RACGP

Royal Australian College *of* General Practitioners

Guide to information backup in general practice

racgp.org.au

Healthy Profession.
Healthy Australia.

Guide to information backup in general practice

Disclaimer

Recommended citation

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

The Royal Australian College of General Practitioners
100 Wellington Parade
East Melbourne, Vic 3002 Australia
Tel 03 8699 0414
Fax 03 8699 0400
www.racgp.org.au

ISBN: 978-0-86906-459-7 (web)

Published September 2016

We recognise the traditional custodians of the land and sea on which we work and live.

Contents

About this guide

This guide does not provide specific advice regarding general practice information technology (IT) requirements, as this is unique to each individual general practice. It is recommended that you consult an IT professional when implementing new technologies into your practice.

About backup

Backup is the process of copying files or databases so they are preserved in the event of equipment failure or other catastrophes. It is an essential activity for general practice to have backup procedures in place.

It is recommended to keep separate copies of your business-critical data in multiple places in case data loss occurs. This data needs to be kept safe, offsite and, if possible, encrypted. The more secure copies of data you have, the safer it will be.

Backup in general practice

Backing up business-critical information is a requirement in order for a general practice to achieve accreditation (refer to the RACGP's *Standards for general practices* [4th edition], Criterion 4.2.2 Information security). It is recommended that practices have a reliable information backup system to support timely access to business and clinical information.

In order to meet accreditation and for purposes of business continuity, ensure your practice backup process:

- is checked at regular intervals (ie daily), including the ability to recover the data
- is consistent with the business-continuity plan your practice has developed, tested and documented
- details how and in which offsite locations information is stored.

Essential backup checklist

This checklist is taken from the RACGP's *Computer and information security standards* (2nd edition). It details the recommended procedures to help achieve the minimum level of secure and reliable backup in your practice:

- ☐ Complete written backup policy in place that is periodically reviewed
- ☐ Backup policy is communicated in written format, training is provided on the process and all practice team members have access to the policy
- ☐ Daily automatic initiation of full backup of all data and programs
- ☐ Backup is encrypted with password
- ☐ Backup is periodically checked for reliability and the outcome tracked
- ☐ Backup is tested daily and regularly manually restored by, or under the guidance of, an IT professional
- ☐ Backup media comprises of a combination of removable hard disk, networked storage that is not generally accessible across the network, separate network, or offsite (cloud)
- ☐ The media used for each method of backup is rotated frequently to ensure there are multiple copies of the practice data at any point in time
- ☐ Current backup is securely stored both onsite and offsite
- ☐ Backup access only for authorised practice team members
- ☐ Retain access to previous backup technology and readability of previous media tested

Cost of data loss

The loss of critical data has the potential to impose a substantial financial and operational cost to your practice when trying to restore day-to-day business operations. The amount of data lost, and the reliability and efficiency of the practice's data recovery system and processes, will determine the magnitude of the cost. A severe disruption and loss of data could cause significant downtime in daily operations, as well as loss of financial revenue. Additionally, if a business continuity plan is not in place, the cost of restoring data by outsourcing to a data loss prevention company can be expensive. Having a business continuity plan and a reliable, frequently-tested backup procedure as part of your normal practice operations is therefore crucial.

Business continuity plan

In addition to having a sound backup system in place, your practice needs a continuity plan to encompass all critical areas of your practice's operations, such as:

- enabling clinical team members to provide adequate clinical care while not having access to electronic health records
- appointment scheduling
- billing
- business financial operations (eg payroll, Medicare claims).

Once a plan has been formulated, it needs to be regularly tested in order to ensure backup protocols are working properly. Refer to RACGP's *Computer and information security Standards* (2nd edition) for a comprehensive explanation of what a business continuity and recovery plan should entail, and templates to assist your practice in developing one.

Refer to the 'Further reading' section for more information on resources that are helpful in business contingency planning.

Tip: A general practice in inner-Melbourne prints out a copy of the following day's appointments each evening. In the event of a computer failure, this allows the practice to continue running and keep appointments while the issue is being resolved.

Who will be responsible for the backup and recovery plan?

As an added precaution, it is recommended you be able to restore data to a test computer which has a separate copy of the practice software, in order to validate data against the live system.

Redundancy

This is the method of using more internal drives than necessary to duplicate and store data (ie storing the same data in more than one place). It offers immediate data protection against drive failure in real-time. The system will indicate that one of the internal drives has failed, offering you the chance to backup important data and replace the failed drive.

It is recommended that you have a primary contact for your practice's backup and recovery plan. Ensure that you have a written agreement that clearly outlines the roles and accountabilities for the primary contact. This role is a key responsibility, so you must ensure the person possesses the necessary skills and understanding of the impact a data loss or backup failure will have on the practice.

