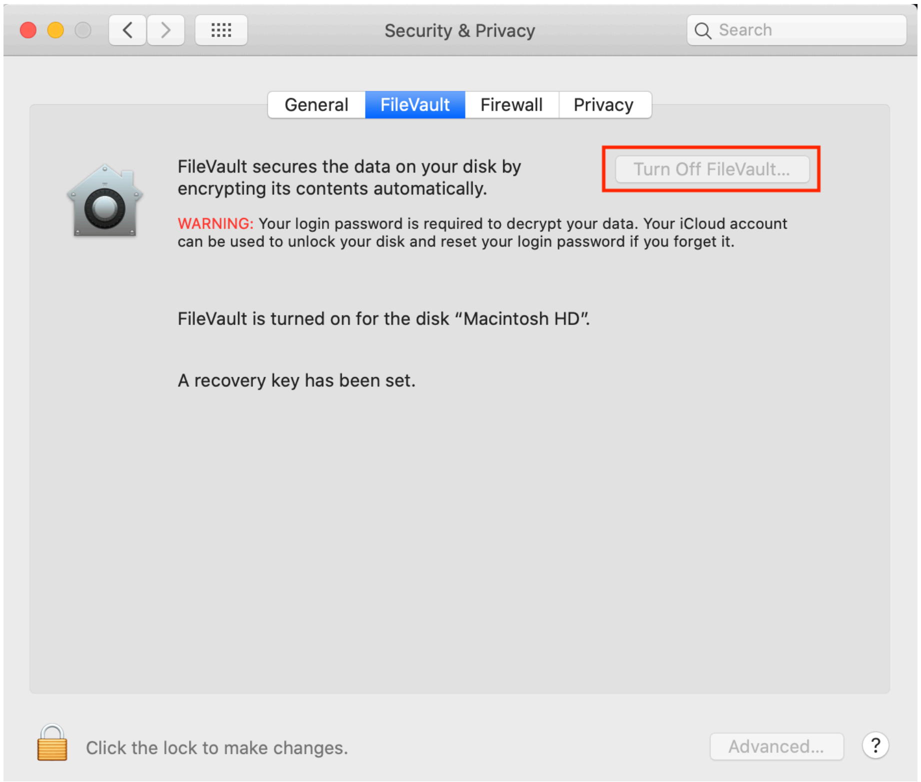
TECH SECURITY

The purpose of this document is to provide a guide for improving security of personal devices. This guide currently only supports devices within Apple Ecosystem. Encryption and security of devices is critically important in the event of loss of a personal device. Whether it is stolen or mistakenly lost and unable to be recovered, an unsecured device risks loss of data to unauthorized entities. You would be surprised the amount of data stored on your computer or phone that you didn't know was there. All your saved logins, email attachments in temporary folders, credit card information, work related data, cookies from your browsing, etc.... the list goes on and on.

How to encrypt your MacOS personal computer:

1. Make sure your computer password is distinct from any other password you use at your institution. and equally as robust.
2. Click the Apple symbol () in the upper left hand computer.
3. Go to "System Preferences"
4. Click "Security & Privacy"
5. Click "Turn On FileVault" (perform this overnight, as it may take some time)



FileVault secures the data on your disk by encrypting its contents automatically.

