To: Faculty and Staff (VCU School of Medicine Computers Only)

On July 31, 2013, SOMTech completed the mandated VCU Security Standard for Encryption Policy that required all laptops to be encrypted. To further enhance the protection of sensitive data and PHI (Protected Health Information) data, the SOM will be requiring encryption on all external devices by implementing Dell’s Data Protection Encryption External Media Edition (formerly known as Credant External Media Shield) on December 9, 2013. Dell External Media Edition will ensure that all USB devices used to access and store data within our environment will be encrypted. The Dell encryption solution protects VCU, SOM, and departmental data from potential breaches should a device become lost or stolen. To ensure interoperability between the SOM and VCUHS, SOMTech will be working with VCUHS to ensure our encrypted USB devices are deemed acceptable for use on VCUHS computers.

By utilizing Dell’s Data Protection Encryption External Media Edition software, any USB flash device can be encrypted. Flash devices are relatively inexpensive and will need to be purchased by your department, division or unit to replace any unencrypted personal flash devices. The flash devices can be purchased by any of our eVA vendors. Visit the SOMTech Purchasing website for more recommendations.

On December 9, 2013, a notification box will appear on your computer asking you to encrypt or not encrypt when inserting a non-encrypted USB device into a SOM supported computer. You must choose encrypt in order to fully use and store files on the device. If you choose to “not encrypt” the device, the data on the USB device will be “read only” - you will be unable to copy new files or make changes to the existing files on the USB device. Once the USB device is encrypted, AccessEncryptedFiles.exe will be installed on the USB device for you to use in order to access encrypted data on computers offsite.

To access encrypted data offsite, two options will be available (EMS Service and EMS Explorer).

**Option 1:** If you have administrative rights on the offsite computer (e.g. Home computers), you should install the **EMS Service**. You only need to install the **EMS Service** on the computer once to allow you to make changes to files stored on the encrypted USB device while offsite by entering the required password.

**Option 2:** If you are off-site and unable to install the EMS Service on the computer (e.g. frequent guest presenter that use computers at other institutions or airport kiosk computers), you can access files by running **EMS Explorer**. Unlike the EMS Service, you can’t use Windows Explorer to access or copy files using this option. **EMS Explorer only allows you to add (by dragging and dropping) files and access existing files via the EMS Explorer Window.** If you fall into this category and would like to have the ability to easily make changes and save files while traveling, please fill out the IronKey User Agreement Form to receive an IronKey USB encrypted device.

For more detailed information please visit the [SOMTech Alerts](http://www.somtechalerts.com) webpage. The website will also list the dates and times for open forum sessions where faculty and staff can come for demonstrations, ask questions and receive answers.