

● ARIA PRODUCTS

Data Processing Agreement

This agreement sits alongside your Standard Form of Agreement and our Privacy Policy. It is the written contract under which Pear processes personal information — including health information — on your behalf when you use Aria.

Who does what

You are the APP entity and the health service provider. You remain responsible for the patient record, for telling patients how their information is handled, and for clinical judgement. Pear processes that information only to deliver the Aria products you have switched on, only in Australia, and never to train an AI model unless you have expressly consented in writing.

● PARTIES

01 • Who this agreement is between

This Data Processing Agreement (Agreement) is between:

- The Customer named in the signing block (or, if you accept this Agreement online or by enabling an Aria product, the account holder named on that account) — you; and
- Pear Australia Pty Ltd (ABN 94 624 986 554) of 25 Gordonia Grove, Baulkham Hills NSW 2153 — Pear, we, us.

It takes effect on the earlier of the date both parties sign it, the date you accept it as part of an Aria order, or the date you first enable an Aria product on a Pear service. It continues for as long as we process Customer Data for you, and for any period after that during which we still hold Customer Data.

Capitalised terms not defined here have the meaning given in your Standard Form of Agreement (SFOA) or in the Privacy Act 1988 (Cth). This Agreement prevails over the SFOA and our Privacy Policy to the extent of any inconsistency about how Customer Data is processed. It does not change prices, service levels, or anything else in the SFOA.

● SCOPE

02 • What this agreement covers

This Agreement covers every current and future Aria product we supply to you, including:

- Aria Receptionist (also called Aria Connect) — answers live calls, handles common enquiries, books, reschedules and cancels appointments where you enable it, takes messages, and escalates the rest to your team.
- Aria Queue Manager — answers instead of a hold message, handles simple requests such as cancellations, and queues the rest for reception.
- Aria Voicemail (AI Voicemail) — takes structured after-hours messages, including name, reason, urgency and a callback number.

- Aria Scribe (Call Intelligence) — transcribes consults and drafts notes, referral letters and similar documents from audio you choose to capture.
- Aria Fax (X-Fax and X-Fax Intelligence) — receives, sends, stores, reads, summarises, flags and routes faxes, including filing into a practice management system where you enable a connector.
- Any other Aria module you later enable — including Assist, Translate, Care, Capture, Debrief, Billing, Compliance, multi-site tools, and any successor or add-on we make available under the Aria name.

It also covers the supporting infrastructure those products run on: the phone system integration, portals, inboxes, directories, notifications (email, SMS and in-product), connectors to practice management software, and the storage of recordings, transcripts, faxes, messages and drafts.

It does not cover Pear's ordinary carriage, internet or billing services except to the extent those services carry Aria traffic. Those remain under the SFOA and our Privacy Policy.

● ROLES

03 • Roles under privacy law

For Customer Data processed through Aria:

- You are the APP entity that collects the information and determines the purposes of the collection. Where the information is health information, you are also the health service provider under the applicable state or territory health records law.
- Pear is your contracted service provider. We handle Customer Data on your behalf and only on your documented instructions, which are this Agreement, your configuration of the products, and any written instruction you later give us that is consistent with this Agreement and the law.
- Callers, patients, referrers, staff and other individuals whose information appears in Aria are not parties to this Agreement. You remain responsible for your privacy notices to them.

Nothing in this Agreement makes Pear a health service provider, a treating practitioner, or the holder of the official patient record. Clinical judgement, diagnosis, treatment decisions and the integrity of the clinical record stay with you and your registered practitioners. Aria does not make clinical decisions and does not decide whether anyone receives care.

We are bound by the Privacy Act 1988 (Cth) and the Australian Privacy Principles, the Telecommunications Act 1997 (Cth), the Telecommunications (Interception and Access) Act 1979 (Cth), and — where we handle health information for you — the Health Records and Information Privacy Act 2002 (NSW) and equivalent state and territory health privacy laws. This Agreement is the written contract those laws expect you to have with a processor.

● DATA

04 • What we process

Customer Data means personal information, sensitive information and health information that we process because you use an Aria product. It includes information about your patients, callers, referrers, staff and contractors that enters Aria through a call, a fax, a message, a booking, a consult recording, a practice-management connector, or anything you or your staff type, upload or configure.

