Synergistic Office Solutions, Inc.

Topic	Backing Up Your Data
Document ID	125
Product	ALL
Last Revised	February 2, 2009
Authors	Seth Krieger, Manon Faucher

The most important task of the day is backing up your data!

Nothing that you do on your computer in the course of a day -- or for that matter, a month -- has anywhere near the significance of your backup procedure. A good backup will someday mean the difference between a minor inconvenience and a very costly disaster. It is only a matter of time before a system crash, burglary, fire, or even a data entry error, will make your backup the only indispensable part of your system.

Consider these scenarios:

- You update the operating system (Windows) in your computer and subsequently find that you can no longer access your data. Your ledger and patient information are destroyed.
- You come into the office one day, only to find that every piece of office electronics you own is missing. On the further investigation, you find that all your tapes, data cartridges, and CD's are gone as well, including those you had been using for your data backups.
- A power outage during a critical data update procedure corrupts several major data files.
- In an attempt to free up some disk space, you accidentally delete all the files in your SOS data directory.
- There is a fire at your office over the weekend and your computer system as well as all disks and tapes are literally melted.
- You have been making backups, but each day, you use the same media for your backup. One day it is necessary to restore from your backup, but you find that the tapes or cartridges are not readable.

There and many other possibilities are out there, just waiting for the day that you can least afford the time and energy to deal with them. **What can I do to safeguard my data?**

1. ***SOS Applications do not have a built-in backup program***. Use high quality, brand name, data backup software or the backup software that came with your tape, cartridge, or CD/DVD drive.

2. Configure your backup software so that all error checking, error correction, and/or verify options are turned ON. Also turn on the data compression feature, which is sometimes called something like *minimize space*. If there is an automatic compare feature, turn that on as well. We recommend that you always use the full backup option, rather that the differential or incremental options. In the event that you have to restore from a backup, having made a full-type backup will make restoring your data much easier. Save these options.

3. Next you may want to follow the instructions that came with your backup software for creating a setup or script that will permit you to backup only those files you want to save. You can, for example, have a setup that backs up only the data files in your \SOS\DATA folder, which is the folder containing the SOS database. If you are using our electronic claims module, you may want to include your \SOS\CLAIMS folder as well.

4. Many backup programs include a configuration option that will tell the program to email a report to you at the end of every backup operation to let you know if any errors were encountered. Checking to be sure your backup is running correctly is critical; this option makes that part of the process quick and easy.

5. Another feature offered by most backup programs is data encryption. If you will be transporting the backup out of the office, encryption is a requirement to be HIPAA-compliant, and an obvious safeguard of your patients' privacy. Make sure that you record the encryption key and that all parties who need it will be able to find it, should the need arise, even years after you have gone on to greener pastures. It might be a good idea to select a reasonably secure encryption key and include it in a written backup/recovery procedure document. Your backups will do you no good if you cannot unencrypt them.

6. It is absolutely essential that you rotate your backup media. In short, what this means is that you never use the same cartridge, tape, or backup disk two days in a row. The bare minimum should be a rotation through three backup sets, but we strongly recommend that you purchase enough cartridges, tapes, or disks to allow you to backup each day of the week on a different tape or cartridge, plus several more for rotating off premises.

For example:

Cartridge/tape/CD/DVD #1	Use for backup on Monday
Cartridge/tape/CD/DVD #2	Use for backup on Tuesday
Cartridge/tape/CD/DVD #3	Use for backup on Wednesday
Cartridge/tape/CD/DVD #4	Use for backup on Thursday
Cartridge/tape/CD/DVD #F1	Use for backup on first Friday of the month
Cartridge/tape/CD/DVD #F2	Use for backup on second Friday of the month
Cartridge/tape/CD/DVD #F3	Use for backup on third Friday of the month
Cartridge/tape/CD/DVD #F4	Use for backup on fourth Friday of the month
Cartridge/tape/CD/DVD #F5	Use for backup on fifth Friday of the month

Note that there is a separate disk, cartridge or tape for each day of the week, Monday through Thursday. Friday will be our safety day, so there are five separate Friday backups. On the first Friday of the month, we make our backup and take it off premises. When we reach the last Friday of the month, we will have four or five Friday backups at our second location. At this point, you bring the one you will need at the end of the next week back to the office. Once the system is running, there will be only one Friday backup at the office at any given time.

Another option is to make a permanent copy of your database on a CDR or DVDR once each week, and store these copies in a secure, off-site location. In that case, you would need only one tape or re-writable disk for each day of the week, including Friday, and you would not need separate monthly archives discussed below.