This staff member might also be responsible for performing or monitoring the actual backup and recovery of data. Alternatively, your practice may contract an IT company to control the backup and recovery process. If you choose to use an external IT company, you will also require a written agreement that outlines the organisation's roles and accountabilities.

Selecting an external IT provider to manage your backups

If you have decided to engage the services of an external IT provider, there are certain factors and questions to consider in order to help choose the right one for your practice needs:

- What is the history and background of the IT business? Does it have experience in the healthcare industry?
- What are the qualifications and expertise of the business' staff members?
- What type of hardware (if any) is supplied and what is the warranty period?
- What are the details of the service agreement? (Request a copy of the service agreement prior to finalising your decision, and ensure that you and the IT provider have agreed on the same terms of the service delivery.)
- What insurance cover does the business have?
- What risk management strategies are in place?
- Will the business be available to provide support if you run into trouble?
- Does the business provide remote monitoring and maintenance systems?
- Is there remote monitoring of backup and regular restoration from backup?
- Does the business' area of expertise cover site servers or cloud-based systems, or both?
- What is the cost of the service? Are there differing price structures depending on the level of support required (eg 24-hour monitoring to ensure there is no down time)?
- What support does the business provide when the practice is undergoing accreditation?

Refer to the checklist in the 'Contracts' chapter of the RACGP's *Guide for hardware and software requirements in general practice* for further information on reviewing contracts and service-level agreements with external IT providers.

What types of data need to be backed-up?

All information that is critical to the operation of your general practice should be backed-up. This includes:

- clinical information system data, patient healthcare information
- patient demographic and contact details, billing and financial information, appointments and practice management
- web page data.

The type of data you are backing up may determine your method and process:

- Critical data – eg your patient healthcare information and any data required to run your business. You may want to have redundant backup sets that extend for several backup periods. Critical data should be encrypted and kept secure.
- Sensitive data – eg personal health information details. It is recommended that you ensure backup data is physically secured and encrypted.

The frequency of data change can affect decisions regarding how regularly it should be backed-up. For example, data that changes daily should be backed-up daily.

Do you have the right equipment to perform backups?

You must have backup hardware and software in order to perform backups. Timely backups may require several backup devices and sets of backup media. There are several types of backup hardware:

- Local or direct-attached hardware:
  - This hardware can include portable hard drives, USB flash drives, desktop external storage devices, tape and optical media (CDs, DVD, or Blu-ray).
  - It is important to store copies offsite, and it is recommended you keep and cycle multiple removable devices (eg portable hard drives), as they can be prone to failure.
  - Using local or direct-attached hardware can be fast; however, you can only back up one computer at a time with each medium.
- Network backup using a local server:
  - Network backup means having one computer as a backup destination for all other computers and devices. The best way to do this is with a network-attached storage (NAS) server.
  - You will still need to have an offsite backup when using a local server backup. It is recommended that a second backup of the local server be taken offsite.
  - Multiple computers can be backed-up at the same time, but initial setup can be costly and complicated.
- Online backup or cloud backup using the internet:
  - An efficient form of backup, but relies heavily on a fast and secure internet connection.
  - These services are provided by external IT companies.
  - It is important to consider where the backed-up data is held. Online and cloud servers may be located outside of Australia, so seek to ensure the information is stored only in countries with privacy protections that are compatible with Australian law.

It is recommended that a combination of backup hardware be used. Your data storage strategy and the types of backup media you use will depend on the volume of data and available budget.

Keep your backup media current

Tapes and recordable DVDs/CDs were once popular backup media, but certain media becomes obsolete as technology changes. It is important that your backup media can be accessed in the future if information needs to be restored and retrieved. Keep your backup media up to date with the technology available.

Physical storage of backups

You will need to consider the physical location of your backed-up data. For general practice accreditation, it is recommended that your backups are stored offsite, as this is essential to recovering your information in the case of a natural disaster. Your offsite storage location should also include copies of the software you might need to install to re-establish and restore operational systems.

Ensure you have offsite copies of installation media for practice software, license information and operating system details. Where backups are retained using old media, the media recorders and players will also need to be retained (eg tape recorders).

Any backup storage location needs to be a secure environment. Lost or stolen data can lead to identity theft and breaches of patient privacy. Wherever the physical location, ensure it is kept secure and limit the number of staff members with access. If your main backup is to NAS, an air-conditioned room will keep it and other hardware from overheating.

It is important to be aware of the physical environment in which backup media is stored. Backup media is often storied in cupboards and safes, for example. The location should be hazard-free in order to ensure media will not be damaged.