Depending on the products you enable, Customer Data typically includes:

- Identity and contact details — names, phone numbers, dates of birth, addresses, email addresses, and the practice, provider or inbox a record belongs to.
- Call audio, voicemail audio, transcripts, summaries, intent tags, urgency flags and routing decisions.
- Appointment, cancellation, waitlist and recall details.
- Fax images and text, sender and recipient details, document type, summaries and filing metadata.
- Consult recordings, draft SOAP notes, referral letters, certificates, care-plan text and similar drafts produced by Aria Scribe or a later clinical-documentation module.
- Limited clinical content the caller states, or that you choose to make available through a connector or configuration — for example a reason for visit, a result description on a fax, or history you surface for a draft note.
- Staff identifiers, extension numbers, inboxes, directories and audit logs of who did what in Aria.
- Technical logs needed to run and secure the service — timestamps, call identifiers, device and session metadata.

We do not need, and you should not send us, more clinical content than a product actually requires. You control what a connector exposes and what a clinician chooses to record.

Account, billing and credit information about your practice as Pear's customer is not Customer Data under this Agreement. We handle that as an APP entity in our own right, under our Privacy Policy and Credit Reporting Policy.

● PURPOSE

05 · Why we process it, and only that

We will process Customer Data only:

- To provide, maintain, support and improve the specific Aria products you have enabled, including routing, transcription, summarisation, drafting, filing, notification and reporting.
- To secure those products, prevent abuse, diagnose faults and measure that they are working.
- To comply with a law that applies to us — including a warrant, a telecommunications interception or access obligation, an emergency-services obligation, or a court order.
- To protect the life, health or safety of any person, including directing a caller to 000 where Aria recognises an emergency.
- On any other documented instruction you give us in writing.

We do not train AI models on your Customer Data

We will not use personal information, sensitive information or health information to train, fine-tune or evaluate a foundation model or any other general AI model, unless you have expressly consented in writing for a defined purpose. We may use de-identified information — with identifiers removed so it cannot reasonably be re-identified — to check quality and improve Aria. You can opt your practice out of even that de-identified use by emailing hello@peartelco.com.au. Opting out does not reduce the service you receive.

We will not sell, rent or trade Customer Data. We will not use it to market Pear products to your patients. We will not use it to make a decision about a Pear account, a credit application, or whether anyone receives care.

● INSTRUCTIONS

06 • Your instructions to us

Your documented instructions are: this Agreement; the products, sites, numbers, inboxes, directories, scripts, opening hours, escalation rules and connectors you configure; and any later written instruction from an authorised contact on your account.

If we reasonably believe an instruction would put us in breach of the Privacy Act, a health records law, telecommunications law or a court order, we will tell you and we will not follow that instruction until it is resolved — unless the law requires us to act immediately, in which case we will tell you as soon as we are allowed to.

Your authorised contacts may give operational instructions through the product itself (for example changing an after-hours greeting, connecting Best Practice, or turning recording on for a consult). Those count as documented instructions.

● YOUR DUTIES

07 • What you are responsible for

You must:

- Have a lawful basis to collect the Customer Data and to engage us to process it — including any consent a health records law or professional code requires for recording a consult or a call.
- Give patients, callers and staff a collection notice that covers Aria, in line with APP 5 and any applicable health privacy principle. Our Privacy Collection Statement is written for Pear's own customers; it is not a substitute for your notice to patients.
- Configure Aria so it only receives the information a product needs. Turn off recording, connectors or filing where you do not have a basis to use them.
- Obtain any consent required before a consult is recorded for Aria Scribe, and stop a recording if a patient withdraws that consent.
- Review, edit and accept drafts before they become part of a clinical record. Aria drafts; your practitioner signs.
- Keep access credentials, inboxes and staff accounts under your control, and tell us promptly when a staff member should lose access.
- Not use Aria as a clinical decision-support device that replaces professional judgement, and not represent to patients that Aria is a treating practitioner.
- Comply with our Acceptable Use Policy. You must not use Aria to collect information you could not lawfully collect yourself.

If a patient, caller or regulator contacts us about Customer Data, we will point them to you unless the law requires us to deal with them directly, or unless the request is about information we hold as Pear's own APP entity (for example a bill).

