**Purpose:**

To provide instructions for saving patient history files using an encrypted USB drive in order to provide patient history information in the event Sunquest system is not operational.

**Method:**

|  |  |  |
| --- | --- | --- |
| **Step** | **Actions** | **Related documents** |
| **Perform Report Capture in Sunquest:** | | |
| 1 | Perform Function BEX in SmarTerm | Patient History Backup Reports in Sunquest |
| **Prepare USB drive:** | | |
| 2 | Insert the encrypted flash drive into the USB port on the hard drive.   * + Even days: “A”   + Odd days: “B”   *NOTE: Alternate using the A and the B drives each day so that if one flash drive goes missing or becomes unusable the data is still recent on the other.*  *A Microsoft Pop-up scan/fix may appear, choose “continue without scanning”* |  |
| 3 | Found New Hardware may appear on lower desktop tool bar. Box opens with “Removable Disk (:E)”. Close this pop-up. |  |
| 4 | Select the TrueCrypt program (blue icon) on the desktop of a blue computer or go to the start menu   * Start, All programs, TrueCrypt, TrueCrypt |  |
| **Step** | **Actions** | **Related documents** |
| **Prepare USB drive (continued):** | | |
| 5 | Click on “Select File…” button |  |
| 6 | In the “Select a TrueCrypt Volume” window:   * + Select “My Computer” or “My Documents”   + Select “Removable Disk (E):”, click “open” |  |
| 7 | Select BBCrypt and click “Open”. |  |
| **Step** | **Actions** | **Related documents** |
| **Prepare USB drive (continued):** | | |
| 8 | *Note: In TrueCrypt, the volume box displays “E:\BBCrypt”.*  Click “Mount”. Notice that the USB drive is 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.    *A pop-up may appear telling you the USB stick is corrupt, click on “no”* |  |
| 10 | Minimize the pop-up screen. |  |
| 11 | The F drive is the encrypted part of the E drive (like a subfolder). This drive must be used for patient information. ***If only the E drive is selected, the information will not be encrypted!*** |  |

|  |  |  |
| --- | --- | --- |
| **Step** | **Actions** | **Related documents** |
| **Capture Reports** | | |
| 1 | Open SmarTerm Roll N Scroll. Log on. |  |
| 2 | MC900432618[1]On the Menu bar, under “Tools”, choose “Start Capture”. |  |
| 3 | “Capture” options box is displayed: |  |
| 4 | Select “Local disk (F)” to identify the file destination where you want the report to be saved.  MC900432618[1] |  |
| **Step** | **Actions** | **Related documents** |
| **Capture Reports(continued)** | | |
| 5 | Select the Transfusion Service Reports folder  MC900432618[1] |  |
| 6 | Assign a file name, typically an abbreviation of the report name combined with the date compiled (i.e., BBR15\_040511.txt).   * Click “Start Capture”.   MC900432618[1]MC900432618[1] |  |
| 7 | Once complete, on the Menu bar under “Tools”, choose “Stop Capture”. |  |
| 8 | Repeat steps 2-7 until all of the following reports have been extracted:   * BBR2 * BBR6 * BBR15 * BBR22 | Patient History Backup Reports in Sunquest |
| **Cleaning Up** | | |
| 1 | Review to ensure reports have been properly saved. Delete previously saved reports. |  |

|  |  |  |
| --- | --- | --- |
| **Step** | **Actions** | **Related documents** |
| **Removing USB drive** | | |
| 1 | ***To properly remove the encrypted USB drive without damage to the files***   * 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. |  |
| 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