Treatment Plans: Stop The Spread

A staff-facing guide for controlling patient-identifiable treatment plans.

Treatment Plans: Stop The Spread

A treatment plan is patient health information, not just a quote.

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.

Why this matters

A treatment plan can contain:

- Patient name and contact details
- Tooth numbers and symptoms
- Clinical context and diagnosis notes
- Proposed procedures
- X-rays or photos
- Costs and payment options
- Risks and alternatives
- Dentist recommendation
- Consent language

That makes it a patient-identifiable clinical and financial document — not ordinary sales copy.

The core risk: once it leaves the system, it's no longer protected

Your dental or practice-management system (PMS) was built to protect patient information. It enforces who can see what, records every access, applies retention rules, and limits how data moves. Those protections exist for a reason.

The moment a treatment plan is taken out of that system — copied into an email, pasted into ChatGPT, saved to the desktop as a PDF, opened in Word or Canva, synced to a personal cloud drive, or forwarded to a marketing tool — **none of that protection travels with it.** The file is now outside the boundary that was designed to keep it safe.

This is the core risk. Not the spread itself, not the overseas server, not the breach finding — those are all downstream consequences of the data leaving the protected system in the first place. The spread path in the next section shows exactly how it unfolds once extraction happens. The overseas-processing and APP 8 consideration later in this guide arises because external tools often sit on infrastructure the practice has no visibility over — and that is only possible if patient information has already left the system.

The principle in plain terms:

> *"You have a dental system for a reason — don't hijack information out of it. Keep patient information inside the protected system; the moment a workflow needs to take it out is the moment to stop and check."*

Once it's out, it doesn't sit still — it multiplies

Extraction is not the end of the story. It is the start of a cycle. A treatment plan that leaves the system becomes a second copy with no controls on it — and that loose copy tends to breed more copies:

- **It gets re-worked, then fed back to AI.** The plan is pulled out, opened in Word to "make it warmer" or "more persuasive", then pasted into an AI tool to polish it — and the result is pasted back in again. Each round trip is another copy and another disclosure.
- **An AI quietly reads the whole folder.** An "AI assistant" or desktop tool that "reviews your Documents folder" or summarises your files will read every extracted plan sitting in Downloads or on the Desktop — including ones you forgot were there.
- **A backup sweeps it up.** That loose PDF on the desktop or in a personal cloud drive gets caught in an automatic backup — copied again, kept for years, and often stored overseas.

So one extraction becomes many copies, in many places you no longer control, persisting long after the original task is done. That is the engine behind every downstream risk in this guide. It is also why keeping the information inside the protected system matters: that is the one place where there is a single copy, with controls, that the practice can actually account for.

How treatment plans spread

Treatment plans often leave the PMS because staff need to make the plan look nicer, rewrite wording, add payment options, email the patient, or follow up acceptance. Each step can create another copy.

Common spread path:

```
PMS / clinical notes
        ↓
Treatment plan generated
        ↓
```

```
Exported to Word or PDF
        ↓
Saved to Desktop or Downloads
        ↓
Edited and reworded
        ↓
Copied into public AI for friendlier wording
        ↓
Attached to email
        ↓
Synced to OneDrive / iCloud / Google Drive
        ↓
Forwarded to patient / lab / finance provider
        ↓
Old versions remain everywhere
```

The red / amber / green rule

Status	Workflow
Green	Generic treatment explanation, no patient data, approved template. *(Stays inside the protected system — no extraction.)*
Amber	Patient-specific plan inside approved PMS or controlled vault.
Red	Patient-identifiable plan in public AI, old Word doc, Desktop, Downloads, personal cloud, personal email or marketing tools. *(Has left the protected system — extraction has already occurred.)*

Do not

- Save plans to Desktop or Downloads
- Use patient names in filenames
- Paste patient plans into ChatGPT or public AI
- Email old versions around
- Store plans in personal cloud drives
- Send plans to marketing tools
- Reuse real plans for staff training without de-identifying and getting approval
- Keep duplicate copies forever

Do

- Use approved templates

- Store plans in the approved location
- Send approved versions only
- Remove old versions
- Ask before using AI
- Keep patient-specific details inside approved systems
- Get dentist approval before sending