● OUR DUTIES

08 • What we will do

We will:

- Process Customer Data only on your documented instructions and as this Agreement allows.
- Take the security measures in section 10 and Schedule 3 — reasonable steps under APP 11 to protect Customer Data from misuse, interference, loss, and unauthorised access, modification or disclosure.
- Ensure anyone we authorise to handle Customer Data is bound by confidentiality and trained on privacy.
- Help you meet your obligations to respond to access, correction and complaint requests, and to assess and notify eligible data breaches, to the extent the relevant information sits in our systems.
- Delete or return Customer Data when this Agreement ends, in line with section 13, except where we must keep a copy under law.
- Tell you if we can no longer meet our obligations in this Agreement.
- Not disclose Customer Data except as section 09 allows.

● DISCLOSURE

09 · Who else may see it

We disclose Customer Data only:

- To your own authorised users, and into the practice management system or inbox you have connected.
- To a sub-processor listed in Schedule 2, or later appointed under section 09, and only to the extent needed for that sub-processor's task.
- To a carrier or network operator, solely to carry the underlying call, message or fax.
- To emergency service organisations, where Aria or a caller engages 000 or where the law requires it.
- To the operator of the Integrated Public Number Database, and to law enforcement or national security agencies, where telecommunications law requires it. Where the law allows us to tell you, we will.
- To the OAIC, a state or territory health complaints body, the TIO, a court, or our professional advisers under confidentiality, where necessary.
- To a buyer of our business, under confidentiality, if we ever sell it — and only if that buyer is bound to protect Customer Data to at least the standard of this Agreement.
- With your written consent.

Before we appoint a new sub-processor that will handle Customer Data, we will update the list we maintain for customers and give you at least 14 days' notice of a material change, except where we have to move faster to keep the service secure or available. If you reasonably object on privacy grounds we will work with you on an alternative; if we cannot agree, you may stop using the affected product without penalty for that product.

Every sub-processor is bound by a written contract that requires protection of Customer Data to a standard no less than this Agreement, use only for the appointed task, and no onward disclosure except as that contract and the law allow. We remain responsible to you for what a sub-processor does.

● LOCATION

10 · Australia only

Customer Data stays in Australia

Customer Data is stored in Australia on encrypted servers. It is not transferred outside Australia and it is not accessed or processed from outside Australia. Aria is operated and supported from within Australia. We do not use offshore support, offshore processing or an offshore call centre for Aria. If that position ever changes we will not move Customer Data offshore until we have updated this Agreement, notified you, and complied with APP 8.

A caller who rings you from overseas is still processed in Australia. A fax sent to you from overseas is stored and read in Australia. That inbound communication is not a disclosure by us.

● SECURITY

11 • How we protect it

The measures in Schedule 3 are the baseline. In plain terms:

- Encryption in transit (current TLS) and encryption at rest.
- Role-based access, individual logins and multi-factor authentication. Access to health information is limited to people whose job requires it.
- Logging of access and of changes, and review of those logs.
- Staff confidentiality obligations and privacy training.
- Secure deletion or de-identification when we no longer need a record.
- Supplier contracts that require equivalent protection.

No system is perfect. If you suspect Customer Data has been compromised, ring 1300 007 327 or email hello@peartelco.com.au immediately.

● BREACH

12 • Data breaches

We are covered by the Notifiable Data Breaches scheme in the Privacy Act. If Customer Data is lost, or accessed or disclosed without authorisation, we will:

- Contain — act immediately to stop further access or loss.
- Tell you — notify your authorised contact without undue delay, and in any case within 72 hours of becoming aware of a suspected eligible data breach affecting Customer Data, unless a law prevents us from telling you. Our notice will cover what we know, what information is involved, what we are doing, and what we recommend you do.
- Assess — assess the suspected breach as quickly as we can, and in any case within 30 days.
- Cooperate — give you the information you reasonably need to decide whether you must notify the OAIC, a state health complaints body, affected individuals, or your professional indemnity insurer, and to make that notification. Where both of us have a notification duty, we will agree who sends what so people are not notified twice with conflicting accounts.
- Fix — remediate the cause and tell you what changed.

