

How safe is your computer data?

Why Backup

Backing up computer information is something we should all do regularly. However, most people only backup with the benefit of hindsight after some dreadful computer problem. By then it is normally too late.

All the information on your computer is held on one or more hard drives. These are discs slightly larger than a packet of cigarettes, running for many hours a day and spinning at speeds of up to 7200 rpm – which is faster than your car engine. Inside a number of heads will read and write information onto the discs at high speed (a bit like a 4-5 very small and fast record players stacked on top of each other). Although these little units can run perfectly for years, they can fail and when they do, the results can be very serious indeed.

The hard disc can fail in a number of ways. Data can simply become corrupt - a few vital bits of information are recorded incorrectly and you will be unable to open the file again. Spinning at high speed can cause any fractures in the disc to eventually crack and can in some circumstances provide an impressive if not completely catastrophic breakup of the disc while rotating at speed.

Perhaps the most common is a head crash, here the reading and writing head comes into contact with the platter or surface of the disk. This results in severe data loss and if the data is required then a specialist would have to be employed to retrieve the data. Simple drive recovery can cost upwards of £4,500 and success is not guaranteed so it is definitely a last resort.

Hard drive failure is not the only reason that you may lose data, hard drives can be lost by fire, laptops misplaced on trains or simply stolen by thieves.

I was once told the following story by a university lecturer. To make your data on your computer secure, take it off the internet, remove the hard drives, place them in a concrete block, take them out to the Mariana Trench and drop them into the ocean. However this is still not 100% secure as the data is still accessible to somebody who really (really) wants the data.

Backing up

So you back up to protect your data from thieves, fire and disk crashes. To protect from disc crashes is quite a simple process. Most modern computers will support multiple hard disks in a RAID (Redundant Array of Independent Disks). RAID comes in a few flavours: RAID1 is the cheapest and uses two hard drives; everything on the first disk is automatically duplicated on the second. In the event of one hard disc failure you have a carbon copy on the other disc ready to use.

Whilst this does solve the problem of hard disc failure, a thief or fire won't leave you your second disc. So a better solution is to store the data elsewhere. NAS (Network Attached Storage) devices can be hidden in attics or even placed in fire proof safes. These are accessed via your local network and are an inexpensive and relatively easy device to set up. They come in many sizes and types, however, ensure that they use RAID1 (or the more efficient RAID5) so that if one of the drive fails

you'll still have your data. Most people using a NAS device access their files straight from it, using it as their main hard drive, so technically, its not backing up but it will keep your files and data relatively safe.

Various versions of windows contain backup solutions which will allow you to backup to disc, some NAS also have one touch buttons or programs that will take the various information stored on your computer and copy it easily to another location.

CD is not a particularly good backup resource as it can degrade over time. Tape back up is still by far the best medium as a little data loss on one part of the tape won't affect the rest of the data. However it is slower and more expensive than hard drives, which for most readers would be the best option.

You can also outsource your backup solution. Clinic management systems tend to have backup solutions built into them. Online clinic management automatically handles all of the backup and security problems for you. Since the data is not stored on your machine or on your premises, you don't need to worry if you computer system gets stolen or damaged. Multiclinic, for example, stores all the user's data on encrypted RAID hard drives, should this data storage be accessed or stolen it would take 100 years to crack the data on the discs. As a further precaution, overnight backups are made to yet more storage at another location. All in all, far more care is taken with the data than most users would ever want to undertake themselves.

For data outside of your clinic management software you can rent offsite storage, Mobile Me from Apple is a good solution or Dropbox if you don't want to pay for it!

If you use paper records you may want to consider scanning them and backing them up. Paper diaries don't crash but they do burn, get torn or even get thrown away. Could your business survive if you lost the contents of you diary tomorrow?

Dominic Hampton is the Director of Attend 2 IT, an IT consultancy company which manufactures Multiclinic – an online clinic management system which handles the backup and data encryption process for you. www.attend2it.co.uk 01763 87 80 86