Device Security

The risks of identity theft, compromised account access, and the potential for lost data requires a particular focus for healthcare organizations such as the OU Health Sciences Center. The protection of our employee, student, and patient information is our primary focus. The OUHSC recognizes this responsibility and is taking the initiative to provide you, our patients, and all HSC community members with a comprehensive approach to security practices and technologies.

In order to protect your devices and meet the obligations and policy requirements of a professional in the healthcare environment, all student personal devices used for University business (which includes email or webmail) are required to complete a Device Security Clinic and use the OUHSC computer security suite. This software is free for your use while you are a student here and will provide your personal devices with up-to-date data encryption, anti-virus capabilities, and other security tools needed to protect your devices and the data they may contain.

In addition to ensuring the safety of your own personal data, these steps also comply with federal regulation that requires any device accessing or creating protected health information be encrypted to ensure the safety of our patients’ data.

Accessing HSC Resources Requires a Secure Computer

What does this mean for me?
First and foremost, this means that your device will be as protected as possible from threats and data loss. The patches and antivirus software will aid in preventing cyberattacks and the data encryption software will aid in preventing data loss and identity theft in the event your device is lost or stolen.

What are we doing to your computer?
The OUHSC computer security suite will be installed and configured during the Device Security Clinic. This suite of tools includes several technical components:

- **Advance Threat Protection (ATP)** - Lightweight anti-virus that prevents 99% of malware using artificial intelligence and machine learning to identify malware before it can execute. ATP provides real-time scanning that prevents advanced threats that traditional anti-virus cannot prevent.

- **Dell Device Protection (DDP) encryption** — DDP encryption enables already-existing features of your operating system (BitLocker in Microsoft Windows OS, FileVault in macOS). This makes data on both internal computer storage and removable storage unreadable without the encryption password.

If you require direct access to OUHSC Business Systems from your personal device (to access a list of designated business systems, see back of pamphlet), two additional technologies will be installed and configured on your computer:

- **PulseSecure VPN client** – The VPN client allows users with the appropriate roles to have access to designated systems. It additionally reviews and reports the status of the other technologies applied during the device security clinic.
HSCACCESS wireless network — The HSCACCESS wireless network is not a new technology, but a hidden wireless configuration that requires the addition of your specific hardware ID (technically, a MAC address) to the list of permitted devices.

During the Device Security Clinic, we must perform a few system tasks. This includes changing your computer device name to a standard format, ensuring that your computer is up-to-date with the latest supported operating system (Windows 10 Education edition, macOS 10.13 "High Sierra" or higher), and install security patches and updates.

How long will this take?
The time required to install, configure, and fully encrypt a device is highly variable. It depends on several factors such as device age, the status of existing upgrades and security patches, and storage size. The goal of the Device Security Clinic is to return your device to you at the end of the same business day that you leave it with the IT Service Desk. However, some devices could take 2-3 business days to fully complete. There are a limited number of laptops available for loan from the Bird Library staff.

What should I expect when this is done?
When the Device Security Clinic is completed on your device, you will be contacted and may pick up your computer from the IT Service Desk. Some of the new features and functions you should be aware of include:

- Your device will now have a designated administrator account which will require a password that you must change to something unique when you pick up your device.
  - You must set and remember this password to successfully validate yourself with the encryption software and login to your computer.
- Your computer will have anti-virus set up to run and update in the background with no intervention on your part. The system should identify and clean any virus or malware that it finds.
  - If you see this is happening frequently, please contact the IT Service Desk for further evaluation.
- Any external storage device (USB drive, flash drive, thumb drive, CD, DVD, SD card) that you attempt to insert via a USB port on your computer will now require your intervention to work. The encryption system will ask if you would like to encrypt the drive inserted into your computer:
  - If you say “Yes,” it will be encrypted and you will be able to read & write data to this device.
  - If you say “No,” the drive will not be encrypted, but it will be read-only and no data may be copied to that device. However, data can be copied off the storage device and onto your computer.

Privacy
In order to successfully install, configure, and implement the security tools in the Device Security Clinic, IT Service Desk staff will need to collect your device administrator password (if you have one) and your HSC account credentials in order to make system level changes and configurations to the security tools. Each of these will be reset and require you to select a new device password and account password when the clinic is complete.

During the time we have your computer, the IT Service Desk will not access any of the personal data you have on the device. Their job is to install all of the latest system patches/updates, antivirus, and data encryption software. After the clinic is complete, the security software being installed on your computer does not track, view, allow access to, or otherwise enable either Information Technology or other university officials to access the data on your computer.

For a list of designated OUHSC Business Systems for your personal device, search “OUHSC Business Systems” at help.ouhsc.edu

Additional frequently-asked questions are updated regularly at https://outservices.service-now.com/kb_view.do?sysparm_article=KB0011230

You may get help, check the status of your requests, or search the knowledgebase on the HSC IT Service Portal at outservices.ouhsc.edu.