You remain responsible for notifications that the law places on you as the APP entity or health service provider. We remain responsible for notifications the law places on us. We will not notify your patients directly about a Customer Data incident without your agreement, except where we are required to, or where we cannot reach you in time and serious harm is likely.

● RIGHTS

13 • Access, correction and complaints

If an individual asks us for access to, or correction of, Customer Data, or complains about how it was handled, we will tell you promptly and give you the information we hold so you can respond. We will not respond on the merits ourselves unless you ask us to, or the law requires us to.

We will give you reasonable assistance — including exports of recordings, transcripts, faxes, messages and logs we hold — so you can meet a 30-day access or correction deadline, an OAIC or health-complaints investigation, or a professional-standards request. We do not charge for ordinary assistance. If a request is unusually large we will tell you before we start and agree the effort with you.

Individuals can always contact our Privacy Officer at hello@peartelco.com.au about how Pear itself handles information. That does not shift your obligations as the practice.

● KEEPING

14 • How long we keep it, and what happens when you leave

Default retention for Aria Customer Data is set out in Schedule 1. You may ask us in writing for a shorter or longer period where the product allows it. We will not keep Customer Data longer than we need it to deliver the product, to resolve a dispute, or to meet a legal obligation — whichever is longer.

When this Agreement ends, or when you disable a product:

- You may, within 30 days, ask us to return Customer Data in a reasonable electronic form or to make it available for export from the product.
- After that 30-day window — or sooner if you ask us to delete rather than return — we will securely delete or irreversibly de-identify Customer Data from live systems, except for copies we must keep under law (for example a telecommunications intercept record, a tax record that happens to contain a number, or a record of a complaint).
- Backup copies age out on the backup cycle and are not restored into live systems except to recover from a fault.
- We will confirm deletion in writing if you ask.

Disabling a product does not delete Customer Data already written into your practice management system. That copy is yours.

● AUDIT

15 • Showing our working

On written request, no more than once in any 12-month period unless you have a reasonable suspicion of a breach of this Agreement, we will provide:

- A current copy of this Agreement, our Privacy Policy, and the sub-processor list.
- A written description of the security measures then in place.
- A summary of any eligible data breach affecting your Customer Data in the previous 24 months.
- Answers to a reasonable security questionnaire.

If that is not enough for a regulator, an accreditator or your professional indemnity insurer, we will discuss a supervised inspection of relevant controls, at a mutually agreed time, in a way that does not compromise other customers' information or the security of the service. You meet your own costs. We meet ours unless the inspection finds we are in material breach, in which case we meet the reasonable costs of that inspection.

● AI

16 • How Aria uses automation

Aria uses automated processing to understand speech and documents, to classify them, to draft text, to suggest a route or a filing location, and to recognise an emergency. That processing is how the product works. It is not an automated decision that has a legal or similarly significant effect on an individual. In particular:

- Aria does not diagnose, prescribe, or decide whether a person receives care.
- Aria does not decide anything about a Pear account, a credit application, a suspension or a complaint.
- Draft notes, summaries and suggested item numbers are suggestions. A practitioner must review them before they become part of a record or a claim.
- Triage and urgency flags are an aid for your team, not a clinical conclusion.

You must not rely on Aria as a substitute for a registered practitioner, and you must not tell patients that they have been assessed by a doctor when they have spoken only to Aria.

● STAFF

17 • Personnel and confidentiality

Only Pear personnel and authorised sub-processor personnel whose role requires it may access Customer Data. Each of them is bound by confidentiality that survives their engagement. We will remove access when the role no longer requires it. We will not use Customer Data to identify a patient in any internal demonstration, marketing material or case study.

● LIABILITY

18 • Liability and insurance

Each party's liability under this Agreement is subject to the limitations and exclusions in the SFOA, except that nothing in the SFOA limits a party's liability for a breach of the Privacy Act, a health records law, or a confidentiality obligation in this Agreement, to the extent that liability cannot be limited under those laws or the Australian Consumer Law.

You indemnify Pear against a claim by a patient, caller or regulator arising from your failure to obtain a required consent, to give a required collection notice, to review a draft before it is filed, or to configure the product lawfully — except to the extent the claim is caused by our breach of this Agreement.

We maintain public liability and professional indemnity insurance appropriate to a carriage service provider that also supplies these products. Evidence of cover is available on request.

