**Purpose**

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

**Method**

|  |  |
| --- | --- |
| **Step** | **Action** |
| **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:** | |
| 3 | Insert the encrypted flash drive into the USB port.  *A Microsoft Pop-up scan/fix may appear, choose “continue without scanning”* |
| 4 | A password prompt will appear. Enter password **bl00db@nk** (the O’s have replaced with zeros and the A is an “at” sign). The flash drive’s assigned letter will appear in the title, denoted here with a black circle. |
| **Step** | **Action** |
| **Access Captured Files** | |
| 5 | Open the flash drive’s assigned drive. |
| 6 | Open folder “Transfusion Services Backup A or B”. Available files:   * **BBR02: Product File List** * **BBR06: Patient BAD file information** * **BBR15: Patient Blood Type and Antibody Screen results** * **BBR22: Test Result Review**   *BBR22 will tell you if the patient had a testing performed in the last three days. Patients not tested within that window will have results in BBR06 and BBR15 but those reports will not state the last testing date.* |
| 7 | Search for **Patient by HID**   * Select EDIT; FIND * Enter **HID**; Click FIND NEXT   *Note: HID can be scanned* |
| 8 |  |
| 9 | Highlight selected patient data   * Right click and copy * Paste to a WORD document * Print data from both files, if applicable |
| 10 | Staple to Blood Request |
| 11 | **Close BBR02, BBR06, BBR15, and BBR22 after each use in order to search for next patient.** |
| **Step** | **Action** |
| **Removing USB drive** | |
| 12 | ***To remove the encrypted drive without damage to the files, eject the flash drive.***   * Right click ejection icon (denoted here with a black circle) * Click Eject Cruzer Micro |
| 13 | Watch the light on the flash drive turn off. |
| 14 | Remove the encrypted flash drive from the USB port on the computer hard drive. |
| 15 | Store USB drive in the Downtime folder. |

**References:**

Standards for Blood Banks and Transfusion Services, Current Edition. American Association of Blood Banks. AABB Press, Bethesda, MD.

Blood Bank User Guide, Misys Laboratory