job duties; recordings and transcripts have narrower access than routine bookings.
Least privilege	No shared administrator accounts; permissions default to no access.
Authentication	MFA for administrative and support access; strong identity lifecycle for staff.
Joiner/mover/leaver	Access approved, reviewed on role change and promptly revoked on departure.
Privileged access	Time-limited where possible, separately logged and periodically reviewed.
Vendor support	Ticket-linked, authorised, time-bound and visible to the service owner.
Audit logging	Log sign-in, view, export, edit, configuration and deletion events; protect logs from alteration.

Control	Required position
Encryption	Industry-standard encryption in transit and at rest, with managed keys and rotation.
Tenant separation	Clinic data is logically isolated and cross-tenant access is tested.
Review cadence	[Quarterly] user access review and [annual] control attestation.

Access Matrix — Complete

Role	Bookings	Messages	Transcript	Audio	Export	Config	Delete
Clinic receptionist	R/W	R/W	R	No	No	No	No
Practice manager	R/W	R/W	R	R	No	No	Request
Clinician	R	R	R	R	No	No	No
Provider support	[Ticket]	[Ticket]	[Ticket]	[Ticket]	No	Limited	No
Provider admin	Metadata	Metadata	R	R	Yes	Yes	Execute

8. Retention & Deletion

Retention must be based on purpose, risk, contract and law—not indefinite convenience. The AI service's transient artefacts should usually be shorter-lived than the clinic's official health record. Required clinical and administrative content should be transferred into the designated system of record.

Record	Operational period	Deletion method	Owner	Exception
Audio recording	12 months - enabled	Automated purge	Quantum	Legal hold/incident
Transcript	12 months - enabled	Automated purge	Quantum	Approved QA case
AI call summary	12 months - enabled	Automated purge	Quantum	Clinical record obligation
Call metadata	12 months - enabled	Automated purge	Quantum	Security investigation
Security logs	12 months - enabled	Automated purge	Quantum	Investigation/law
Backups	12 months - enabled	Cryptographic/request	Quantum	Documented hold
Support tickets	Unlimited	Upon request	Quantum	Contract dispute
Test data	30 days	Delete after test	Quantum	None; no live patient data

Authenticate deletion requests, trace them across production systems, exports, and subprocessors, and complete them within the contractually agreed timeframe. Where deletion cannot occur because law or a legal hold applies, restrict access and document the reason. Deletion from active systems and expiry from backups may occur on different timelines and must not be described as instantaneous if it is not.

9. Incident-Response Procedure

A privacy or security incident includes suspected unauthorised access, disclosure, loss, wrong-recipient messaging, cross-clinic exposure, compromised credentials, prompt or knowledge-base manipulation, unsafe output, unavailable transfer, or failure to honour recording or deletion settings.

1. **Detect and report** — staff, monitoring and vendors report suspected events immediately through QD Basecamp.
2. **Contain** — disable affected integrations, revoke credentials, isolate data, stop unsafe calls or recording, and preserve evidence without altering it.
3. **Triage** — assign incident lead; classify severity; identify clinics, people, data types, systems and time window; consider clinical as well as privacy harm.
4. **Notify customer** — provider informs the clinic within 8 hours of confirmed or reasonably suspected impact and provides continuing updates.

5. **Investigate** — establish facts, affected records, access, exfiltration, configuration changes and subprocessor involvement; maintain an evidence timeline.
6. **Remediate** — close the weakness, reset access, correct misdirected information, restore safe service and test before resuming.
7. **Communicate** — coordinate legally required notices, patient support, regulator engagement and internal briefings; avoid speculation.
8. **Review** — document root cause, control improvements, owner and due dates; verify completion and share an appropriate post-incident report.

Severity & Notification Targets

Severity	Example	Initial internal response	Customer notice
Critical	Large health-data exposure; active attacker; unsafe system creating immediate clinical risk	Immediate, 24/7	Immediately; target [≤1 hour]
High	Confirmed unauthorised access; wrong-clinic disclosure; material recording breach	Immediate, 24/7	Target [≤4 hours]
Medium	Contained limited disclosure; control failure without confirmed access	Same business day	Target [≤24 hours]
Low	Attempt blocked; no data affected; minor reliability issue	Business process	Periodic or on request

PRESERVE DECISION RIGHTS The clinic should lead patient and regulator communications about its records unless the contract or law requires otherwise. The provider must not delay facts needed for the clinic's assessment.

