Australian Government
Australian Digital Health Agency

BACKUPS

Prepare for an emergency

A guide for
healthcare providers

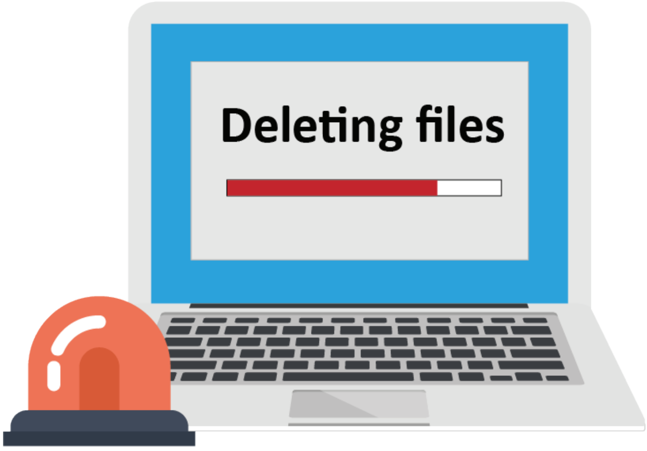
This document has been prepared for small to medium healthcare providers. It outlines some of the ways backing up your data can protect your practice. This document provides general guidance in relation to backing up data and is not intended to be comprehensive.

Do you have a recent backup of your important files?

Have you ever:

- Accidentally deleted a file?
- Lost your phone, laptop or tablet computer (or had it stolen)?
- Experienced a computer hardware failure (e.g. your hard drive died)?
- Had your computer infected by ransomware or other malicious software?

If a situation causes you to lose access to your important files, it is likely that the only way to recover is to retrieve your files from a backup.



Backup basics

A backup is a copy of your computer files which is stored separately from your computer or device. To protect your healthcare business from loss of information and damage to your reputation, you will need to:

1. Backup regularly
2. Store the backups offsite and offline
3. Ensure backup data is encrypted with a password and stored in a physically secure location
4. Test your backups to make sure they work as expected.

> *"Hardware failure, theft, or malware infection (such as the cryptolocker ransomware attack) can make recovering data that is critical to your business expensive or impossible. To avoid this, you need to back-up your data."*[1]

Protect your data and your reputation

Imagine the consequences if you lost all of the data stored on your computer! This would be disastrous for your reputation and could jeopardise the safety of your healthcare consumers.

Regularly backing up your data is like another type of insurance policy for your business. Having multiple backups, stored off-site, provides protection against a range of incidents such as theft, natural disasters, fire or a lost device.[1]

If your computer hardware, fails or you become a victim of a cyber-attack, having a recent backup of your data will help you to recover more quickly.

Getting started

There are four major steps to backing up your data:

Step 1: Identify the data to be backed up

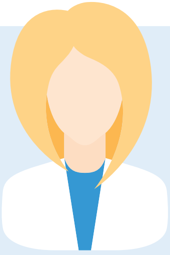
Consider all the information you access and store electronically. Identify the data that you would be most concerned about losing. Consider what the impact on your business would be if this data could not be accessed. In some circumstances, you may wish to back up everything stored on your computer, including your files, applications and operating system. This approach will take a lot longer to complete; and will result in larger backup files, which require a larger amount of storage space than a targeted backup regime. You may decide that a hybrid approach is best, backing up your most important files more frequently, and performing a full backup less often.

> *"All information that is critical to the operation of your [healthcare] practice should be backed-up."*[2]

Step 2: Determine backup frequency

The frequency of data backups will vary, depending on how often you enter new information, and the importance of the data you store. You may wish to backup frequently (e.g. hourly, or immediately as a file is saved), or you may prefer a less frequent backup timeframe, such as daily or even weekly. The key to determining the best frequency for your backups is to consider how much data you could lose and the impact of that data loss. The following scenarios may assist in determining how frequently you need to back up your data.

Scenario 1



I am a healthcare practitioner running a small private practice clinic which opens one day each week. The clinic books hourly appointments, for up to six consumers, on that day. In this situation, the amount of data that would be lost if I only backed up weekly would be data regarding six consumer appointments. I need to decide whether the risk of losing this data outweighs the effort to perform a backup more frequently.