● CHANGES

19 • Changes to this agreement

We may update this Agreement when a product changes, when the law changes, or when we add a module. The current version will always be available on our website. Material changes that reduce your rights or increase what we may do with Customer Data will be notified to your authorised contact at least 14 days before they take effect. If you do not agree, you may disable the affected product before the change takes effect. Continuing to use the product after the effective date is acceptance of the update.

A change to Schedule 1 that only describes a new Aria module you have not enabled does not require notice until you enable that module.

● GENERAL

20 • General

- Law. This Agreement is governed by the laws of New South Wales. The courts of New South Wales have exclusive jurisdiction, except that either party may seek urgent interlocutory relief in any competent court.
- Severability. If a clause is unenforceable, the rest remains in force.
- Waiver. A failure to enforce a right is not a waiver of it.
- Entire agreement. This Agreement, the SFOA and the order for the relevant Aria products are the entire agreement about processing of Customer Data. A practice-management vendor's terms apply between you and that vendor, not to us, except to the extent we have a separate connector agreement with that vendor.
- Notices. Notices under this Agreement may be emailed to hello@peartelco.com.au and to the authorised email address on your account.
- Counterparts. This Agreement may be signed in counterparts and electronically. An electronic signature is enough.
- Order of documents. For processing of Customer Data: this Agreement, then the Privacy Policy, then the SFOA. For everything else: the SFOA.

● SCHEDULE 1

S1 • Processing details by product

This schedule describes the processing for each Aria product. Only the rows for products you have enabled apply. Enabling a further product later adds that row automatically.

Common to every Aria product

- Subject matter: provision of the enabled Aria product to an Australian medical or allied-health practice, or to another business customer who has enabled Aria.
- Duration: the life of the product on your account, plus the retention period below, plus backup ageing.
- Nature: collection, recording, organisation, storage, retrieval, transcription, classification, drafting, disclosure to your users and connected systems, erasure.

- Purpose: section 05.
- Categories of data subject: patients and prospective patients; callers and people they call about; referrers and other providers; your staff and contractors; senders and recipients of faxes.
- Special categories: health information and other sensitive information that appears in a call, a fax, a message or a draft.

Product-specific processing

Product	Typical Customer Data	Default retention	Where it goes besides Pear
Aria Receptionist / Connect	Live call audio; transcript and summary; caller identity and number; reason for call; appointment requests; symptoms or urgency the caller states; booking writes you enable.	Call recordings and transcripts: 90 days, unless you set a different period or a complaint or legal hold applies.	Your reception inbox and nominated staff. Your PMS, if a booking connector is on. Email or SMS notifications you configure.
Aria Queue Manager	Live call audio while Aria is on the line; structured message (name, reason, urgency, callback); queue events.	Recordings and messages: 90 days, unless you set a different period or a hold applies.	Your reception inbox and nominated staff. Email notifications you configure.
Aria Voicemail	Voicemail audio; structured message (name, reason, urgency, callback); after-hours context.	Audio and structured messages: 90 days, unless you set a different period or a hold applies.	Your reception inbox and nominated staff. Email or SMS notifications you configure.
Aria Scribe / Call Intelligence	Consult audio you choose to capture; transcript; draft SOAP notes, referral letters, certificates and similar; any history you surface for the draft.	Audio and drafts: 30 days after the consult unless you export or file them sooner. Filed copies in your PMS are yours and follow your record-keeping rules.	The clinician's inbox and the PMS or document destination you choose. Nothing is filed until a person acts.
Aria Fax / X-Fax Intelligence	Fax images and extracted text; sender and recipient numbers and directory names; document type; summary; urgency flag; filing metadata.	Fax images and intelligence output: 12 months, unless you set a different period, file them into a PMS, or a hold applies.	Your fax mailbox and nominated provider inboxes. Best Practice or another PMS if a connector is on and a person files the fax.
Later modules (Assist, Translate, Care, Capture, Debrief, Billing, Compliance, multi-site)	Only the data that module needs — for example a recall list you load, a language pair, a consult already in Scribe, or billing codes a draft suggests.	The period published for that module when you enable it, or 90 days if none is published.	The destinations you configure for that module. We will describe them in the product notice at enablement.

