

Backing Up Your Data

Don't put all your data in one basket!

WHY SHOULD I BACKUP MY DATA?

Human Error – Ever hit the 'Delete' key by accident?

Hard Disk Failure – This can occur without warning at anytime.

Viruses and Spyware – These can enter your system through the internet or when using removable media e.g. USB flash drives.

Unforeseen Disasters – Including fires, floods, lightning and theft.

WHAT DATA SHOULD I BE BACKING UP?

All business documentation i.e. emails, marketing, financial/accounting, planning etc and all patient information including patient records stored in your clinical software database along with any other patient-identifying documentation. The general rule is, if you think you may need something should a system recovery be necessary then back it up!

WHERE WILL I BACKUP MY DATA?

OPTION	PROS	CONS
USB Flash Drive	<ul style="list-style-type: none">• Small size• Inexpensive	<ul style="list-style-type: none">• Limited storage capacity• Easy to lose
Online Backup	<ul style="list-style-type: none">• Completely automated• Backups are stored offsite• No handling of media	<ul style="list-style-type: none">• Fees can be expensive• Can slow down internet connection during process
External Hard Drive	<ul style="list-style-type: none">• Large storage capacity	<ul style="list-style-type: none">• Bulky• Often need their own power source
CD/DVD	<ul style="list-style-type: none">• Inexpensive	<ul style="list-style-type: none">• Time consuming• Storage of CDs/DVDs as they accumulate

No matter which local backup option is chosen you should always have an offsite backup as well. Your IT provider can give you advice on which backup media best suits your needs.

HOW OFTEN SHOULD I BACKUP?

Each and every day your practice is operating. Backing up should form part of your practice's daily processes.

WHERE DO I START?

Once you have selected the backup media that suits your practice it is time to create a backup strategy or have your IT provider assist you in doing so. This should include the following elements:

- 1) **Backup Software** – what software will control the backup process? There are ample software packages available online or from your local technology vendor. Ask advice and read reviews online to assist you in making a decision.
- 2) **Plan your Backups** – what time of the day will you do your backups and will using the automatic scheduling tool available in most backup software packages be useful?
- 3) **Check Backup Integrity** – you may have backed up your data, but what guarantee do you have that it will be there should a recovery be necessary? Your backup software may have a data verification option to check data integrity each time you backup and flag any issues. Otherwise you may want to schedule a restore of your backup each month or so.
- 4) **Check Backup Medium** – as we established earlier hard drives do fail so as your computer is protected using anti-virus and spyware software, it will do no harm to scan your backup medium regularly so it too is protected.

WANT MORE INFORMATION?

If you require a Disaster Recovery Plan template or assistance with computer security relating to accreditation, please contact our General Practice and Allied Health Help Desk on: (02) 8811 7117 Option 1 or email support@wentwest.com.au

www.wentwest.com.au



WentWest Limited
Level 1, 85 Flushcombe Road
Blacktown NSW 2148

PO Box 5,
Blacktown Post Shop
NSW 2148

T: (02) 8811 7101
F: (02) 9622 3448

ACN 089 255 106 / ABN 80 089 255 106