Scenario 2

I am a healthcare practitioner running a medium-sized healthcare clinic with four other practitioners. We each see four healthcare consumers per hour for 15-minute appointments. This equates to 140 appointments per day, with five healthcare practitioners working 7 hours each (plus breaks). If I only backup data for my healthcare clinic once per week, I risk losing information for 700 appointments, over a five-day working week. In reviewing the risk in terms of clinical outcomes, reputational, financial and time costs, I am likely to conclude that a weekly backup may be insufficient, given the potential impact of the data loss. Therefore, it is likely that I will select a more frequent backup regime, perhaps daily.

Step 3: Select the backup method

There are a number of backup methods, where you either backup all data, some data or only data that has changed. An overview of the advantages and disadvantages of each method is provided below.[1]

Table 1: Comparison of backup methods

Backup Method	***Advantages***	***Disadvantages***
Full backup	✓ All of the data on your computer is backed up, including files, applications and operating system. ✓ Facilitates a complete restoration of the computer.	× A large amount of storage is required. × The backup process can take a long time (the more data you have the longer it will take).
Partial backup	✓ Enables you to select the files you want to backup. ✓ Requires less storage than a full backup. ✓ The backup process takes less time to complete than a full backup.	× Only enables you to recover the files you have chosen to backup. × Doesn't enable a full restoration of the computer.
Differential backup	✓ A full backup is undertaken before the first differential backup. ✓ Backs up any files that have changed since the previous full backup. ✓ Enables full recovery, using the full backup and one differential backup. ✓ Takes less time to complete each backup, compared with full or partial backups, but takes longer than an incremental backup.	× Recovery takes longer, as the full backup and each differential backup must be restored.
Incremental backup	✓ Similar to the differential backup – a full backup is undertaken before the first incremental backup. ✓ Backs up any files that have changed since the previous incremental backup. ✓ Enables full recovery. ✓ Takes less time to complete each backup, compare with full, partial or differential backups.	× Recovery takes longer, as the full backup and each incremental backup must be restored.

> *"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."*[2]

Step 4: Choose your backup storage option(s)

There are a number of ways to store your backups, but essentially, they fall into two main categories:[1]

1. Physical storage devices, such as external hard drives; or
2. Online backups, such as cloud-based data storage solutions.

You may decide to use either or both backup storage options. There are a number of factors to consider when selecting the most appropriate option(s) for your business.

Things to consider when implementing your backup solution

Offline backups are important to help you recover if you are affected by malware, such as ransomware. Research reveals that for the healthcare industry, ransomware accounts for 70% of incidents involving malicious code.[3] For example, in May 2017, the WannaCry ransomware attack prevented 596 General Practitioners, across Britain, from accessing their data and being able to manage appointments for healthcare consumers for over a week.[4]

If your backups are stored on a device that is always connected to your computer, the information stored on this device can also be affected by any malicious software that affects your computer. As a consequence, the backups may no longer provide a recovery option, if they have been compromised. For this reason, it is important to disconnect the storage device and store backup data offline, each time you have completed the backup process.

A comprehensive data recovery plan will take into account physical, virtual and cloud environments that are used by your practice. Ideally most or all parts of your backup process can be automated, but in some cases, you may need to conduct backups manually. If so, you will need to schedule your backup process into your organisation's diary. The goal of your backup strategy will be to ensure that at least one copy of your data will survive any incidents. A strategy that is being adopted by many businesses is based on the 3-2-1 rule:[5]

Make **three** copies of every important piece of information

Store that data in **two** different formats

Keep **one** copy offsite

Following the 3-2-1 rule can help to ensure that your data won't be lost through a single event, as you will have multiple copies of the data, stored in multiple formats and in more than one location. This approach can protect against physical disasters, such as fire, flood and theft, as well as cyber security attacks, such as ransomware.[5]

It is also important to retain copies of your backups for a reasonable period of time, as data loss can happen slowly without being noticed. This may occur due to malicious software, inadvertent deletion of files or hardware failure. Therefore, it is a good idea to keep your most recent backups, plus backups that were captured at different time periods, such as one week ago, one month ago, six months ago, for example.[1]

"68% of breaches took months or longer to discover."[6]

Planning to recover your data

Just as a fire drill helps to ensure emergency evacuation procedures are working effectively, it is important to test your backups regularly, to make sure the backup process is working as expected. This will help to ensure you are able to successfully recover from a disaster that affects your digital information. One way of testing whether your backup process is working is to open a selection of files from a backup and compare them with the original files, to ensure they are the same.[7] It is important to be aware that using a backup to recover from a disaster or cyber incident can be complicated, particularly when a complete system rebuild is required. Depending on your circumstances, restoration of your practice computers may require specialist technical support.