Telecommunications metadata that the law requires us to retain as a carriage service provider is retained for the statutory period and is not Customer Data under this Agreement, even if a call also passed through Aria.

● SCHEDULE 2

S2 • Sub-processors

The categories below are authorised from the commencement of this Agreement. A current named list is available from hello@peartelco.com.au and will be provided with any material-change notice.

Category	What they do	Where	Customer Data they may handle
Australian-region cloud infrastructure	Host compute, storage, databases, queues and backups for Aria.	Australia (for example an Australian availability region of a public cloud).	Whatever the hosted product stores — recordings, transcripts, faxes, messages, configuration.
Onshore AI processing infrastructure	Run speech-to-text, document understanding and generation for Aria.	Australia.	Audio, fax images and text submitted to a model at inference time. Not used for training unless section 05 consent applies.
Carriers and interconnect	Carry the underlying telephone call, SIP trunk or fax transmission.	Australia, plus the public telephone network to the extent a call or fax originates or terminates elsewhere.	Signalling and media for the duration of the transmission. Not stored by Pear as Customer Data beyond what Schedule 1 allows.
Email and SMS notification providers	Deliver the alerts and message copies you configure.	Australia, unless a recipient's own mailbox provider stores mail offshore after delivery — that is outside our control.	The content of the notification you configured (for example a voicemail summary emailed to reception).
Practice-management connectors	Write or read the records you instruct — appointments, filed faxes, copied notes.	Australia, on the vendor's systems under your own contract with that vendor.	Only the fields you enable. The PMS vendor is your processor or APP entity, not ours, once the record is in their system.
Support and professional advisers	Diagnose a fault you have raised; legal, audit and insurance advice to Pear.	Australia.	The minimum needed for the ticket or the advice, under confidentiality.

A named individual contractor working under Pear's direction in Australia is personnel, not a sub-processor.

● SCHEDULE 3

S3 · Security measures

Pear maintains, and will maintain for the term of this Agreement, at least the following:

Governance

- A named Privacy Officer reachable at hello@peartelco.com.au.
- Privacy and security training for staff at induction and at least annually.
- Confidentiality obligations in every staff and contractor agreement.
- A written incident-response process aligned to the Notifiable Data Breaches scheme.
- Vendor due diligence before a sub-processor handles Customer Data.

Access control

- Unique user accounts. Shared logins are not used for systems that hold Customer Data.
- Multi-factor authentication for staff access to production systems.
- Role-based access; health information is not available to staff who do not need it.
- Prompt revocation when a person leaves or changes role.
- Customer-side access is limited to accounts you create and can revoke.

Encryption and isolation

- TLS for data in transit over public networks.
- Encryption at rest for stored Customer Data.
- Logical separation of customer environments in application systems.
- Production Customer Data is not copied into non-production systems unless de-identified.

Operations

- Logging of access to systems that hold Customer Data, and of administrative changes.
- Malware protection and timely security patching on systems we control.
- Backups stored in Australia, encrypted, with a tested restore process.
- Secure destruction of decommissioned media and of expired Customer Data.

Buildings and people

- Production systems are in professionally managed Australian data centres or equivalent Australian cloud regions, not on an unattended office desk.
- Pear offices do not keep standing copies of patient recordings or faxes on local disks.
- Paper, if any ever exists, is locked and shredded when no longer needed.

SCHEDULE 4

S4 • Execution

Executed as an agreement. If you accepted this Agreement by enabling an Aria product or by an online tick-box, that acceptance is your signature and the account-holder details on file are your signing-block details.

Signed for the Customer	Signed for Pear Australia Pty Ltd
Practice / entity name	Entity
_____	Pear Australia Pty Ltd
ABN	ABN
_____	94 624 986 554
Address	Address
_____	25 Gordonia Grove, Baulkham Hills NSW 2153
Authorised contact email	Privacy Officer
_____	hello@peartelco.com.au
Signature	Signature
_____	_____
Name / position / date	Name / position / date
_____	_____

● TALK TO US

Questions about this agreement

Email hello@peartelco.com.au or call 1300 007 327 and ask for the Privacy Officer. There is no charge, and asking does not affect your service. If you want this agreement in large print or as a plain-language summary, say so and we will provide it.