Minimum Security and Network Requirements Guideline

ICHA | Inner City Health Associates

Purpose

This reference is for the use of any agency partnerships intending on accessing ICHA's Electronic Medical Record (EMR) system. The minimum security and network requirements outlined in this guide are for the purpose of securing and maintaining the integrity of the Personal Health Information (PHI) contained in ICHA's EMR.

Overview

ICHA's EMR is hosted within St. Michael's Hospital's data centre. Encrypted access is provided using an SSL certificate signed by means of a SHA-256 signature algorithm with RSA encryption that is compatible with any modern browser. Although connection to ICHA's EMR and other eHealth applications containing PHI is secure, often times PHI can be stored locally on devices in Temporary Internet Files or the Downloads folder. These guidelines are to safeguard this PHI when it is being stored locally.

SSL Certificate *– Secure Sockets Layer (SSL) is a widely-recognized security technology for ensuring an encrypted link between a web server and a browser. This link ensures that vulnerable information passed between the web server and browsers remains confidential.*

SHA-256 Signature Algorithm *– A critical element in the security of a certificate, a generated almost-unique cryptograph hash or "signature" is assigned to text. SHA-256 is one of the strongest hash functions available.*

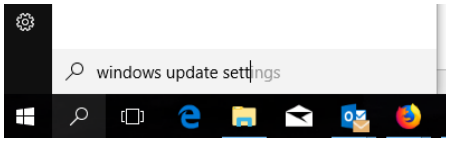
RSA Encryption *– RSA (Rivest–Shamir–Adleman) is an algorithm used in modern cybersecurity to encrypt and decrypt messages.*

Software Patch and Browser Updates

All workstations that connect to ICHA's EMR must be protected from malicious threats. To support this, ensure all systems are running the current version of the internet browser (Mozilla Firefox) and Operating System (OS) software. Security patches are often made available each update and should be applied in a timely manner according to the risk they mitigate.

Windows Recommendations

1. Open *Windows Update Settings*
    - Using Windows 10 you're able to find this using the search bar in the bottom left corner.
2. Select *Check for Updates* and/or ensure automatic updates has been activated.



MacOS Recommendations

1. Open *Apple Menu > System Preferences > Software Updates*
2. Select *Automatically keep my Mac up to date* to automatically install updates.

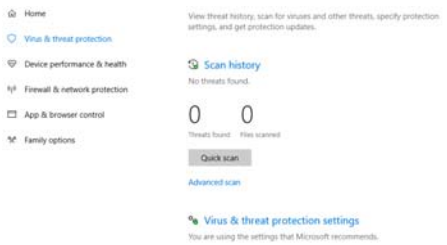
Anti-Malware Software

Malware, short for "malicious software" is software that is intentionally designed to disrupt, damage, or gain unauthorized access to a computer system. Most devices come equipped with an anti-malware software that can be enabled, or a third party anti-malware software can be purchased and installed. All workstations/devices connecting to ICHA's EMR must be equipped with Anti-Malware Software with the following conditions:

- Software must be running and up-to-date
- Real time scanning must be enable and/or scheduled to scan the device on a regular basis

Windows Recommendations

1. Open *Windows Defender Security Centre*
    - Using Windows 10 you're able to find this using the search bar in the bottom left corner.
2. Click *Virus & threat protections* on left menu > *Quick Scan*.
3. Select *Virus & threat protections settings* > Turn *Real-time protection* ON



MacOS Recommendations

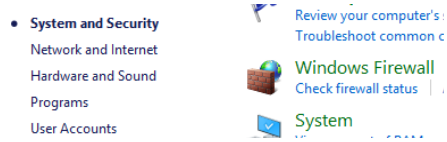
1. Open *Apple Menu > System Preferences > Software Updates*
2. Select *Automatically keep my Mac up to date* to automatically install updates.

Firewall

To further protect devices and ICHA's EMR, it is recommended to have a host enabled firewall active on each device. A firewall is the first line of defense against malicious attacks and acts as a barrier between trusted and untrusted networks. Most devices come equipped with a firewall software that can be enabled, or a third party firewall software can be purchased and installed.

Windows Recommendations

1. Open *Control Panel*
    - Using Windows 10 you're able to find this using the search bar in the bottom left corner.
2. Select *System and Security* and then *Windows Firewall.* Ensure firewall is enabled.



MacOS Recommendations

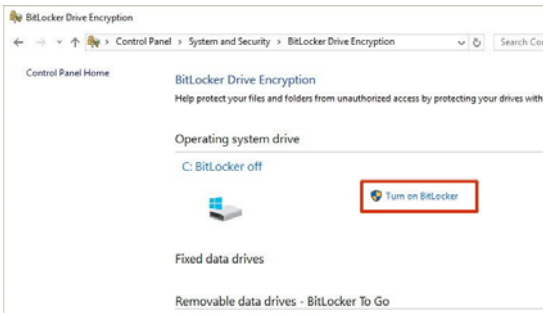
1. Open *Apple Menu > System Preferences*
2. Click *Turn On Firewall*

Encryption

ICHA EMR users may download PHI to their computers from time to time. This data can be collected and stored in a browser's Temporary Internet files or in a Downloads folder. In order to protect this downloaded data, all temporary files should be encrypted with a strong password.

Encrypting data stored on a hard drive uses mathematical functions to prevent unpermitted viewers from accessing the stored information without the proper password of security key. Valid options for encrypting workstations that access ICHA's EMR include Container or Volume Encryption, File or Folder Encryption or Full Disk Encryption.

Windows Recommendations



1. Open *Control Panel*
    - Using Windows 10 you're able to find this using the search bar in the bottom left corner.
2. Select *System and Security* and then *BitLocker Drive Encryption.* Click *Turn on Bitlocker* and follow steps.
3. Enter a password using a mix of upper/lower case, numbers and symbols.

MacOS Recommendations

1. Open *Apple Menu > System Preferences*
2. Select *Privacy & Security > File Vault* tab
3. Click on the lock in the bottom left corner of the window
4. Enter your administrator name/password > *Unlock > Turn On File Vault*

Minimum Security and Network Requirements Guideline

ICHA | Inner City Health Associates

Password Authentication and Policy

Complex and sophisticated passwords are required for all devices accessing ICHA's EMR. Devices will also need to be shutdown, locked and logged off before the device is left unattended or users switch. Auto-logout settings should be updated on devices to show log off screen after 5 minutes of inactivity. This can typically be done in the Screen Saver and Personalization settings of a device.

Requirements for Complex Passwords

- At least 8 characters in length
- Not based on dictionary/common words
- Contain a mix of upper and lower case letters
- Contain a mix of numbers and special characters (!?$<> etc.)

Network Configuration

A partnership with ICHA's Clinical Services requires dependable internet access. Using ICHA's EMR, physicians and allied staff will need secure, reliable internet either via direct data line or dedicated Wi-Fi to connect with ICHA's browser-based EMR.

In terms of performing bare minimum functionality, internet speed will need to meet 20mbps down – 10mbps up.

Wi-Fi configuration will need to have an SSID devoted to ICHA programming (i.e "ICHA Clinic"). It cannot be publically broadcasted and will require WPA Encryption with a long password that is changed quarterly.

Routers will need to have a complex administrator password updated from the original "out of the box" password. Updates will need to be configured on an annual basis. Recommended brands include; DLink, Netgear, Cisco and Asus.