Case studies

The case studies below illustrate how an effective backup strategy can protect your healthcare business. It is important to note that backups are only one security measure that needs to be augmented by several layers of information security controls. In both of these case studies, the businesses implemented additional security measures to prevent other incidents.

Case Study 1: small sleep centre

In September 2017, a sleep centre was affected by a ransomware attack that potentially compromised 16,476 consumer records. The hacker demanded a ransom to unlock the files. This was not paid as the practice had an offline backup of their files and engaged IT specialists to confirm that the records were intact. During the incident, the sleep centre hired a computer forensics team to help with the investigation and make recommendations on how to better protect its systems in the future.[8]

Case Study 2: general practice

Following a power outage which resulted in corruption of data, a general practice in New South Wales experienced significant disruption and expense when their backups failed. As a result of this incident, the practice was unable to view appointments that had been booked, with patients arriving for appointments that were no longer available in the practice management software. In addition, due to the loss of clinical information, the GPs had to rely on patients to provide them with details of what had been discussed during previous consultations. This situation highlights the importance of regularly testing backups and other business continuity measures, such as the uninterruptible power supply (UPS), to ensure the processes are working as expected.[2]

Further information

The Australian Digital Health Agency offers resources to assist healthcare providers to enhance their security practices. Visit the Agency's website for additional guides and information on enhancing the security of your healthcare practice: www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre

Other organisations you could contact for more information or specific advice include:

Table 2. Australian Cyber Security Organisations

Organisation	***Role***
Australian Cyber Security Centre	The Australian Cyber Security Centre (ACSC) provides advice and assistance to help businesses, individuals and governments to protect information from cyber threats, respond to incidents and develop information security strategies including backups.
Stay Smart Online	Stay Smart Online provides simple, easy to understand advice on how to protect yourself online as well as up-to-date information on the latest online threats and how to respond. This includes information about establishing a regular backup program.
Australian Cybercrime Online Reporting Network	The Australian Cybercrime Online Reporting Network (ACORN) provides a national online system for reporting cyber incidents and obtaining advice about cyber security.

You may also like to visit the World Backup Day website, an independent initiative to help raise awareness about the importance of regular backups. The site includes free resources to assist organisations to understand the need to back up data at work and home.

References

1 Stay Smart Online, Protect Your Business: Do Things Safely - Backups for Business. Available from: https://www.staysmartonline.gov.au/protect-your-business/doing-things-safely/backups-business

2 Guide to information backup in general practice. Available from: Available from: https://www.racgp.org.au/download/Documents/e-health/Guide-to-Information-Backup-in-General-Practice.pdf

3 2018 Verizon Protected Health Information Data Breach Report. Available from: https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pdf

4 Department of Health, Investigation: WannaCry cyber attack and the National Health Service. Available from: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

5 Acronis 3-2-1 Rule of Backups. Available from: https://www.acronis.com/en-us/articles/backup-rule/

6 2018 Verizon Data Breach Investigation Report. Available from: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

7 SANS, Ouch! Newsletter - Backup & Recovery, August 2017. Available from: https://www.sans.org/security-awareness-training/ouch-newsletter/2017/backup-recovery

8 Healthcare IT News, Ransomware attack on NJ provider locks 16,000 patient records. Available from: http://www.healthcareitnews.com/news/ransomware-attack-nj-provider-locks-16000-patient-records

Publication date: March 2019

Contact for enquiries

Telephone: 1300 901 001 or **email:** help@digitalhealth.gov.au

Disclaimer

The Australian Digital Health Agency ("the Agency") makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

Acknowledgements

Council of Australian Governments

The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Australian Government

Australian Digital Health Agency

digitalhealth.gov.au