BACKING UP DATABASES & ASSOCIATED FILES

It is not the responsibility of Incisive Software Limited, or any agent appointed by us, to configure or ensure the reliability and validity of the backing up of any electronic material that is used or produced by software we produce.

This document is meant as a guide only.

Disaster Recovery is so important we believe that the Directors of your company should receive a quarterly or half-yearly report of the success or failure to being able to perform a test restore of files and databases critical to their business.
Receipt of such a report should be an item on their meeting agenda.

A backup system is only as good as the ability to restore the data

.

Use a tape backup storage device or other high-quality storage repository, with good quality backup software which allows for scheduled start times and can back files that are 'in-use'. Do a file dump to another workstation or server each day. Use five different storage media to rotate the daily backup. Take the last backup off-site each day. Test the backup by doing a 'test' restore at least every three months.

DO NOT ASSUME THAT THE BACKUP IS CORRECT. MAKE SURE IT IS.

Backup Devices

There are a range of backup devices depending on your budget. Generally they fall into two groups - disk based & tape based.

Tape backup.

Tape backups are still considered the most reliable method of backup system but only good quality systems should be used, and these are generally more expensive. The actual tape cassettes need replacing on a regular basis as they can degrade if they are used frequently.

External drives

External drives are a very cheap with a huge storage capacity. These are a suitable backup medium but at least two will be required to ensure at least one can be taken off-site.

Onsite repositories

Often an existing server or workstation will be used as an onsite repository of the backed-up files as a supplement to the off-site storage. This option can assist with the rapid restore of corrupt data files.

Internet-based backup servers

These off-site repositories are very easy to set up and take little to maintain. However, in our opinion, these should only be used as a tertiary level of backup. You should also be aware of any governmental restrictions of putting patient-related data onto off-shore servers such as Amazon, Dropbox etc.

Whole computer image snapshots

These are very fast and complete methods of backing up a server but do not run backup routines required by SQL Server to truncate the transaction log files.

Backup software

Special software is usually required to be able to copy and compress the data onto the backup disk or tape.
There are a range of choices you can use for the backup software:

Batch files

These are file created by a text editor and have a number of commands typed in it to perform the backup. eg.

```
xcopy C:\spmwin\data\*.mdb /d D:
```

Batch files are simple to create and alter but are really only suitable for doing basic, simple backups to external drives, or DVD writers.

CopyToLocal

This is a small Incisive tool that can copy Microsoft Access databases, and associated data or image files, from a server location to a laptop, or secondary workstation. The file CopyToLocal.exe is found in the \SPMWIN directory.

Microsoft Backup

All of the versions of Microsoft Windows operating system, except Windows 8.0 & 8.1, have Microsoft Backup software included with them. The Backup function may need to be enabled.

Microsoft Backup does allow you to nominate the individual files you wish to include in your backup routine and you can use an option to only backup the file if it has changed since the last backup.

Microsoft Backup does not delete or truncate the SQL Server Transaction Log.

Microsoft SQL Server

All editions of Microsoft SQL Server can use 'SQL Server Management Studio' to perform a manual backup of its databases. However, be aware that the 'Express' edition does not have the Agent tool to perform the backup on a schedule.

'Transaction Log Shipping' is an ideal method of using SQL Server to make frequent (hourly) partial backups and use them to build a clone of the live database on a server at a different location.

Third Party backup software

There are a range of companies who produce backup software that perform a large range of backup and verification functions. A very popular product is called Backup Exec produced by Symantec (Norton). In addition to the usual ability to select individual files to be backed up they also provide the following options:

- copy a 'file in use'
- email you or the technician if the backup failed
- perform SQL backups

The ability to backup a database file that is still open, that is, being used by at least one of the computers, is important especially for larger practices and hospitals. Without this ability, if even one computer was still connected to the database when the backup routine started it would not allow the database to be included in the backup.

If you are backing up an SQL database you should use the specialist functions of 'SQL Server Agent' software which allows, amongst other benefits, the ability to 'roll back' which enables a database to be recovered to a specific moment in time rather than a backup job.

ExpressMaint from CodePlex is an open-source application that is frequently used to perform scheduled backups of the SQL Server databases. It has a large range of options to configure the backup and reporting processes.
You can download it from: http://www.codeplex.com/ExpressMaint

Frequency

A backup of the patient databases and associated external files must occur on a daily basis, including the weekend if new records are added during this period.

The daily backups during the week may be partial or incremental backups as these are faster to perform than a full backup.

If using tapes for daily backups, you will normally have 5 (or 6) separate backup disks or tapes which will be labelled for each day of the week, and will be used on that day. Therefore, the last backup on a 'daily' disk or tape will be from the week before.

Each week, usually during the weekend, a full-backup is made of the whole system.

