**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:** | |
| 3 | Insert the encrypted flash drive into the USB port.  *A Microsoft Pop-up scan/fix may appear, choose “continue without scanning”* |
| 4 | Found New Hardware may appear on lower desktop tool bar. A box opens with “Removable Disk (:E)”. Close this pop-up |
| 5 | Select the TrueCrypt program (blue icon) on the desktop of a blue computer or under the Start menu.   * Start, All programs, TrueCrypt, TrueCrypt |
| **Step** | **Action** |
| **Prepare USB drive (continued)** | |
| 6 | Click on “Select File…” button |
| 7 | In the “Select a TrueCrypt Volume” window:   * Select “My Computer” or “My Documents” * Open “Removable Disk (E):” |
| 8 | Select BBCrypt and click “Open”. |
| **Step** | **Action** |
| **Prepare USB drive (continued)** | |
| 9 | *Note: In TrueCrypt, the volume box displays “E:\BBCrypt”.*  Click “Mount”. Notice that the USB drive now displays a pulsing light. |
| 10 | Password prompt: Enter **bl00db@nk**. (o’s are zeros, a is @ symbol). Do not check any of the boxes and click on OK.    *A pop-up may appear telling you the USB stick is corrupt, click on “no”* |
| 11 | Minimize this pop-up screen |
| **Access Captured Files** | |
| 12 | Open local disk (F): |
| **Step** | **Action** |
| **Access Captured Files (continued)** | |
| 13 | 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.* |
| 14 | Search for **Patient by HID**   * Select EDIT; FIND * Enter **HID**; Click FIND NEXT   *Note: HID can be scanned* |
| 15 |  |
| 16 | Highlight selected patient data   * Right click and copy * Paste to a WORD document * Print data from both files, if applicable |
| 17 | Staple to Blood Request |
| 18 | **Close BBR02, BBR06, BBR15, and BBR22 after each use in order to search for next patient.**  Clear WORD document after each printing. |
| 19 | Repeat steps 6 through 9 until Sunquest is available. |
| **Step** | **Action** |
| **Removing USB drive** | |
| 20 | ***To remove the encrypted drive without damage to the files, perform Dismount.***   * Restore TrueCrypt session. * Click DISMOUNT |
| 21 | Watch the pulsing light on the USB drive change from a steady, rapid pulse to a slow pulse. |
| 22 | Remove the encrypted flash drive from the USB port on the computer hard drive. |
| 23 | Store USB drive in the Downtime folder. |
| 24 | Click Exit button. |

**References:**

AABB Standards for Blood Banks and Transfusion Services, Current Edition

Blood Bank User Guide, Misys Laboratory