



Ten IT checks for a private dental practice

A short, plain English list. Nothing here needs a technical background.

Most of this can be checked in an afternoon, and several items cost nothing to fix beyond the time to do them properly.

1. Has anyone actually restored from your backup?

Not whether a backup exists, whether it restores. A backup nobody has tested is an assumption, not a safety net.

How to check: ask whoever set it up to restore one file, in front of you, today. If they cannot, or it takes days, you have found your first problem.

2. Do you know where patient records physically live?

Cloud practice management systems hold the notes, but scans, referral letters, consent forms and correspondence often sit on individual computers or in email.

How to check: ask reception where they saved the last referral letter they sent. The answer is rarely the system you paid for.

3. Is every computer encrypted?

If an encrypted laptop is stolen, it is an inconvenience. If an unencrypted one is stolen, it is a reportable data breach.

How to check: on Windows, search for BitLocker and see whether it says On. On a Mac, look for FileVault in Settings. Both are built in and free.

4. What happens to accounts when staff leave?

Dental practices have associates, hygienists, nurses and locums coming and going. Old accounts tend to linger for years.

How to check: list everyone who has left in the last twelve months, then check whether their logins still work. It is usually an uncomfortable exercise.

5. Is two factor authentication switched on?

The single cheapest thing you can do. It stops the most common way small organisations lose control of their data, which is somebody guessing or stealing a password.

How to check: log in to your practice email from a device you have never used. If it lets you straight in with just a password, two factor is off.

6. Are you using a personal email account for practice business?

Gmail, Hotmail and similar cannot be handed over when someone leaves, cannot be properly backed up, and sit outside the practice's control.

How to check: look at the address on your website and appointment reminders. If it does not end in your own domain, this applies to you.

7. Who has access to the practice management system, and at what level?

Most practices give everybody full access because it is easier. That means a temp nurse can see, edit or delete anything.

How to check: open the user list in your system and look at the permissions column. Anyone who does not need full access should not have it.

8. Can your practice work if the internet goes down?

Cloud systems are excellent until the line drops. If your diary, notes and payment terminal all depend on one connection, that connection is your single point of failure.

How to check: ask what the plan is. If the answer is that everyone goes home, that is worth knowing before it happens.

9. Do you have a written record of what data you hold?

The ICO expects you to know what personal data you hold, why, where it is, and how long you keep it. This is not a technical document, it is a page of plain writing.

How to check: ask whether it exists. If nobody can produce it in five minutes, it does not.

10. Who do you actually ring when something breaks?

Not who you think you ring. Who answers, how fast, and what it costs.

How to check: ring them now, on a normal Tuesday, and see how long it takes to reach a human.

If several of these made you uncomfortable, that is normal, and it is not a reflection on how well you run the practice. IT is the one part of a healthcare business that nobody trained you for. I am happy to walk through any of it with you, free and with no obligation.



Tareq Aloush, Norven IT
Managed IT support for private healthcare
norvenit.co.uk