Data Protection

About

This page describes the requirements and best practices in place within SOM to protect data. While most security policies and standards are applied to systems, the ultimate goal of these is to protect data within the environment. This may be student data, research data, demographic and administrative data, and so much more. There are certain legal requirements and ethical concerns that must be considered when looking at options for protecting this data. In general, SOMTech leads toward protecting managed devices and data as if it is category 1 data. The goal of this page is to describe how SOMTech protects the data and to help SOM faculty, staff, and students protect data they are using while still being productive.

Consultation Requests

If you are interested in meeting with SOMTech to discuss ways that you can effectively work while still following VCU, VCU Health, and SOMTech security and privacy standards (among others), please submit a ticket requesting a meeting.

Encryption

One of the easiest ways to verifiably protect data is for it to be encrypted. VCU has an encryption standard which outlines when and how data should be encrypted. While this is not exhaustive (please read the standard), the primary times that data must be encrypted is as follows:

- Laptops (all laptops must be encrypted with a managed encryption solution)
- Category 1 data not stored on centrally secured and approved storage (e.g. VCU Health OneDrive, SOM T:\ and U:\ drives, and VCU Health H:\ and S:\ drives)
- Category 1 and 2 data transferred over untrusted networks
- Category 1 data being emailed and transferred over any network

External Media Encryption

Over the years, SOMTech has enforced encryption on flash drives primarily using 2 different solutions (IronKey drives and DDPE). In 2021, these solutions are being phased out in favor of VCU Health's OneDrive cloud storage and BitLocker EME. More details are below, but if you have any questions or concerns, please submit a ticket to SOMTech.

BitLocker To Go External Media Encryption

BitLocker To Go external media encryption is the new standard for encrypting external storage devices within the School of Medicine. Any external storage drives that you will need to transfer data to from a SOM Windows computer will be required to be encrypted. If you do not encrypt the drive, you will still be able to copy data off. You can read more info on this process at the link **here**. If you have further questions or you have an external drive that will need to remain unencrypted feel free to submit a ticket for assistance.

SOMTech started deploying BitLocker To Go on some new SOMTech-managed Windows computer in the spring of 2021 and will expand the deployment On August 3rd, 2021. SOMTech has created an FAQ to answer common questions and provide a little more details about BitLocker To Go.

Be advised that BitLocker Encryption is not Mac compatible so there will be no way of using these encrypted drives on a Mac device at this time. If you plan on working on Windows & Mac devices it is recommended you use your Home Drive, VCU Health OneDrive, or VCU Google Drive accounts to transfer data.

DDPE External Media Encryption

SOMTech is phasing out the use of Dell Data Protection in 2021. With that being said it is recommended that you start making preparations for this change while we look to move to a new form of data protection. VCU Health's implementation of OneDrive is a cloud based file storage alternative to encrypted physical drives however if you do need to use a physical drive for data storage and we have you on record of having a encrypted drive in your possession then you can expect communication from us soon on how to proceed.

IronKey Drives (Deprecated)

SOMTech and VCU Health provided hardware-encrypted IronKey devices for many years. These devices required a password every time they were used, but worked on both VCU and VCU Health computers. They were also able to be used on any computer without administrative rights. If the password was forgotten, SOMTech could reset the password administratively (on SOMTech-managed drives). VCU Health used unmanaged IronKey drives which meant that they weren't able to help with forgotten passwords. They stopped providing IronKey drives in 2019.

IronKey Drives Phase-out Plan

As of March 10, 2021, SOMTech will no longer be supporting the IronKey drives. After this date, SOMTech will **not** be able to help you reset your password if you forget it. This means that your data will be unrecoverable if you forget your password. The drives also have a self-destruct security feature after entering your password incorrectly 10 times.

SOMTech and VCU Health recommend that you use the VCU Health instance of Microsoft OneDrive in replacement of the IronKey drives. OneDrive is a secure location where HIPAA data can be stored and accessed from any computer or device connected to the internet. Google Drive is also a reasonable alternative, but functionality is limited and there is not as much integration with email and other Microsoft Office tools.

In order to protect any data on IronKey drives, we are strongly encouraging that everyone who has an IronKey drive to please follow these steps:

1. Copy all data off of your IronKey drive
    a. If you have forgotten how to use your IronKey drive or have forgotten your password, please submit a ticket to SOMTech. **Do not attempt to login more than a few times as the drive will self-destruct after 10 incorrect attempts.**
2. Physically send your IronKey to SOMTech so that they can be removed rom the environment. Please do **not** include the password.
    a. Campus mail: Send to SOMTech, Box 980565
    b. Drop off: Drop off in the bin outside of the SOMTech Client Services office in Sanger Hall, B1-039 (near the rest rooms)