Where Your Patient Files Go When You Press Save

A patient file saved to the desktop doesn't just sit there — it syncs to a cloud backup, often overseas. The backup is the quiet end of the extraction cycle.

Where Your Patient Files Go When You Press Save

> A patient file on the desktop doesn't sit still. It gets backed up to the cloud — often overseas — copied and kept for years, whether you meant it to or not.

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

In the foundational guide we describe how extracted patient data multiplies once it leaves the system. **The backup is the quiet end of that cycle.**

A staff member exports a report, saves an X-ray, or drops a treatment-plan PDF onto the Desktop or into Downloads "just for a minute". On a modern computer or phone, that folder is often **automatically synced to a cloud backup** — iCloud, OneDrive, Google Drive, Dropbox, or the device's built-in backup. No one chose to send patient files to the cloud; it happened by default.

What gets backed up without anyone noticing

- PMS exports and reports saved locally
- X-ray and clinical images opened or downloaded from the PMS
- Treatment-plan PDFs and quotes
- Screenshots of patient records
- Email attachments opened and saved to a synced folder

Why a backup is different — and harder to undo

A backup is not just one more copy. It is a copy that:

- **Sits outside the system**, without the PMS's access controls or audit trail.
- **Is often stored overseas.** Many consumer cloud backups process or store data outside Australia — which can raise **APP 8** cross-border-disclosure considerations (and the equivalent NSW HPP).
- **Persists.** Backups keep versions for a long time, so a file you "deleted" may still exist in the backup.
- **May be tied to a personal account.** If a work folder syncs to a staff member's personal iCloud or Google account, patient data is now in an account the practice does not control — a security concern under **APP 11**.

Keep the record, not the sprawl

This is **not** about deleting records. The authoritative clinical record must be kept inside the system for its mandatory retention period. The problem is the opposite: **loose duplicates sprawling into personal and overseas backups** you didn't choose and can't see. Keep one controlled copy in the system; stop the uncontrolled copies escaping into backups.

Backup exposure check

Walk through these for each practice device:

1. Is automatic device or folder backup turned on? Where does it sync to?
2. Is that backup stored in Australia, or overseas?
3. Are any **personal** cloud accounts (iCloud, Google, Dropbox) syncing folders that contain work files?
4. Do staff save PMS exports, images or PDFs into a synced folder (Desktop, Documents, Downloads)?
5. Who can access the backup, and could the practice delete a file from it if needed?

If any answer is unclear, that is a review item before more patient files accumulate there.

What good looks like

- **Keep patient files in the system.** Don't save them to the Desktop, Downloads or a synced personal folder "temporarily".
- **Use a practice-controlled backup** with a known location and known access — not whatever a staff member's personal device happens to sync to.
- **Separate work from personal cloud accounts** on practice machines.
- **Know where your backups live.** If a vendor or device backs up overseas, treat that as an APP 8 / HPP review item.

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.

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.