Browser Extensions Are Reading Your Patient Data

When a staff member opens your PMS in a browser, every extension they've installed can potentially read what's on the screen — patient data, to a tool you never vetted.

Browser Extensions Are Reading Your Patient Data

> Many browser extensions ask to "read and change all data on all websites". When the PMS is one of those websites, the extension can read patient information — and you never decided to share it.

This is general educational material for dental practice owners and staff, not legal advice.

> **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

If your practice opens its PMS, booking system or email in a web browser (Chrome, Edge, Safari), then **every extension installed in that browser is a piece of software with potential access to what's on the screen.**

Many popular extensions request the permission "**read and change all data on all websites you visit**". With that permission, the extension can read the page content of your PMS — patient names, notes, treatment details — and send it back to the extension's own servers, often **overseas**. This is the extraction problem again, except no one chose to extract anything; an installed tool does it silently.

The everyday culprits

These are the kinds of extensions staff install without thinking:

- **AI writing assistants and grammar tools** (e.g. Grammarly-style tools) — they read text fields to "improve" them.
- **AI chat / "summarise this page" assistants** — they read the whole page.
- **Screenshot and screen-recording extensions.**
- **Transcription and meeting tools.**

- **PDF, coupon, shopping and "free" utility extensions** — often the riskiest, with broad permissions and unclear owners.

The danger is not that the staff member is careless — it is that a tool installed for a personal reason quietly gets access to patient data the moment the PMS is open.

How to check what's installed

1. Open the browser's **Extensions / Add-ons** page on each practice machine.
2. For each extension, look at its **permissions** — flag anything that can "read and change all data on all websites".
3. Ask: do we know **who makes this**, and do we need it on a machine that opens the PMS?
4. **Remove** anything not needed. Be especially wary of extensions that read or rewrite text, capture the screen, or have vague ownership.

Managed vs personal browsers

- A **practice-managed browser** can restrict which extensions are allowed (an allowlist) so staff cannot install risky ones on PMS machines.
- A **personal / unmanaged browser** lets anyone install anything — which is why the PMS should not be opened in a browser full of personal extensions.

What good looks like

- **An approved-extensions allowlist** on machines that open the PMS; remove broad "read all data" extensions.
- **A clear rule** that staff do not install browser extensions on practice machines without approval.
- **Consider a separate browser or profile** used only for the PMS, with no extensions.
- Treat an extension that sends data overseas as an **APP 8 / HPP** review item, and the access itself as an **APP 11** security question.

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