



The Backup Secret That Computer Companies Don't Tell You

ExpressPlan
7078 Peachtree Industrial Blvd.
Suite 200
Norcross, GA 30071
877-294-1211
© 2004 ExpressPlan

The Backup Secret That Computer Companies Don't Tell You

The Problem

If yours is like most dental practices, you have invested significant time and resources into selecting and implementing computer systems that support the safe and efficient operation of your practice. This information generally includes patient demographic, billing, medical history, appointment scheduling and insurance information. You may have also computerized your patient charting and imaging records including digital x-rays and patient photographs. Additionally you may base mailings and phone calls such as appointment reminders and birthday cards on your computerized data. Without these records your practice would have an extremely difficult time functioning.

You probably think your practice management data files are protected. You probably think that your backups will pull you through any computer disaster you can envision. You are probably wrong. All of your practice's data can be lost forever in an instant without proper backup. Most computer companies talk about how much data a particular backup device can store or how fast the data can be written to it or retrieved from it. However, what they don't tell you is that the solutions they offer generally have at least one fatal flaw.

Backup Solutions

The most popular traditional backup solution is to run a backup program as part of the practice's normal administration tasks — usually at the end of the day. The backup media may be tape, disk, ZIP disc, CD-R, CD-RW or Jaz disc. Recently, it has become affordable to back up to a second disk drive in real time as the data changes throughout the day.

Typically, backup schemes call for multiple sets of backups that rotate in a son, father and grandfather sequence. Thus, today's backup is the son, yesterday's is the father and backup from two days ago is the grandfather. On the fourth day, the grandfather becomes the son, the son becomes the father and the father becomes the grandfather. More sophisticated schemes provide for weekly and monthly rotating backups as well. When these schemes are managed properly, there are always multiple backups to fall back on.

Backup Media

Tape

In the past, most sizeable data backups were stored on tape. At the time tape was the least expensive, most reliable data backup solution available. However, as drive sizes increased beyond the capacity of a tape cartridge, tape backup became more difficult because tapes are relatively slow and a single backup often required multiple tape changes. Tape drives and tape cartridges are also expensive devices. Now, many corporate practice administrators use a separate backup server, but this is not an economical solution for most dental practices.

ZIP, CD-R, CD-RW and Jaz Discs

These are all relatively inexpensive media to use for backup. Zip and Jaz have become less widely used due to their proprietary format and their higher cost compared to CD-R and CD-RW discs. The difference between CD-R and CD-RW is that CD-Rs can be written to only once while CD-RW disks can be reused many times. The trade off is that CD-RW read and write speed is several times slower than CD-Rs.

The advantage of both CD-R and CD-RW is their industry-standard format and low cost (usually under \$1 per disc). The disadvantage is that their storage capacity is 500-600 megabytes and a daily backup can fill several disks. Also, to restore the data the discs must be read in the same order as they were written so care must be taken to label them accurately.

Hard Drive Mirroring and RAID

Mirroring the hard drives in a server involves installing two disk drives in it. When the server writes data to one drive, it automatically writes that data to the other drive. Such a mirroring system is not very expensive, it provides nearly instantaneous, synchronized copies on both drives, and it does not require any special restore process should one drive fail.

The other multi-disk backup solution to consider is RAID, an acronym for redundant array of independent disks. If one drive fails, the storage system can recreate data from the missing drive. In some RAID systems, it is possible to hot-swap (while the computer is running) the failed drive in a RAID system for a new one. The RAID system then rebuilds the data onto the new drive. RAID systems can be more expensive than mirroring but they are also more reliable.

External USB Hard Disks

These drives combine the advantages of a hard disk with the convenience of removable media. They are fast and relatively easy to carry. Each drive must be large enough to contain all of the data with three of them needed to implement a three-generation backup. Weekly and monthly backups each require an additional disk.