10. Notifiable Data Breach Procedure

Under the Commonwealth NDB scheme, covered entities must notify affected individuals and the Australian Information Commissioner when an eligible data breach is likely to result in serious harm and remedial action has not prevented that likely harm. State and territory schemes or sector obligations may also apply.

9. **Suspect** — open an NDB assessment when there are reasonable grounds to suspect an eligible data breach.
10. **Assess promptly** — gather evidence and complete the assessment within the statutory timeframe applicable to the entity. Under the Commonwealth scheme, take all reasonable steps to finish within 30 calendar days.
11. **Test eligibility** — determine whether there was unauthorised access or disclosure, or loss likely to lead to it; whether serious harm is likely; and whether remedial action has prevented that likely harm.
12. **Consider serious harm** — sensitivity of health information, volume, security measures, who may have obtained it, likely misuse, affected individuals' circumstances, and physical, psychological, financial, reputational or other harm.
13. **Take remedial action** — recover information, obtain reliable deletion, revoke access, reset credentials, stop disclosure and reduce likely harm.
14. **Decide and record** — the Privacy Officer and legal adviser document the facts, reasoning, evidence, affected population, and decision.
15. **Notify if required** — prepare the statutory statement, notify the OAIC and affected individuals using an approved method as soon as practicable.
16. **Support and review** — provide practical protective steps and contacts; monitor new facts; update notices if materially required; complete post-incident actions.

Notification Area	Name
Clinic incident lead	[Name, mobile, email]
Clinic Privacy Officer	[Name, mobile, email]
Provider incident lead — 24/7	[Name/team, number, email]
Legal adviser	[Contact]
Cyber insurer / forensic adviser	[Contact]

Notification Area	Name
OAIC notification owner	[Role]
Patient communications owner	[Role]

11. Human Escalation Rules

The agent must make transfer or callback easy, preserve the caller's request for a person, and never trap a caller in a repeated automated loop. A concise handover should include only information relevant to the receiving staff member.

Trigger	Agent action	Priority
Caller asks for a person	Transfer during opening hours; otherwise offer an approved callback/message pathway.	Routine unless risk cues exist
Agent is uncertain/fails twice	Stop guessing; apologise; transfer or take a minimal message.	Prompt
Identity cannot be verified	Do not disclose information or change sensitive details; transfer call	Prompt
Complaint or privacy issues	Answer questions; refer to Privacy Policy, transfer call	Prompt
Medication, diagnosis, results or advice	Do not answer; transfer to staff	Restricted
Distress, self-harm, violence or urgent symptoms	Use the clinic-approved safety script; direct to emergency services if there is immediate danger; alert the human team if safe and configured.	Urgent / emergency
Child or vulnerable person concern	Avoid investigation; collect minimum details; escalate urgently under clinic policy.	Urgent
System/integration failure	Do not claim a booking succeeded; provide alternative contact and flag the failure.	Operational

Handover minimum

- Caller name and callback number, subject to verification policy.
- Reason for transfer in a short, neutral summary.
- Actions already attempted and whether any booking or message was actually created.
- Relevant urgency or safety cue without making a diagnosis.
- Recording/consent status and any caller objection.

12. Emergency & Clinical-risk Limitations

CORE LIMITATION: The AI receptionist is an administrative service. It is not a clinician, does not diagnose, does not determine clinical urgency, does not interpret results, and must not be relied upon as an emergency service.

The agent may use only clinic-approved safety wording designed to recognise broad risk cues and safely route the caller. Keyword detection is imperfect: callers may describe symptoms indirectly, use another language, be unable to speak, or lose connection. The service must never promise continuous monitoring or emergency dispatch unless that capability genuinely exists and is clinically governed.

Emergency Script

AUSTRALIA "I'm an administrative AI receptionist and cannot assess or manage an emergency. If you or someone else is in immediate danger, hang up and call Triple Zero (000) now. If you need urgent medical advice and it is not an immediate emergency, contact your usual clinician or an appropriate urgent-care service. Would you like me to connect you to the practice team if they are available?"

