

Dental Privacy Edge Map

By Scott Farrell — LeverageAI · dental.leverageai.com.au/about

A map of the systems around the PMS where patient data may move before AI is switched on.

Dental Privacy Edge Map

Prepared for Example Dental Clinic, Sydney · 15 Jun 2026 · part of your private Dental AI Blueprint. Review and adapt before adopting — general guidance, not legal advice.

Your PMS is not the only patient system.

Two privacy laws apply in NSW. As well as the Commonwealth *Privacy Act 1988* and its Australian Privacy Principles (APPs), dental practices in NSW are also bound by the NSW *Health Records and Information Privacy Act 2002* (HRIP Act) and its Health Privacy Principles (HPPs). Read the considerations here against both. General information, not legal advice.

The edge problem

Most dental practices have a good PMS. The privacy risk in the AI era often moves to the systems *around* the PMS: booking widgets, contact forms, email inboxes, AI scribes, cloud drives, call tools, chat widgets, marketing platforms, and AI tools.

This guide maps the common edges so practices can review them before switching on AI tools.

Where patient information may move

System	What it may hold	Review question
Online booking widget	Name, contact details, appointment reason, symptoms	Who processes this? Where is it stored — Australia or overseas?
Website contact form	Name, contact, health details ("I have swelling...")	Does the privacy notice cover health information? Where does form data route?
Email inbox	Referrals, X-rays, patient questions, treatment plans	Who can access this? Are AI inbox tools in use? Where is email processed?
Shared drive	Treatment plans, photos, templates, patient letters	Who has access? Is it cloud-synced? Where is data stored?

System	What it may hold	Review question
Call recording or missed-call AI	Patient name, symptoms, urgency details	Where is audio stored — Australia or overseas — and who can access it?
Marketing platform	Patient lists, email records, review responses	Was patient data approved for this purpose? Where is it processed?
AI scribe	Audio, transcript, clinical notes before PMS write-back	Where does audio and transcript go before it reaches the PMS? Is processing overseas?
Chat widget	After-hours health enquiries, symptoms	Third-party storage, escalation and retention rules? Where is this hosted?
Analytics or ad pixels	Health-page visits, form fields, session behaviour	Are tracking tools loading on health-related pages? Where does data go?
Cloud backup	All of the above if uncontrolled	What is backed up? Where? Who has access? Is storage overseas?
Overseas processing	Any patient information handled by a system with servers, AI subprocessors, support staff or backups outside Australia	Where is this system processed or stored? If overseas, APP 8 considerations apply — see section below.

A day in the practice: invisible privacy edges

Time	What happens	The privacy edge
7:45am	Reception opens Gmail and sees a patient email with an X-ray attached	Email is now a shadow patient-record system.
8:30am	A new patient fills in the website contact form: "I have swelling near my wisdom tooth"	The contact form is collecting health information, even if the practice treats it as a generic enquiry form.
9:15am	Reception opens the online booking dashboard	Booking reason, symptoms, appointment type and contact details may be health information.
10:00am	Dentist uses an AI scribe during consultation	Where does audio and the generated note go before it reaches the PMS?
11:00am	Staff upload patient photos for a treatment plan presentation	Shared drives and design tools may become health-information stores.
3:00pm	Staff paste a patient message or enquiry into a public AI tool	Patient details may be processed outside Australia.

Time	What happens	The privacy edge
4:00pm	Reception uses call transcription or missed-call AI	Call audio can contain names, symptoms and treatment history.
8:30pm	A patient uses an after-hours chatbot	Urgent health details may be collected through a third-party widget with unclear storage.

APP 8 and overseas processing: what to look for

Many common dental tools — booking widgets, chat platforms, call-transcription services, AI scribes, email systems, cloud drives and analytics tools — are provided by vendors whose servers, AI subprocessors, support infrastructure or backups may be located outside Australia.

Under APP 8 of the Privacy Act, when an APP entity discloses personal information to an overseas recipient, it must take reasonable steps before that disclosure to ensure the overseas recipient does not breach the Australian Privacy Principles. The entity may also remain accountable for what the overseas recipient does with the information.

This is a review trigger, not a compliance determination. Whether a given data flow amounts to a "disclosure" under APP 8 depends on factors including the nature of the flow, contractual controls, effective access and consent — a nuanced question best resolved with qualified legal or privacy advice. The purpose of this guide is to surface possible APP 8 exposure, not to declare a breach.