Backup rotation

More than one backup method should be used if it is practical to do so. Backup media should be cycled, or rotated, so that there are multiple backup copies of the practice data at any point in time.

The best time to schedule backups

Scheduling backups during times of lower system use will help speed up the process. Try to schedule backups for a time during which the process is less likely to impact on day-to-day business, ie out of business hours or overnight.

Your clinical information system is likely to have an inbuilt automated backup function, and you should consult with your vendor regarding how these backups are undertaken and how they can be accessed if required.

Types of backup

Synchronisation

A process in which files in multiple locations update each other – copying changes back and forth – whether it be real-time local or offsite. There are many different file synchronisation software packages.

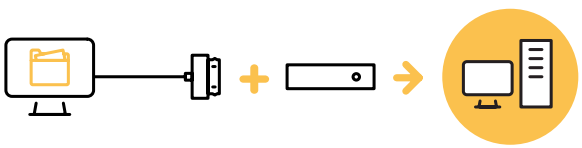
Cloud backup

Login and upload to the cloud

This process is ongoing backup to a storage medium that is always connected to the internet. The term 'cloud' refers to the backup storage facility being accessible from the internet. Cloud backup is different to online backup in that the data can be accessed securely from any other computer with an internet connection.

+	−
» Good physical protection » Easy to access » Files are automatically backed-up » Data is replicated across several storage media	» More expensive than local backups » Slow initial backups » Slow to restore » Requires fast internet connection for optimal performance

Local backup



Backup by connecting directly to a storage device

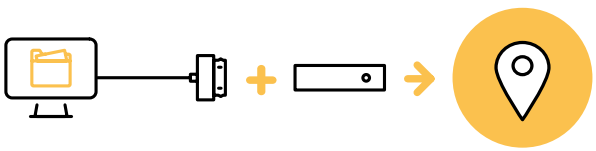
Any backup where the storage medium is kept close at hand. Typically, the storage medium is plugged directly into the computer that is being backed-up.

+	−
» Good protection from hard-drive failures, virus attacks, accidental deletes » Fast backup and restore » Low cost » Backups are easily obtained » Full internal control over the backup device (no third party involved)	» Does not offer good physical protection from theft and natural disaster » Prone to virus attack and accidental deletes

Defense in depth

A strategy whereby security controls are multi-layered throughout an IT system in order to reduce the risk of network attack.

Offsite backup



Backup by connecting to a storage device and relocate offsite

The backup storage medium is kept at a different geographic location from the source. The backup is initially completed locally on the usual storage devices. The storage medium becomes an offsite backup once it is taken to another location.

» Offers additional protection from natural disasters in comparison to local backup	» Requires more due diligence to bring the storage media to the offsite location » Increased handling increases risk of damaging the device

Online backup

Login via internet and upload directly to a storage device offsite

A storage medium that is always connected via the internet and is usually located offsite.

» Good physical protection » Data is replicated across several storage media » Frequent backups » Requires little manual interaction after setup	» More expensive than local backups » Initial backups are slow » Slow to restore

Data recovery

How quickly do you need to recover the data?

The time taken to restore data is an important factor in creating a backup plan. In the case of critical systems, for example, you might need to get back online quickly and thus might need to alter your backup plan.

Frequent testing and validation of data readability will assist with a more timely data recovery and reassure your practice that its backup and recovery system is working.

How do you know the backup has succeeded?

It is important to regularly test that your backup has worked and to test the integrity of your backup data once it has been restored. This ensures the backup has been successful and the restored data is accurate, correct, complete and preserved for future use.

Ensure that your backup software performs these tests and restores to 100% accuracy by validating the restored data against what is held in the live system.

Things to consider and discuss with your IT professional

It is essential to consult an IT professional about your specific requirements when looking at different types of backups for your practice. Potential questions:

- Who is responsible for ensuring the backup happens?
- How often should we backup our data?
- Where is the data being held offsite and is it being held securely?
- What information do we need to back up?
- Discuss the IT professional's role in your practice's business continuity plan?
- How quickly can our practice recover in the event of a disaster?
- Is our practice backing up all the data it requires?
- How do we perform routine checks to validate that our backup data is complete and correct?
- How do we regularly test the restoring of our backup data?
- What type of security is used to protect our practice backups?

Data integrity and security

Your practice must have an effective system for managing patient information, as well as ensuring the security of your patient health information, in order to meet general practice accreditation requirements and comply with the RACGP's *Standards for general practices* (4th edition) (Criterion 4.2.2 Information security). This includes ensuring practice computers:

- are only accessible, via individual password access, to people in the practice team with appropriate levels of authorisation
- feature screensavers or other automated privacy protection devices that have been enabled in order to prevent unauthorised access
- are protected by regularly-updated antivirus software
- that are connected to the internet are protected by appropriate hardware/software firewalls.