Mental-health, family-violence, poisoning, paediatric and other high-risk scripts should be separately approved for the clinic's services, state or territory and operating hours. Do not overload the opening greeting with condition-specific helplines; provide an approved service only when relevant and keep emergency instructions first.

Clinical-safety Controls

- Approved knowledge base limited to administrative content and carefully governed general information.
- Explicit prohibited topics and refusal/transfer responses for clinical advice.
- Adversarial and scenario testing before release, after material changes and at a scheduled cadence.
- Monitoring of missed escalation cues, false reassurance, booking failures and unsafe summaries.
- Named clinical owner with authority to pause the agent.
- Change control for prompts, models, voices, integrations and knowledge sources.
- Fallback when telephony, PMS, model or transfer services are unavailable.
- Clear display to staff that AI-generated summaries require review and may contain errors.

Operational Assurance & Evidence Register

Attach or link the following evidence. Record the version and review date so the pack remains auditable.

Evidence item	Owner	Version/date	Status
System and data-flow diagram	Quantum	Ver 1.10	Available Upon Request
Privacy impact assessment	Client	[Date]	Website Link
Data processing agreement	Client	[Date]	Website Link
Subprocessor register	Client	[Date]	Website Link
Vendor security reports/certifications	Quantum	-	Available Upon Request
Penetration test summary	-	-	n/a
Access MFA control (unless using client's license)	Quantum	Ver 1.10	Available Upon Request
Retention configuration and deletion test	Quantum	[Date]	Available Upon Request
Incident and NDB plans	Quantum	-	With serious occurrence
Conversation and clinical-safety test report	Quantum	-	Available Upon Request
Business continuity/recovery test	Quantum	-	Available Upon Request
Insurance certificates	Quantum	-	Available Upon Request

Go-live Approval Checklist

- ☐ Legal entities, product name, responsibilities and contacts are correct.
- ☐ All data fields and purposes have been approved and minimised.
- ☐ Every storage, processing, backup and support location is verified.
- ☐ All subprocessors and cross-border disclosures are documented.
- ☐ Recording status, script, consent choice, redaction and retention are tested.
- ☐ Privacy notice and clinic privacy policy are updated and accessible.
- ☐ Role permissions, MFA, logging and staff access reviews are operating.
- ☐ Retention rules and end-to-end deletion have been tested.
- ☐ Incident contacts work outside business hours; NDB decision roles are assigned.
- ☐ Human transfers, callbacks, outage fallbacks and failure messages have been tested.
- ☐ Emergency, distress and prohibited-clinical-advice scenarios have passed testing.
- ☐ The clinic owner, Privacy Officer, security owner, and clinical owner have signed below.

Approval	Name	Signature	Date
Clinic operational owner			
Clinic Privacy Officer			
Provider security/privacy owner			
Clinical safety owner			

Patient-facing Short Notice

Add the following to the Clinic Privacy Policy or seek further legal advice.

WEBSITE / APPOINTMENT NOTICE [Clinic] uses an AI receptionist to answer calls, manage appointments and take messages. The service may collect your contact details, appointment information and the information you choose to provide. [Calls are recorded and transcribed for {purpose}. You may {decline recording / request a person}.] Our contracted technology providers may handle information in [countries]. The AI receptionist does not provide medical advice or emergency care. For immediate danger, call Triple Zero (000). See [privacy notice URL] or contact [Privacy Officer details] for access, correction or complaints.

Reference Framework

This pack is designed around the Privacy Act 1988 (Cth), the Australian Privacy Principles, OAIC health-privacy and data-breach guidance, and the need to check applicable state and territory health-record, privacy, and surveillance legislation. The following sources should be reviewed when the pack is finalised:

OAIC — Guide to health privacy

OAIC — Australian Privacy Principles

OAIC — APP 5 notification of collection

OAIC — APP 8 cross-border disclosure

OAIC — APP 11 security and deletion

OAIC — Data breach preparation and response

Australian legislation — Privacy Act 1988

Australian Digital Health Agency — Clinical safety

Revision history

Version	Date	Change	Approved by
1.10	14 Sep 2026	Initial completion draft	[Pending]