For each tool the practice uses, ask:

1. **Where is this system hosted, processed or stored?** Check the vendor's privacy policy and data processing terms.
2. **Do any overseas servers, AI subprocessors, support staff or backups receive or access patient information?** Even a tool marketed as "secure" may have overseas components.
3. **What contracts or data-processing agreements govern the overseas component?** APP 8 and APP 11 require more than vendor assurances.
4. **What were patients told?** If the practice's privacy notice does not mention overseas processing, that is a separate review consideration.

The formula for possible APP 8 exposure: overseas processing + patient information + no clear disclosure, contract, effective control or consent = **cross-border review trigger** requiring qualified review before proceeding.

Offshore storage or processing is not automatically a breach. But patient information that reaches overseas recipients without a clear basis reviewed against the APPs is a possible APP 8 exposure that should be assessed — not assumed away.

Purpose-fit: collected for one purpose, used for another (APP 6)

The quietest privacy edge isn't a system — it's a *purpose*. Patient information collected for clinical care doesn't automatically become available for marketing, "win-back" campaigns, training an AI tool, or a spreadsheet someone wants to analyse. Under the Australian Privacy Principles, using health information for a **secondary purpose** generally needs consent or a closely related, reasonably expected use — and health information is held to the stricter "directly related" standard.

A 30-second purpose-fit check before reusing patient data anywhere new:

1. **What was this information collected FOR?** (clinical care, billing, bookings)
2. **Is the new use the same purpose — or something else?** Recall reminders sit close to care; marketing campaigns, lookalike audiences and AI experiments do not.
3. **Where is it going?** The same question gets sharper when the destination is a public AI tool, a marketing platform, or any system outside the practice's control — that combination (sensitive data + new purpose + external destination) is the strongest review trigger of all.

If the new use fails any of the three, stop and check before proceeding — consent, your privacy notice wording, or qualified advice. A classic example: a bad Google review arrives, and someone looks the reviewer up in the PMS to "check their history" before replying. That's clinical-care data used for reputation management — a purpose it was never collected for.

As everywhere in this guide: these are review questions and triggers, not compliance determinations.

Six edge questions for practice owners

Before switching on any AI tool, ask:

1. **What patient data does this tool read, process or store?**
2. **Where does that data go, including overseas processing?**
3. **Who can access it inside the vendor's systems?**
4. **Can the practice delete it if needed?**
5. **Is the practice's privacy notice current for this use?**
6. **Were patients told this is how their information may be used?**

These are review questions, not compliance determinations. When unsure, treat the workflow as high-review and get advice before proceeding.

Red flags

High-review signals that warrant closer look:

- AI tool that connects to email, PMS, bookings, Xero or multiple systems at once
- Booking or contact form that routes health details to a marketing platform
- Cloud backup that syncs everything including the PMS folder or email

- Public AI used for patient-facing documents, notes or communications
- Marketing agency with access to patient lists or contact records
- AI scribe with unclear audio storage, retention and deletion rules
- Analytics or ad scripts loading on pages where patients enter health information
- Booking widget, chat tool, call-transcription service or AI feature with overseas hosting, AI subprocessors or support staff — possible APP 8 cross-border review trigger
- Privacy notice or vendor terms that make no mention of overseas processing or cross-border disclosure

Safer approach

A high-review workflow is not the same as a prohibited one. Use this framing:

- **"This workflow should be reviewed before patient data is entered."** (not "it is illegal")
- **"The vendor offers the feature, but the practice remains responsible for how patient information is handled."** (not "the vendor made you breach")
- **"Any scanner or audit tool used should access only public pages and visible signals, not patient records."** (confirm scope with any scanner vendor before use)

When a workflow is high-review, document the review, get vendor confirmation in writing, and check whether the practice privacy notice covers the use.

This guide is educational practice workflow material only. It does not constitute legal or compliance advice. When uncertain about a specific tool or workflow, seek qualified legal or privacy guidance.

Disclaimer: Educational guidance only, not legal advice. This guide is intended for practice workflow education. Do not enter patient-identifiable information into public AI tools.

Author: Scott Farrell, LeverageAI — scott@leverageai.com.au · <https://dental.leverageai.com.au>