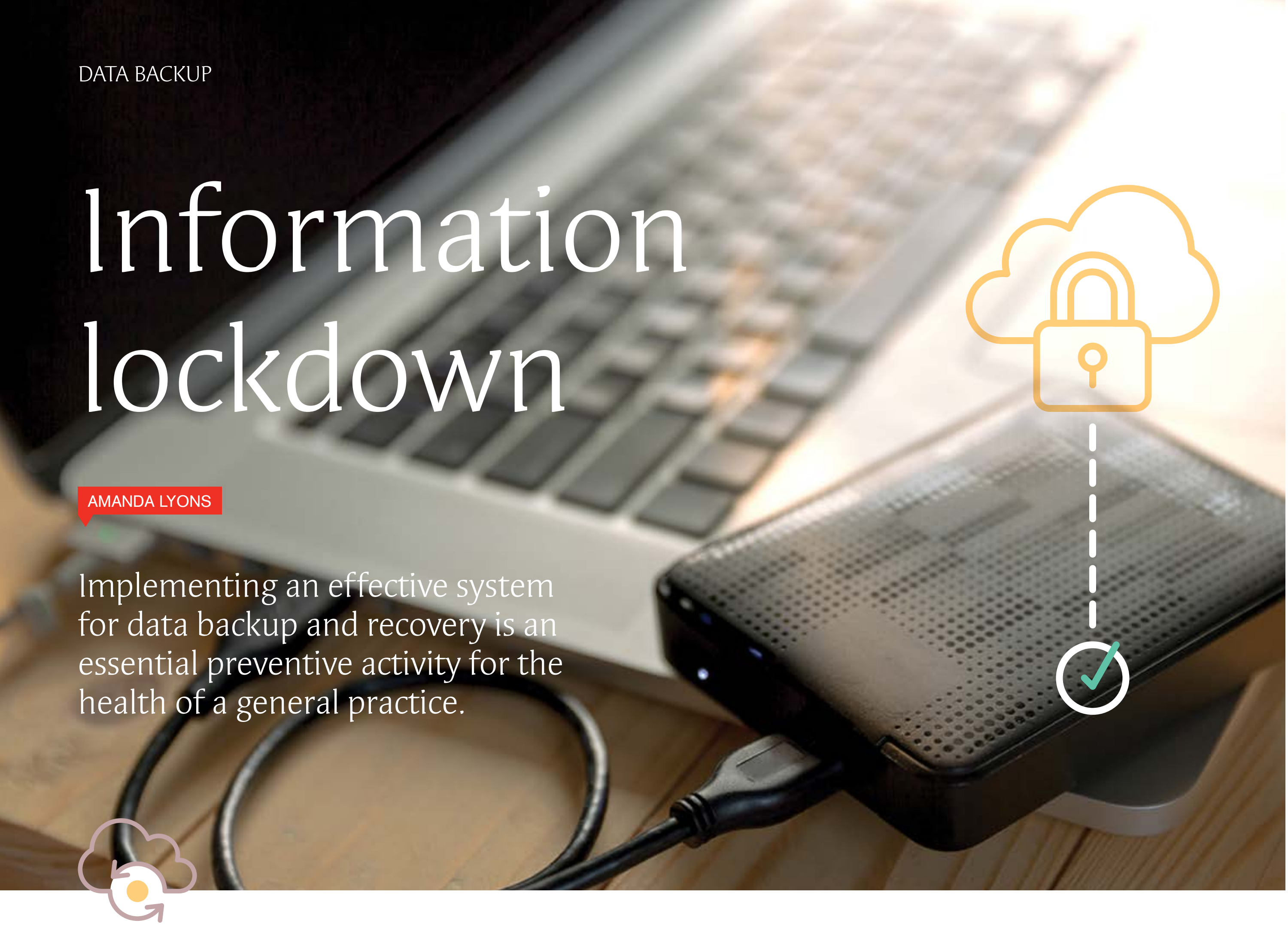
Information lockdown

AMANDA LYONS

Implementing an effective system for data backup and recovery is an essential preventive activity for the health of a general practice.



It is no exaggeration to say that data is the lifeblood of the modern general practice.

'If there's any interruption to the medical record, it can be financially, medically, professionally and personally devastating,' Assoc Prof Chris Hogan, GP and Associate Professor of General Practice at the University of Melbourne, told *Good Practice*.

The importance of data itself is not new; patient information has always been vital to the running of a practice. As technology has developed, however, so have methods of data storage, creating new efficiencies and possibilities – and vulnerabilities.

Dr Chris Mitchell, GP and member of the RACGP Expert Committee – eHealth and Practice Systems (REC–eHPS) and the General Practice Data Governance Council, learnt the consequences of these vulnerabilities the hard way.