File naming rules

Avoid patient names in filenames:

```
[Patient name] implant plan final.docx   ← avoid
[Patient name] crown quote v2.pdf        ← avoid
```

Use a reference number instead:

```
TP-2026-000142.pdf
Plan-InternalID-000142.pdf
```

AI wording rule

Do not ask public AI:

```
Rewrite this patient treatment plan for [patient name]...
```

Do ask approved AI or generic public AI:

```
Write generic patient education wording about what a crown is.
Do not include patient-specific details, guarantees, testimonials
or risk-free or pain-free claims.
```

Overseas-processing and APP 8 consideration

If an AI tool drafting, summarising or rewording a treatment plan processes data on overseas servers — including many widely-used public AI services — that may constitute a disclosure to an overseas recipient under the Privacy Act (Cth). APP 8 requires an APP entity to take reasonable steps before disclosing personal information to an overseas recipient, and may hold the practice accountable for what that overseas recipient does with the information (s 16C). This is a consideration to assess with qualified legal or privacy advice, not a definitive conclusion. It applies whenever the plan contains patient-identifiable information — name, health details, costs or clinical context — and the AI tool's processing location is unclear or offshore.

The same consideration may apply to:

- cloud storage services (OneDrive, iCloud, Google Drive) if patient-identifiable plans sync to overseas-processed storage

- email providers that process attachments on overseas infrastructure
- finance or third-party providers who receive plans and use offshore systems

Sending generic wording requests with **no patient-identifiable information** to public AI does not raise the same concern.

Treatment coordinator checklist

Before sending a plan:

- Plan is in the approved location
- Correct patient, correct version
- Dentist has approved
- No old template leftovers
- No patient data entered into public AI
- No patient name in an uncontrolled filename
- No duplicate local copies left behind
- Sent by approved method
- Follow-up task created
- If any AI tool was used to draft or reword the plan, confirm whether it processes data overseas (if overseas and the plan contained patient-identifiable information, flag for manager review — this may require an APP 8 assessment)

Manager checklist

Review monthly:

- Are treatment plans stored outside the PMS or approved vault?
- Are staff using Word templates?
- Are files saved to Desktop or Downloads?
- Are plans emailed as attachments?
- Are loose old copies (not the PMS record) cleaned up?
- Are plans synced to personal cloud drives?
- Are staff using public AI for wording?
- Are plans sent to finance or third parties?
- Is there an audit trail?
- Do any AI tools, cloud storage services or third-party recipients used in the treatment-plan workflow process patient data overseas? If so, has an APP 8 assessment been done or referred to qualified legal or privacy advice?

Safer workflow

A seven-step model for safer treatment plan handling:

1. Create the plan inside the PMS or approved vault.
2. Use approved templates and wording blocks.
3. Do not save patient-identifiable plans to Desktop or Downloads.
4. Do not paste patient plans into public AI. If an AI tool is used for any part of drafting or summarising, confirm whether it processes data overseas — if it does and the plan contains patient-identifiable information, an APP 8 assessment may be required before use.
5. Send secure links where possible, not attachments. Consider whether the recipient's systems (finance providers, third-party labs) process received data overseas, as this may also require an APP 8 review.
6. Keep one approved version with an audit trail.
7. Destroy the loose duplicates — never the record. Delete the copies that escaped the system (email attachments, Word drafts, desktop PDFs, personal-drive syncs). Do **not** delete the authoritative clinical record: dental records must be kept for a legally required minimum period (longer again for a minor). The aim is one controlled copy in the PMS, kept for the required period — not fewer records.

> **Destroy duplicates, keep the record of truth.** "Get rid of old copies" means the *proliferated duplicates* a treatment plan spawns — not the patient's clinical record. Deleting the authoritative record to "tidy up" creates its own problem, because dental records carry a mandatory minimum retention period. Keep one controlled copy in the PMS for the required period; destroy the loose copies that escaped it. Confirm the exact retention periods against current NSW and Commonwealth requirements.

This guide is educational practice workflow material only. It is not legal advice. Identifying a risky workflow indicates possible exposure, not a declared breach. Seek qualified legal or privacy advice for your specific circumstances.