visual-eyes
Simplify Your Life!

Backup Reference Guide

Backups are the most critical part of a practice's infrastructure. Without them, the failure of a single key element could result in the complete loss of valuable patient data. In this guide, we will review some backup best practices that you can use to ensure that your Visual-Eyes patient data is safely and securely recoverable in the event of a disaster.

What should I backup?

Before we talk about *how* you should back up your data, we need to discuss *what* data needs to be backed up. Our recommendation is as follows:

Visual-Eyes Data Files: Most of our clinics are setup with two different VE7 data folders, located on two separate hard drives. You want to ensure that you are frequently backing up the following databases on a regular basis:

- VE.FDB – *This is the most important file to backup as it stores your main patient information*
- BILLING.FDB
- CATALOG.FDB
- EXAM.FDB
- LIST.FDB
- LIST_PUB.FDB
- LIST_STATIC.FDB

Your main Visual-Eyes database will also produce a number of .ILOG and .IMLG files, which should also be backed up on a regular basis.

Patient Links: If you are using File Linking through Visual-Eyes, you need to back up your links as well. They are typically stored in your VE7\VE_Links directory in the form of an .IZIP file. Every month a new subfolder is created, which allows you additional control over the age of the files you are backing up.

Other Key Clinic Data: Other third-party databases you use, such as advanced imaging, field, accounting software, or anything else not stored in Visual-Eyes, should also be backed up on a regular basis. The size and location of this information can change based on the software you are using, so consult your vendor's documentation for their recommended best practices.

What should I store my data on?

There are several types of storage mediums available, however some are more reliable than others. It is recommended that, if possible, your data is backed up onto an external media such as a Solid-State USB Drive. This includes all USB thumb drives, as well as a selection of larger external hard drives. The model you opt to use will depend on the amount of data you are backing up.

We recommend that you use more than one method to backup your data. This can be accomplished in a few ways, such as pairing one of the below options with the usb/external hard drive option:

Mirrored Onsite Data: This means that a copy of your data exists on another physical machine within your office. Many backup solutions will provide a mirror option to accomplish this.

Cloud Backups: Cloud backups leverage third-party infrastructure to safely and securely store your data off-site. It is important that your medical data is being stored within Canada. Amazon S3, Bell, and Sync.com are some third-party options that offer these services with region control. The services typically include file versioning, which allows you to recover historical copies of your data in the event of a corruption. Your backup software may integrate with one or more of these services. If it does not, you can perform a manual backup by uploading a copy of your data to a service of your choice.

How should my data be stored?

As with any sensitive and private information, it is critical that any patient data leaving the premises is encrypted. Encryption is the process of obscuring a file to make it unreadable without access to the encryption key you set – therefore, it is crucial that you do not lose your encryption key as this would leave your data inaccessible. Ensure there is someone else that you trust that knows your encryption key, or that it is stored in a secure location, such as a fireproof safe.

Once your backup is complete, it is important to store the data in an appropriate physical location. Typically, this means somewhere outside of your physical business that is secure, and where environmental conditions will not negatively affect the storage device.

What kind of backups are there, and which ones should I use?

Depending on the backup software or solution you choose, there are different ways to back up your data. The most common methods are:

File Level Backups: This creates a copy of your selected data (ie. the files listed on page 1) onto the external media mentioned above. These files will be unencrypted by default, so it is a best practice to ensure your backup solution is capable of encrypting File Level Backups, or that your external media is encrypted in some way.

Machine Level Backups: This creates a copy of the entire computer, including the operating system and file structure. Machine level backups are ideal if you anticipate having to completely replace a computer and do not wish to set it up from scratch. They tend to be larger and take longer to run and restore. Again, you will need to enable encryption and create an encryption key for these backups.

What is an incremental vs a full backup?

When creating a backup job, your solution will likely ask you to choose between incremental and full backups.

An **incremental** backup compares the existing backup files against the current data, and only backs up data it determines is new. This optimizes the time it takes your backups to run, as well as the storage space they use. For something like patient links, this is a common option as links are grouped by month.

A **full** backup does a full backup of your database each time it runs, regardless of what already exists on the external media. This can lead to duplication of data, but also ensures a fresh copy is made each time.

When should I backup my data?

Typically, backups should be performed after hours on a set schedule. We recommend an incremental backup be performed nightly, with a full backup being performed once per week to ensure total file integrity.

How do I verify my backups?

The most important part of any backup policy is ensuring that your backups work. It is important that backups are regularly confirmed to ensure that they can restore the correct information properly. Depending on your preferred solution, there are different ways of achieving this. Some backup software will allow you to perform a verification on the backup files, while others allow you to enter the encryption key and view the data.

Please discuss your backups with your hardware support vendor to verify your backups are being properly managed. You can also contact our Technical Support team at support@visual-eyes.ca for additional questions regarding backup procedures.