Maintenance and Recovery for Your System

Each surgery has the responsibility for protecting its own data files. If this process fails then your financial and clinical records could be irretrievably lost.

The risk of data loss is always present however data loss need not be a disastrous experience if this eventuality is planned for. The strategy employed to guard against data loss should be equal to the importance of the data you wish to protect.

1. Keep your computers and network in good working order.
2. Carry out regular software maintenance with updates and patches.
3. Perform regular backups and have a disaster recovery strategy.

Maintain Your Computers and Network

- Equipment must meet the minimum recommended level to operate satisfactorily (refer to recommended hardware specifications).
- Remove problem computers from your network until they are fixed. If the problem computer is required then have it fixed immediately - Problem computers compromise the correct functioning of the whole network and the integrity of your critical data.
- Network equipment such as switches or routers, especially wireless devices, must be setup and configured by a trained technician. Test and keep network cabling and switches in good order. Poor connections can cause errors in your systems and can be very difficult to trace. It is critical that your computers are connected using properly installed and certified cabling. If you are unsure of your wiring or are planning a replacement, including a wireless network, consult a specialist in this field.
- HCN highly recommends the installation of a UPS (Uninterruptible Power Supply) to prevent damage to your hardware and data files from power fluctuations. We also suggest power points be installed or are available for the exclusive use of the computer and peripheral equipment.
- Install a virus checker and keep signature files current. Set up to auto update if your software offers this facility.

- For Internet connection, we recommend you install an Internet Firewall to protect your system unless this service is provided by your ISP. Consider whether a firewall is required – seek professional advice.
- Only use Operating systems designed for business environments. These operating systems have greater internal security for networks and users.
- Keep up to date with Operating System service packs and security fixes.
- Remember this is business environment – limit unnecessary software and use reputable hardware. ‘Freeware’ is software that may cause disruption to your

business environment - generally speaking this software is provided after limited testing and on as is bases with no support. We suggest limiting the use of such software as much as possible.

- Ensure all users have sufficient access permissions to perform required tasks.
- Use reputable and appropriately qualified professional technicians; particularly if you plan to use Terminal Server or Citrix Metaframe. The cost is small compared to fixing incorrectly configured systems and networks.

Items for Regular Maintenance

Daily - Weekly

- Re-boot your computers, daily for workstations, weekly for servers (more frequently if required). Re-booting computers flushes the memory which can be occupied by memory 'leaks' that can disable even simple operations such as printing.

Every 2-4 Weeks

- Clean-up temp files – Temp files (.tmp, .temp and temporary internet files) will occupy valuable hard disk space. You can use Windows Disk Cleanup.
- Check hard disk for adequate operating space. (Approx 2.5 x the size of the largest database.) *NOTE: Medical Director 2x requires this hard drive space to be on the drive that contains the Medical Director program files.*
- Run Scandisk or Chkdisk on all drives
- Defragment hard drives – This will increase stability and help protect against slowness, cross linked files and data loss. The following articles might assist: http://www1.execsoft.com/pdf/Stability_WhitePaper.pdf http://www1.execsoft.com/pdf/Effects_of_Fragmentation_on_Reliability.doc
- For Medical Director run File Repair Utility monthly unless otherwise advised by HCN Technical Support.

Backup and Disaster Recovery Strategy

Backing up the data from your practice management and clinical software is one of the most important "housekeeping" tasks that should be performed on a daily basis.

Most practices are aware of the need to secure their data but seldom check the integrity of the process by restoring the data to confirm that a successful backup has taken place. Computer systems are generally reliable but for most users the need to recover from a system failure will occur at some time. It is also important that you know how to retrieve data should the need arise. With some forward planning this potential disaster can be little more than a short and inexpensive process.

Recommendations for Back Up

- Take a daily backup of all files that are important to the running of your practice. (ie: clinical data files, practice management data files, document files, financial records, etc.)
- Keep separate backup media for each day of the week.
- Take some backups offsite but keep them readily accessible should the need arise.
- Periodically restore a backup to a temporary location to check the integrity of the backup process and to test the ability of your staff to perform this task.

These recommendations represent a *minimum* set of standards to protect you. Other considerations are:

- A permanent weekly, fortnightly or monthly backup, burnt to a CD or DVD. This provides an historical record that could be used to restore your data or as proof of the integrity of your records.
- If you do not have a CD burner, an increase in the number of backup cycles can provide a better coverage than the common 'once a day' backup. Refer to the Backup Cycle Example for a more secure process.

A good backup strategy is business critical, therefore consult with your IT specialist to ensure that your strategy is correct for your situation.

The responsibility your surgery has for protecting your data deserves due consideration and forward planning. If you have a system failure in your surgery and you are prepared for this eventuality then the downtime and costly staff hours can be avoided.

Backup Cycle Example

Organise your backup strategy based on weekly and monthly cycles. The weekly cycle will ensure you can call on your information as far back as 3 weeks and your monthly will allow you to call back on your data as far back as 12 months. The cost of backup media can be insignificant compared to the costs of data loss or an extended recovery.

Daily - Backup every day Monday to Thursday (this should include Friday if the practice is open 6 days per week or Friday and Saturday if the practice is open 7 days). Each day's media will be overwritten on the same day next week.

Weekly - Take a full backup at the end of the working week. This backup is executed on Friday, Saturday or Sunday depending on the days worked per week.

Ensure you have media for Weeks 2 and 3 (and Week 4 for 5 week months) as explained above. Each weekly media will be overwritten on the same week next month.

The last week of the month (Week 4 or 5) you will need a monthly backup

End-of-Month - Take a full backup for the last working day of the last week of the month. This may be a Friday, Saturday or Sunday depending on days worked. This end-of-month media should be labelled with the name of the month and securely stored for 12 months. This media will be overwritten in the same month next year.

Example: The backup cycle below is for a 5 day working week and caters for a 5 week month. An extra 5 Media would be required for a 6 day week, an extra 10 for a 7 day week.

Week1	Mon	Tue	Wed	Thu	Week1 Backup	
Week2	Mon	Tue	Wed	Thu	Week2 Backup	
Week3	Mon	Tue	Wed	Thu	Week3 Backup	
Week4	Mon	Tue	Wed	Thu	Week4 Backup	
Week5	Mon	Tue	Wed	Thu		Month1 Backup
						Months 2-12 Backup

- Rotate backup media on Monday to Thursday (4 media required)
- Have 4 Weekly media available (to accommodate 5 week months)
- Have 12 Monthly media.
- Total 20 media required for 5 day working week.