

Ten IT checks for a community pharmacy

Including the technical sections of DSPT that most teams find hardest

Written for independent pharmacies without an IT department. Community pharmacy carries NHS level data responsibilities with none of the NHS IT support behind it.

1 What happens when the PMR goes down?

Everything else can wait. That cannot. When your patient medication record system stops, dispensing stops.

How to check: who do you ring, how fast do they answer, and has anyone ever timed it? Most pharmacies discover the answer during the incident rather than before it.

2 Has anyone restored from your backup?

Not whether a backup exists, whether it restores. This is also a direct DSPT question and the one most often answered on trust rather than evidence.

How to check: ask for one file to be restored in front of you today.

3 Smartcards and who has what access

Smartcards are personal, not shared, and access should match the role. In practice cards get left in readers, and locums use whatever is nearest.

How to check: walk the counter at close of business and see how many cards are still in readers. It is a five second audit and it tells you a lot.

4 What happens to access when staff leave?

Pharmacy has high turnover, particularly with locums and part time staff. Old accounts and unreturned smartcards accumulate quietly.

How to check: list everyone who has left in the last twelve months and check whether their access has actually been removed.

5 Are your computers encrypted?

If an encrypted machine is lost or stolen it is an inconvenience. If an unencrypted one is, it is a reportable data breach involving medication records.

How to check: on Windows search for BitLocker and see whether it says On. It needs Windows Pro rather than Home, which is worth confirming.

6 Two factor authentication on email and cloud systems

Free, ten minutes per person, and it prevents the most common cause of data loss in small organisations.

How to check: log in to your pharmacy email from an unfamiliar device. If a password alone gets you in, it is off.

7 What leaves the building on delivery rounds?

Names, addresses and medication details go out every day, on paper or on a driver's phone. This is the single most likely place for a data incident in a delivery pharmacy.

How to check: look at what your driver is carrying right now. Is the phone locked, is the list secure, and what happens if either goes missing?

8 Are you using a personal email account for pharmacy business?

A Gmail or similar cannot be handed over, cannot be backed up properly, and is not appropriate for anything patient related. NHS mail exists for a reason.

How to check: look at the address on your website and your paperwork.

9 Can you evidence your DSPT answers rather than just assert them?

The clinical and procedural sections are usually straightforward. The technical sections, backups, access control, device security and leaver processes, are where most pharmacies guess.

How to check: pick one technical question from your last submission and try to produce the evidence behind it.

10 Do you have a written record of what data you hold?

What personal data, why, where it lives, and how long you keep it. A page of plain writing, and the thing an inspector or the ICO will ask for first.

How to check: does it exist and can somebody find it in five minutes?

If several of these made you uncomfortable, that is normal. Community pharmacy carries NHS level data responsibilities with none of the NHS IT support, and nobody trained you for the technical side of it. 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