**Purpose:**

To provide instructions for saving patient history files using an encrypted USB drive in order that patient history information is available even when the Sunquest system is not operational.

**Method:**

|  |  |  |
| --- | --- | --- |
|  | **Actions** | **Related Documents** |
| **Perform Report Capture in Sunquest:** |
| **1** | * Perform Function BEX in SmarTerm
 | Patient History Backup Reports in Sunquest |
| **Prepare USB drive:** |
| **1** | 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.* |  |
| **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”
	+ Select “Removable Disk (E):”
	+ Click “Open”

 |  |
| **7** | Select BBCrypt and click “Open”. |  |
| **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. |  |
| **10** | * Volume for F: drive is E:\BBCrypt.
* Diminish the pop-up.

 |  |
| **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!*** |  |
| **Capture BEX Reports** |
| **1** | Open the SmarTerm Roll N Scroll area of MISYS. Log on. |  |
| **2** | MC900432618[1]On the Menu bar, under “Tools”, choose “Start Capture”. |  |
| **3** | “Capture” options box is displayed: |  |
| **4** | Select “Removable disk (F:)” to identify the file destination where you want the report to be saved. MC900432618[1] |  |
| **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 pulled (i.e., BBR15\_04052011.txt). This will allow you to easily check the date.
* Click “Start Capture”.

MC900432618[1]MC900432618[1] |  |
| **7** | * Perform extract from SmarTerm
 | Patient History Backup Reports in Sunquest |
| **Cleaning Up**  |
| **1** | Delete the 2 day old files from the USB drive. The files are all additive so there isn’t a need to keep multiple days’ worth.  |  |

|  |
| --- |
| **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