For monthly backups a single separate disk or tape is repeatedly used each month.It is recommended by the manufacturers that the cassette tapes are replaced on an annual basis. It would be advisable to have this verified by the technician configuring the tape backup device

Files to back up

The files that need to be backed up depend on the type of database that is being used.

Microsoft SQL Server

If the patient records are being stored in a Microsoft SQL Server database it will require the specialist skills of a suitably qualified technician to configure the backup depending on the software and hardware configuration.

Type of File	File	Expected Location
main patient database	spm_data.mdf	…\spmwin\data\spm_data.mdf
main patient database log	spm_log.ldf	…\spmwin\data\spm_log.ldf
dictation & lab results database	spmwork_data.mdf	…\spmwin\data\spmwork_data.mdf
dictation & lab results log	spmwork_log.ldf	…\spmwin\data\spmwork_log.ldf
spm log files	*.tra & *.trc	…\spmwin\data*.tr*
scanned documents, include subdirectories	*.tif etc.	…\spmwin\scandocs\allocated*.*
digital images & movies, include subdirectories	*.png, wmv etc.	…\spmwin\images\allocated*.*
spell check dictionaries	*.tlx	…\spmwin
faxes		…\spmwin\fax
email		…\spmwin\email
Pdf	*.pdf	…\spmwin\pdf

Note – the actual database names may differ from this example

To find the correct paths for the SQL database and other files listed above either:

1. Print a 'Workstation Setup' report from the Reports module in the SPM or PHM software, or;
2. Check the path setting used by the relevant ODBC driver. The correct name of the ODBC driver can be found in the SPM.INI file (which is in the SPM or PHM program file directory on any workstation) and on the lines where DSN= and DSNWORK=. The names after the '=' sign is the name of the ODBC driver. To find the correct path used for the storage of scanned documents and digital images log into the SPM or PHM software, select 'System' from the 'Setup' module and then choose 'File locations'.
3. Open the Properties of each database in Microsoft SQL Management Studio and find the location of the database files in the Files section
4. In SPM/PHM look to the locations specified in Setup -> System -> File Locations

The SQL Transaction Log must also be deleted each time the backup has been successfully completed otherwise it will continue to grow until it reaches maximum size.

Microsoft Access

If you are still using a Microsoft Access database, the points listed above still apply except that you will not have database log files and the database files will have a .mdb extension instead of .mdf.

Local file copies

In addition to performing a daily backup and getting those files off-site, we also recommend that a copy of the patient database(s) and associated files are copied to another computer on the network.

The reason for this procedure is to enable a practice or hospital to get the SPM or PHM software up and running again as fast as possible in the unlikely event that the main server has completely died and needs to be taken away for servicing.

It is very unusual for a tape drive to be installed onto a second computer on the network to allow the Restore of patient data, whereas with the 'File dumping' procedure we can change the ODBC settings of all the workstations to point to the copy of the database on this 'pseudo-server' and continue using it.

It may be that the computer where the copy of the database resides is not as fast as the failed server but it will allow patient notes to be printed, appointments to be made, and invoices to be printed until the server is repaired or a replacement server is found.

Notification

Use the function in the backup software to email a daily report to the practice or hospital manager, of the success or failure of the backup routine. The email address used should be a generic one (not personal) such as office@practice-abc.com so that the backup reports will continue to be received even if the current manager no longer works for you.

Restoring data

The key purpose of the backup is to be able to retrieve the data that has been backed up and allow it to be restored.

Unfortunately it happens, more often than not, where a copy of the backup data needs to be restored – but the data on the backup media is unreadable or even not there.

IT IS IMPERATIVE THAT TESTS ARE REGULARLY PERFORMED TO VERIFY THE QUALITY OF THE DATA ON THE BACKUP MEDIA AND THAT THE DATA CAN BE RESTORED.

These test restorations should be performed on a regular basis, preferably every 3 months. **Care must be taken to ensure that the current database(s) are not overwritten during the restore process.**

Confirmation of Patient Data Backup

On behalf of: _____

Name of Hardware Company

I, _____

Name of technician

confirm that the database files, log files, scanned document files, image files and any other files related to patients or the practice/hospital, that are used by the 'Specialist Practice Manager' or 'Private Hospital Manager' software produced by Incisive Software Ltd. are being correctly copied to the storage media that has been designated for purpose of backing up this data and that this backed up data on the storage media has been validated.

Date of check: _____

Signed by technician: _____

Date: _____

****

Confirmation of Patient Data Restoration

On behalf of: _____

Name of Hardware Company

I, _____

Name of technician

confirm that the database files, log files, scanned document files, image files and any other files related to patients or the practice/hospital, that are used by the 'Specialist Practice Manager' or 'Private Hospital Manager' software produced by Incisive Software Ltd. have been successfully restored from previous backups and that the above applications are able to perform correctly and with all the data expected.

Date of check: _____

Signed by technician: _____

Date: _____