PowerSoftMD Backup Information

All data, information, and software programs relating to your PowerSoftMD system is your responsibility. Data Tec is not responsible for backup of anything in any way. But, here is some information that might help you develop and implement your backup strategies.

Basics:
1) All PowerSoftMD Patient Data and PowerSoftMD programs are in the **\EZW** folder on your server. This is the **\EZW** folder in the root directory of the drive you share with all your work stations.
2) Additional Insurance claims information is stored in the **\EZWCLAIM** folder on your server. Again, this is the **\EZWCLAIM** folder in the root directory of the drive you share with all your work stations.
3) You need to have a complete backup of these two folders (**\EZW** and **\EZWCLAIM**), their subfolders and files to recover from any type of failure.
4) Periodically check your backups to make they are actually working.

Levels of Backup we would recommend:
1) The server computer should be completely backed up to a remove storage device on a nightly basis. Rotate through at least 5 different backup storage devices, and take the devices out of the office in case of theft or fire. (Fire Proof Boxes Don't Work)
We recommend this backup contain the complete server computer including the disk you share PowerSoftMD on, as well as your operating system.

2) Let the PowerSoftMD Cross Network backup run on the network work stations, these backups do not backup EMR data, but they do backup the Billing and Scheduling information.

3) EMR users should enable the SOAP Note options to backup up SOAP notes on the local work station C: drive. From the SOAP Notes screen select the top Tools option, then "Option Setup" and check options 3 & 4 on the left side. This causes copies of your SOAP Notes to be stored on the work station where they were created or edited. There is also a built in recovery option available from the Tools option.

Caution be sure to scrub the hard drives of any work stations you sell or give away, to make sure any copies of patient information have been removed completely (your hardware people can help you with this).

4) Attach an extra external portable Hard Drive to one of your computers, I recommend the computer in the doctor's or business managers office, that is set to copy any files that have changed on an hourly or every two hours during the business day. I recommend using a fast USB 3 or Fire Wire or SATA connection. Just something that is fast. You can do this by creating a simple batch file and having your Windows Scheduler run it every hour or two hours. The first time it runs could actually take a couple days because of the initial volume of files that will be backed up.

PowerSoftMD Backup Information

4) continued……
The batch file would look like:

Hourlyback.bat

```
---------------------------------------------------------------------------------------------------
echo off
cls
Z:
md      Z:\EZWBK
md      Z:\EZWCLAIMBK
xcopy   H:\EZW\*.*          Z:\EZWBK\*.*          /S /H /D /R /C /Y
xcopy   H:\EZWCLAIM\*.*  Z:\EZWCLAIMBK\*.* /S /H /D /R /C /Y
exit
```

Where H: is the PowerSoftMD Shared Drive Letter, and Z: is the letter of your backup device.

I would also set up an evening batch file that clears all the file attributes on your external drive backup. The batch file would look like:

Evening.bat

```
---------------------------------------------------------------------------------------------------
echo off
cls
Z:
attrib –s –h –r    Z:\EZWBK\*.*   /S
attrib  -s –h –r    Z:\EZWCLAIMBK\*.*   /S
exit
```

Where Z: is the letter of your backup device.

5) Online or Internet backups. As an added layer of backup protection you can also subscribe to an Online Internet backup service. Some considerations in using such a service include:

A: Make sure the service encrypts the data and is HIPAA compliant.
B: The first time you backup could take overnight or even multiple days; unless the service lets you send them a external disk image to start from.
C: Backup any changed files from EZW and EZWCLAIM folders just like your local backups.
D: Password protect the backups, and put the password in a safe place where you can find it if you need it. Periodically change the passwords, and change them for sure when staff changes.
E: Have the service keep multiple versions of your data, so they can go back several days or even a month or so to retrieve a file. You may not know a file was damaged for several days.