Refer to the RACGP's *Computer information and security standards* (2nd edition) for extensive information relating to computer security in general practice.

Bare-metal restore

When your backed-up data is available in a form that allows you to restore a complete computer system from 'bare metal', ie restoration of previously installed software, operating system and applications.

Case studies

Case study 1 – Optimal backup process

A group of Melbourne-based general practices have sought to achieve an optimal backup procedure across their businesses. The optimal process may seem overwhelming and excessive; however, while having had some unexpected system downtime, none of the practices have ever lost any significant data.

Each practice has taken the 'defense in depth' approach to backup. This multi-layered and extremely thorough backup process provided extra assurance that business-critical information is secure and easily recovered in the event of a disaster or system failure.

When using the 'defense in depth' approach, the mission-critical primary physical server database (clinical and financial) is initially synchronised to a secondary onsite physical server every 15 minutes, and checked daily. Additionally, the backup is synchronised over the internet to a cloud-hosted storage site overnight. This occurs automatically.

Data is backed-up daily to a NAS and a USB hard drive (which is rotated), and is then stored offsite.

All of the practices also backup their entire server system daily using third-party software in case a 'bare-metal restore' is required. Archived backups dating back at least three years are kept offsite and stored in a dedicated archive server. If a backup is not completed successfully, failure notification email messages are automatically sent to the IT team and practice manager. The entire process is documented and reviewed periodically.

These thorough backup protocols have been incorporated across the practices to help guarantee there is enough redundancy to ensure the entire database can be restored and the practices can return to normal working order in the event the system completely fails. The ultimate objective of the backup strategy is to ensure business continuity by keeping unplanned downtime to less than 15 minutes.

Case study 2 – The potential financial impact of not regularly testing your backups

A practice in New South Wales suffered a devastating failure a few years ago when a power outage occurred during the night and the uninterrupted power supply (UPS) did not correctly shut down the servers. The UPS instead ran until it was exhausted and the servers were suddenly without any power. This caused corruption in the database.

When IT support tried to restore the data from the previous night's backup, from the backup the night prior to that, and so on, it was discovered that those three most recent backups were unusable. No one in the practice was aware the backups were unusable as they had not been tested for readability.

The practice consequently lost three days' of patient and business data, which proved to be disruptive and expensive for months afterwards.

The loss of data resulted in patients arriving for previously-booked appointments that were no longer recorded in the practice systems due to the faulty backups. GPs in the practice had to rely on patients to provide information on what had occurred during visits on the days where the clinical information system data was missing. While there is no firm figure of the total cost resulting from the loss of data, for a practice with 12 full-time equivalent (FTE) GPs, the expense is likely to have run into the tens of thousands of dollars.

Case study 3 – The severe repercussions of not performing backups

A medical centre that had been operating the same clinical information system for five years, recently encountered some serious issues.

A power outage in the surrounding area left the medical centre's hardware to rely on its battery backup system to help 'softly' shut down its systems in the correct manner and sequence in order to avoid hardware

damage and data corruption. Unfortunately, in the same way data backups need to be tested for validity, the battery backup had not been tested and failed when it was needed for the first time, leaving the server unprotected when power to the suburb was cut.

The consequences of not shutting down or restarting a computer safely can be catastrophic, especially when databases are not safely stopped and the hardware was not powered down. As a result of the power outage, the medical centre discovered it had not performed any backups of patient data, or of the server itself. The failure of the server hard drives and the subsequent data corruption due to the sudden power outage left the medical centre unable to recover any electronic patient files. This loss of data was a major disruption as the medical centre had been in operation for 15 years and converted to electronic records five years earlier.

Further reading

The RACGP has a number of documents available to assist general practices with information backup:

- The Emergency Response Planning Tool (ERPT) is designed to help general practices better prepare for, respond to and recover from the impacts of emergencies and pandemics. The ERPT guides you through a series of planning templates, where critical information about your practice can be entered and saved. This information will be used to create an emergency response plan that is individually tailored to your general practice. Customised emergency response plans can be accessed on any computer or mobile device that is connected to the internet using your specific username and password. You can also print a hard copy resource for future reference, which should be stored offsite.
- *A guide for hardware and software requirements in general practice* is designed to provide general practices with assistance in choosing what type of IT requirements are needed for their specific business needs. The guide also includes a checklist on business continuity and redundancy.

RACGP

Royal Australian College *of* General Practitioners

Healthy Profession.
Healthy Australia.