**Purpose**

To provide instructions for accessing patient history files using an encrypted USB drive when the Sunquest system is not operational. (SQ Downtime)

**Method**

|  |
| --- |
| **Select the USB drive used for Daily Patient History Back-up** |
| **1** | Remove the flash drive from the Downtime Folder. |  |
| **2** | Drives are labeled ODD and EVEN. Select the flash drive that has the **most current** capture:* If the capture has not been done yet, select the drive for the previous day.
* If the capture has been done, select the drive for the current day.

**Example:** Downtime starts at 0200 on the 15th. Capture is scheduled for dayshift. Select the EVEN drive to access the capture of the 14th. |  |
| **Prepare USB drive:** |
| **1** | Insert the encrypted flash drive into the USB port on the hard drive.  |  |
| **2** | Found New Hardware appears on lower desktop tool bar. Box opens with “Removable Disk (:E)”.  |  |
| **3** | Select folder “TrueCrypt” |  |
| **4** | Select the TrueCrypt program (blue icon). |  |
| **5** | Double-click on “Select File…” button |  |
| **6** | In the “Select a TrueCrypt Volume” window:* Select “My Computer” or “My Documents”
* Open “Removable Disk (E):”

 |  |
| **7** | Select BBCrypt and click “Open”. |  |
| **8** | *Note: In TrueCrypt, the volume box displays “E:\BBCrypt”.*Click “Mount”. Notice that the USB drive now displays a pulsing light. |  |
| **9** | Password prompt: Enter **bl00db@nk**. (o’s are zeros, a is @ symbol). Do not check any of the boxes and click on OK. |  |
| **10** | Diminish this screen *Note: the F drive is now open. This encrypted part of the E drive (like a subfolder) contains the captured patient information.*  |  |
| **Access Captured Files** |
| **1** | Open local disk (F): |  |
| **5** | Open folder “Transfusion Services Backup A or B”. Available files:* **BBR06: Patient BAD file information**
* **BBR15: Patient Blood Type and Antibody Screen results**

*Note: Neither file will give you the last testing date.* |  |
| **6** | Search for **Patient by HID** * Select EDIT; FIND
* Enter **HID**; Click FIND NEXT

*Note: HID can be scanned* |  |
|  |  |  |
| **7** | * Highlight selected patient data
* Right click and copy
* Paste to a WORD document
* Print data from both files, if applicable
 |  |
| **8** | Staple to Blood Request |  |
| **9** | **Close BBR06 and BBR15 after each use in order to search for next patient.**Clear WORD document after each printing. |  |
| **10** | Repeat steps 6 through 9 until Sunquest is available. |  |

|  |
| --- |
| **Removing USB drive** |
| **1** | ***To remove the encrypted drive without damage to the files, perform Dismount.*** * Restore TrueCrypt session.
* Click DISMOUNT
 |  |
| **2** | Watch the pulsing light on the USB drive change from a steady, rapid pulse to a slow pulse. |  |
| **3** | Remove the encrypted flash drive from the USB port on the computer hard drive.  |  |
| **4** | Store USB drive in the Down Time folder. |  |
| **5** | Click Exit button. |  |

**References:**

AABB Standards for Blood Banks and Transfusion Services, Current Edition

Blood Bank User Guide, Misys Laboratory