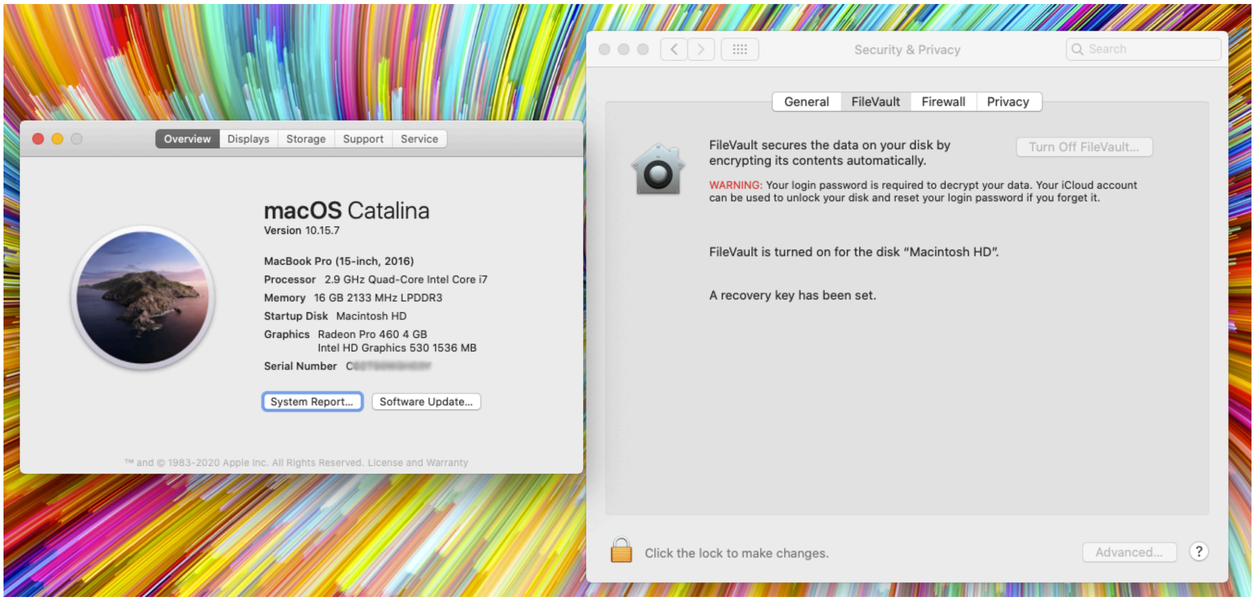
WARNING: Your login password is required to decrypt your data. Your iCloud account can be used to unlock your disk and reset your login password if you forget it.

FileVault is turned on for the disk "Macintosh HD".

A recovery key has been set.

Click the lock to make changes.

6. You can set a recovery key in your iCloud. This should have a password distinct from other passwords and be as robust, with a variety of alphanumeric symbols.
7. Now as proof of encryption, click the Apple symbol () in the upper left hand corner, click the “About This Mac”. Next place the “Security & Privacy” window next to the information window. Take a screen shot (command, shift, option 4) and crop the screen area utilizing the target symbol and your cursor.



macOS Catalina
Version 10.15.7

MacBook Pro (15-inch, 2016)
Processor 2.9 GHz Quad-Core Intel Core i7
Memory 16 GB 2133 MHz LPDDR3
Startup Disk Macintosh HD
Graphics Radeon Pro 460 4 GB
Intel HD Graphics 530 1536 MB
Serial Number C[redacted]

™ and © 1983-2020 Apple Inc. All Rights Reserved. License and Warranty

FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: Your login password is required to decrypt your data. Your iCloud account can be used to unlock your disk and reset your login password if you forget it.

FileVault is turned on for the disk “Macintosh HD”.

A recovery key has been set.

Click the lock to make changes.

8. Open Preview app. Press command+n. Save this and back it up online, preferably in a secured email. In the event of data breach, this can be used as proof any PHI that may be on the personal computer is secure.
9. You should also enable FileVault for any usb backup drives or usb peripheral drives.

Enable firmware password on your Apple computer:

1. Enabling a firmware password on your computer will prevent users from being able to boot your computer from an external drive, unless they know the firmware password. It may seem like overkill, but this is the final step to complete data protection
2. Follow this link to the Apple website for a detailed guide: https://support.apple.com/en-us/HT204455

How to encrypt your iPhone:

1. Requiring a passcode to open your iPhone now automatically encrypts your iPhone. If you chose to use native Northwell Health® email on your iPhone, you will be required to enter an alphanumeric passcode which will further enhance security.

How to further secure your iPhone:

2. Open “Settings”
3. Open “Face ID & Passcode”
4. Enable Erase Data after 10 failed attempts. This will further protect possible breach of PHI.