'My first experience of data loss was right in the beginning of my career,' he told *Good Practice*. '[Our practice] had a computer that wasn't connected to the internet, so I thought, "Oh well, we won't need any anti-viral protection".

'Then one of the administrative staff brought in something to look at on the computer – this was in the days of floppy discs. Everything crashed and was unrestorable. Since then, I've learnt my lesson.'

Digital benefits

The advent of digital data has brought with it clear advantages, including the fact this type of storage is more robust and less likely to be misplaced than paper records.

'Anybody who has used paper systems would know that they are not that reliable,' Dr Mitchell said. 'They get taken out on a home visit and never come back. They get misfiled and are never found.'

Paper also has obvious vulnerability to disasters such as fire or flood, with little recourse in the event it is lost.

'Paper records are not backed up. If the practice burns down, or even if one patient's paper record is misplaced, it's gone forever,' Dr Oliver Frank, GP, member of the REC–eHPS and University Senior Research Fellow at the University of Adelaide, told *Good Practice*.

But while digital data offers many advantages, it is not infallible.

'There are only two kinds of computer users: those who have lost data and those who are going to lose data,' Dr Frank said, quoting a general practice colleague.

Digital data can be threatened by the same naturally occurring scourges as its paper counterpart, but its very medium exposes it to new types of threats.

'You need to consider how you're going to manage fire and floods, but also how you're going to manage prolonged power outages,' Dr Mitchell said. 'At one point in the past, our practice lost power for three days when there was a terrible accident that took out basically all of the electricity coming into our rural town.

'We were very fortunate that we had a generator that we could pull out, but even so it's a challenge.

'We have since had to make changes to the way we operate with the generator going. For example, we can't use our laser printers because the laser drags too much power. We have got to have some inkjet printers in the practice.'

Images iStock; Oliver Frank, Chris Hogan; Chris Mitchell

There are also the modern digital problems of computer hacking and the introduction of malware, such as viruses and worms.

'Before, we had to worry about mischance and misadventure, but now we also have to worry about mischief and mayhem,' Assoc Prof Hogan said.

There can be various motivations behind attacks on software and systems. For example, practices can be faced with 'ransomware', where a computer system is essentially blocked and won't be restored until a sum of money is paid to those who implemented the software. The desirability of medical data on the internet's black market is another security issue.

'Medical data has a high level of value among hackers because it contains sufficient demographic details to enable identity fraud,' Assoc Prof Hogan said.

Protecting patient data is a fundamental issue of patient and practice safety.

'Data security is key,' Dr Mitchell said. 'It's really important that that information is maintained securely; for the reputation of your practice and for the protection of your patients' personal health information.'

Although ensuring data backup and security comes with a financial price tag, Dr Frank cautioned that not doing so carries a much more significant expense.

'To some extent, it's a question of cost versus how much data you're prepared to lose,' he said. 'The more you spend, the more likely you'll lose less data and be able to recover your data sooner and more easily. So there is a balance in that.'

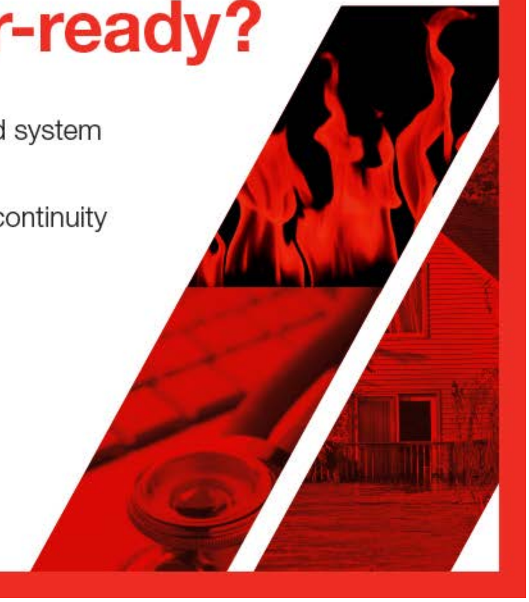
Tricks and traps

While the technology involved can be complex, the ultimate goal of data backup systems is fairly straightforward.

'The aim is to have all the information available at any time you might need it, and to be able to restore it quickly and efficiently,' Dr Frank said.

There is a range of methods and systems available and a practice needs to decide what is best for its needs (refer to breakout on page 20 for more information). According to Assoc Prof Hogan, however, there is one consideration that should be common to all practices: the need for offsite storage in order to be prepared for several disaster-type scenarios. >>

From top: Assoc Prof Chris Hogan, Dr Oliver Frank and Dr Chris Mitchell all believe high-quality data backup systems in general practice are worth the financial investment.