The safety location is often the home of one of the people in the office, perhaps the owner of the practice or the person responsible for making the backups. Storing some backups off premises provides you with an extra margin of safety in the event of a fire, burglary, or other event that might result in the loss of the data on your hard disk, as well as any media stored near the computer. Some people use a fireproof box or safe at the office for the safety backups, but we see this as a compromise and strongly suggest storage in another location.

For additional security, SOS recommends that you make an archival backup at the end of the month, and rotate through several monthly backups. Even better would be to make the archival backups on CD-R, or DVD disks (CD's that can be written only one time. They are very inexpensive and take up very little space.) Archival backups are also stored off premises, sometimes in a bank safe-deposit box. This extra step will allow you to restore your financial data for an entire quarter or longer.

7. In addition to all of the above, you should subscribe to one of the many HIPAA-compliant online backup services (do a web search for "online backup"), or have your IT consultant set up daily uploads of an encrypted backup to an off-site web server, preferably located far from your office. This copy will be your doomsday backup, to be used if a natural disaster or other event makes recovery of your regular backups impossible. With a backup of this sort, you can be back in business within a day or two even if your entire town were to be destroyed by a hurricane, flood, tornados, etc. The steps you would follow in the event of such a catastrophe should be written in your policy and procedures manual (another HIPAA requirement, by the way). Online backup services such as MozyPro.com are inexpensive and easy to set up. In addition, most services save several versions of your backup, in case you need a copy of a backup from a couple of weeks ago and are not following the multi-generational strategy outlined above.

The bottom line is that you can never have too many backups!

8. Periodically, no less that once a week and preferably after every backup, run a compare on your backup immediately after completing the backup process itself. Most backup software can be configured to do a "compare" or "verify" pass automatically. This operation will compare the data on your backup to that on your hard disk to be sure that you are making an accurate backup. It will also alert you to the possibility of a bad or worn out tape or data cartridge. If doing your compare pass automatically, ***be sure to check the backup error log every day*** to see the results of the compare. Again, doing so is a simple matter if your backup software supports email notification.

9. Have a disaster recovery drill on a regular basis. Start by renaming your \SOS\DATA folder to something else, such as DATASAVE. Now try to restore your backup, following the appropriate restore procedure for your backup software. When the restore is complete, open OMWin to be sure the database is intact and contains all the data that you believe it should. If you cannot open the database, something is wrong with your backup procedure and you must correct it. If the program starts fine and you can access all your data, you know your backup procedure is working. You can now delete the DATA folder, including the files you just restored, and rename DATASAVE back to DATA.

If you follow the type of procedure outlined above, you can rest assured that your data will be safe and available should you ever have to restore from a backup.

Backing Up a Database While It Is Running

In some installations it is desirable to keep the database running 24 hours a day or to do a backup without stopping the database. You cannot backup a running Adaptive Server Anywhere database using *any* commercial backup software, so a special procedure must be used. (Even if you manage to make such a backup of the files while they are open, it is exceedingly unlikely that the database would run after restoring from it.)

There is a downside to running the database non-stop. There are several maintenance/clean-up procedures that run automatically when the database is started. If you never restart the database, it is possible that you might run into minor issues, such as the inability to log into the system with a particular user ID after that user disconnected from the database in an unusual fashion. See Database Tools in the Admin Module to do the cleanup manually. SOS recommends that you restart the database once each day to allow these maintenance procedures to run.

Even though you cannot backup the data files while the database is running, you can make a copy of the running database in a separate directory. You can then configure your backup software to backup the copy and to ignore the directory in which the production database files are located.

Create a batch file (CMD file) containing the following commands. The first command runs a verify test on the database to alert you to certain types of data corruption. The results open in a NotePad window. You can omit that step if you want to:

```
c:\sos\dbtools /v
c:\sos\dbtools b=<target directory> -y
```

where <target directory> is an existing directory in which you want the copy of the database to be created. This directory must be located on the computer running the database. It should NOT be a shared folder on another computer! Make sure that this target directory is included in your backup configuration so that the database copy is backed up, and set the backup to skip the \SOS\DATA directory in which the running database files are located.

The first line of this batch file runs a "validation" of the database. When it is complete it displays the results on screen. Be sure to check this display each day so that you will know if any problems have developed since the previous backup was done.

You can run either the validation or the database copy interactively from the menus in the DBA Utils progam in the Admin Module. Once the program has started, go to the **Tools** menu. Run the validation by selecting **Check Database**. Select **Copy Database** to make a live copy of the running database into a different directory.

It is absolutely essential that you monitor your backups closely to be sure that the current database files are being copied to your backup media. If you are using commercial backup software, be sure to turn on the "verify" or "compare" operation and inspect your backup logs every day!