LAN Backup

As the speed of Local Area Networks (LANs) has increased, LAN backup has become practical. LAN backup is a technique in which the data from the server on the LAN is backed up to another computer on the LAN. To do this requires establishing a procedure to copy the data from the

data server across the LAN to other machines with sufficient space to store a copy of the data. In a practice with multiple computers, it is advisable to back up the data server to one or more of the workstations, preferably in a rotating pattern.

Remote Backup

No backup solution is secure if the backup media is stored at the practice. Fires or other disasters that can damage the practice and its computers can also destroy this on-site backup. Even putting the backup in a fire-rated safe is seldom useful since most of these safes are rated to protect paper, not computer media. Computer storage media such as tape or disk can be destroyed at much lower temperatures than paper.

The traditional remote backup procedure requires physically removing the backup media from the computer and storing it off-site. Recently, faster networking speeds, both locally and on the Internet have made electronic remote backup an affordable and practical reality.

The Backup Secret That Computer Companies Don't Tell You

It is generally accepted that the safest path is to use as many of these backup techniques as you can. Raid and LAN backups should protect most dental practices from the most common data-loss problems. However, neither will protect the data should a disaster occur in the practice office. To be as safe as possible the practice needs off-site backups that can reliably be used to restore the data.

The secret that is often not disclosed is that all of the off-site backup techniques rely on manual intervention and none of them guarantee that you will be able to recover from a disaster should you need to restore your data from them.

The Fatal Flaws

There are a number of conditions that can render your backup scheme ineffective.

Tape

With tape, the backup must be entirely error free. Just one error on a tape can make it unreadable and useless as a recovery source. Further, many incompatible tape formats exist and even new models from the same vendor could be incompatible with their earlier products. It's possible that a backup tape from a two- or three-year-old computer may not be usable because tape drives using that tape format may no longer be manufactured and, if it's available at all, must be special ordered. Tape drives are also sensitive to head alignment issues that can make a tape created by one drive unreadable by another drive of the same model.

ZIP and Jaz Discs

These are obsolete technologies and it would be difficult to find replacements should these drives be damaged. Practices currently relying on these products for their backup needs should be investigating other alternatives or supplementing these backups with other technologies.

Mirrored and RAID Disks, and External Disk Drives

These disk solutions address many of the shortcomings inherent in tape, but they still present a significant problem. In a scenario where the server fails due to a non-disk issue it would be expected that at least one (and usually both) of the redundant disks would still contain current data. If the external disk were available on-site, it too would be assumed to contain current data. However, there would be no other server-grade computer in which to put the disk. Thus, the practice would still be without its data until the server could be repaired or replaced.

Common Issues With All of These Technologies

There is an inherent issue that all of these backup technologies share. All are dependant on the memory and conscientiousness of the person in the practice who is responsible for maintaining the backups. All of these technologies rely on a human being to rotate the media in the server on a daily basis and remove/return the media to an off-site storage location (often the employee's home).

The difficulty is that people often don't remember, or simply fail to perform, the necessary steps:

- Media is not rotated and the same disk or tape is written over repeatedly.
- Media is left in the server and not removed from the building. (Although we've seen this happen with disks, it is especially common with tapes. Since tapes are slow they are often left to complete the backup overnight and they are not taken from the building the following morning.)
- Failed backups are not recognized and restarted.
- Manual backups often fail to include needed files or directories.
- The responsible person leaves the practice and the procedures aren't passed on accurately or don't get passed on at all and the backup isn't even initiated.

Cases have been documented in which, due to staff turnover, the backup process was not executed and the backup media had not been rotated for more than 6 months. The practice was totally without a backup and nobody knew it for half a year. Even if the employee does perform the backup there is still a critical step that is almost never executed — restoring and testing the data to verify that it can be used. ***Without performing this verification step there is no way to determine if the backup can be used for its designated purpose.***

The Risk Of Not Validating The Backup

Performing the backup data verification on the practice's server presents risks of its own. In order to test the restored data safely, all system users must be logged off of the system. Then a copy of the live data and the relevant program files on the server's disk must be copied to another location on the server's hard drive, another LAN-connected computer, or one of the other media described in this paper. The backup file must then be restored over the live data, thus destroying it. Then the programs that use the data must be executed to ensure that the restored data is usable.