>> 'First of all, [be prepared for] the destruction of your general system. For example, your office burning down,' he said. 'The next thing is when there has been an incident whereby the whole building is inaccessible, usually due to extensive flooding.'

There are many types of backup, including local, in which practices back up data to a physical storage device onsite or at a nearby location. There are also options in which data is stored offsite, either physically or online. Finally, there is the option of storing data in the 'cloud'.[1]

Each of these options contains its own benefits and drawbacks: physical onsite storage remains vulnerable to theft and natural disaster, online storage is dependent on internet access,[1] and use of third-party storage companies can expose practices to external risk.

'It's tempting to think that one could outsource all of this and let someone else manage the data,' Dr Frank said. 'But then you're very dependent on the organisation maintaining it. Even if they are doing the right thing but then go out of business, there's potentially a problem.

'And, of course, there are questions about the data being hosted in Australia, and even about your connection to where your backup is working.

'There's quite a few steps along the way.'

Once the practice backup system has been selected and implemented, it is important to ensure it is operating as it should.

'The area where I see practices getting into strife is thinking that they've got an automated backup process when they don't,' Dr Mitchell said. 'They've set up, or their IT [information technology] manager has set up, a process of automated backups that has fallen over for whatever reason, and nobody knows that it's fallen over.

'The other problem I often see is backups occurring, but the data is not readable. The key is to ensure that backups are occurring every day, at least, and that they are checked and you can restore from them.'

There are also more technological concerns to consider, such as compatibility between systems.

'When your system goes down, how do you collect the information?' Assoc Prof Hogan said. 'It needs to have a computer that's compatible with the data-retrieval system. The technology you use has to be robust and able to do the job that you are asking it to do. For instance, USB sticks are useful for intermittent backup, but not for doing it regularly.

'The other thing is that once you've got your backup system, the computer you are using must be able to read and cope with the backup and not corrupt the data.

'And when you are using the system away from the practice, you need to make sure that the information you collect can be integrated back into your main system.

'We have had issues after a bushfire where people collect all of the data and then realise they have to manually re-enter it because they've used a manual system.'

System education

It is not just data backup technology that requires attention, but also the people who are using it.

'Even with the best IT system in the world, people have to be aware of the risks,' Dr Mitchell said. 'So it's not just about investment in infrastructure, but also about investment in training.'

Effective training is vital to ensure that practice staff members understand the correct procedures to safeguard the security of their IT system.

'A chain is only as strong as its weakest link, and the person who has the passwords on sticky notes on their computer isn't what you would call the strongest link,' Assoc Prof Hogan said.

In addition to day-to-day use, it is also important to have dedicated staff members who have detailed background knowledge of the practice system.

'You've got to have at least one person, ideally two people, who understand the backup process and who are involved with checking it over,' Dr Mitchell said. 'Because it isn't just IT systems that fall over, [human] systems fall over as well, and it's pretty awkward if the only person who knows how that system works leaves the practice for sickness or any other reason.

'So you've really got to have some allowance for redundancy in terms of your staff knowledge of the system.'

RACGP resource

The RACGP released its *Guide to information backup in general practice* in 2016. The document is designed to assist general practices in selecting and implementing secure and reliable information backup and data recovery processes.

The guide provides details of backup procedures, case studies and checklists, and should be used in conjunction with advice from an IT professional.

Visit www.racgp.org.au/your-practice/ehealth/protecting-information/guide-to-information-backup-in-general-practice to access *Guide to information backup in general practice*.

Given the technical knowledge needed to understand and run these systems is so specialised, it is also important for GPs seek professional assistance and advice.

'GPs are not computer technicians,' Dr Frank said. 'Some of us have a bit of an interest in these things, but even then it's probably dangerous to think we can actually manage it ourselves. It's too technical.'

Assoc Prof Hogan emphasised that it is important to expect the unexpected when it comes to system failure.

'We always used to say that we believe in Mrs Murphy's law: that Mr Murphy was an optimist, because even things that couldn't go wrong, would go wrong,' he said.

With this principle in mind, Dr Mitchell recommends ensuring a practice has a comprehensive system manual on the premises.

'Unfortunately, disaster won't always strike when your most senior practice manager is available, or when the person with the IT responsibilities is there,' he said. 'So you need to make sure that your training and manuals are sufficient for people to understand what they need to do.

'That first step might be calling in your practice manager. But often there are steps that can be taken and [in our practice] we've tried to outline those in the manual to show exactly what to do.'

References

1. The Royal Australian College of General Practitioners. Guide to information backup in general practice. East Melbourne, Vic: RACGP, 2016.