This is seldom the type of task that a non-technical practice staff member would be comfortable performing. And, while the verification test is being performed, the server cannot be used. At

best, this will only inconvenience some of the staff while the data is restored and successfully verified. At worst, the restored data will be unusable and the live data could be corrupted or otherwise not usable — leaving the practice with no valid data and a non-functional system.

Solutions

After extensive research and numerous product evaluations, ExpressPlan has identified two solutions that address all of the shortcomings of the backup technologies and schemes discussed above. The first is a dual or Gemini server; the second is automated network backup via the internet.

Gemini (dual) Server

ExpressPlan's Gemini Server is comprised of two LAN-connected computers with identical hardware configurations except for their hard drives. The primary computer contains two RAID disk drives — one fixed and the other removable. Under normal circumstances this computer is used as the network server and the second computer is used as an administrative workstation.

During normal operation all data is written simultaneously to both the internal hard drive and the removable hard drive on the primary server. **Should one of the hard drives in the must be replaced.** Once it is replaced the drive will be detected and the contents of the functioning drive will be written to the secondary drive and once again the server will operate with two drives.

In the event that a failure occurs with the server such as a motherboard or power supply failure, the removable drive, which contains all the server data up to the time that the server failure occurred, can be removed from the server and used to replace the removable drive in the spare server. The main server is left turned off and the system recognizes the spare server as the “new” server. This swap-out procedure can occur in less than 5 minutes. This can be accomplished by a non technical staff person who can follow a few simple instructions.

Because the primary server is capable of duplicating the internal drive to the removable drive automatically, this removable drive can be used as an off-site backup device. At the end of the day, the removable drive is replaced with another removable drive. The internal drive is then told to duplicate itself to the new removable drive. After the duplication process is completed the server is once again functioning with two identical drives. The recently removed drive can be packed in a carrying case and removed from the premises.

DigitalShelter - Automated Network Backup Via The Internet

DigitalShelter is an on-line backup service that automatically transfers practice management data to secure servers each night without any intervention by the practice's office staff. DigitalShelter online backup system is completely automated. There are no schedules to keep up with and no removable media deal with. There is no human intervention required whatsoever.

DigitalShelter includes a monthly test of the practice's backup. To ensure the integrity of the data it is restored to a server at ExpressPlan that contains your software systems. The data is

then run through your software on our server and tested for validity. A summary page print out of the daily transaction report of the most recent day in the backup set (daysheet) is faxed to the practice for comparison with the report from that day, providing proof that the backup set is able to be restored when necessary.

DigitalShelter meets HIPPA disaster backup and recovery requirements. Before this sensitive practice data leaves the server, it is encrypted with Triple DES, 168-bit encryption to protect it. The fully encrypted backup file is then transmitted to triple redundant servers located at three different locations across the U.S. Removing the backup from the premises provides an automatic additional layer of security should the office experience a destructive event.

Conclusion

Computers have never been a better value and the variety of backup solutions available is many and varied. Unfortunately, almost all of these technologies and the commonly used backup schemes require daily attention, the physical removal and rotation of the backup media, and the potential for a data crisis. It's virtually inevitable that the manual procedures will at some point break down. ExpressPlan's experience indicates that the most affordable and reliable means to provide a secure backup environment is through a "dual" server and an automated network backup via the internet. Either would be a vast improvement over the backup schemes used in most dental practices and using both would provide the highest level of security and peace of mind.

If you would like additional information on any of the topics discussed in this paper or related issues that may be a concern to you please feel free to contact ExpressPlan. 877-294-1211. www.expressplan.com.