Mission Neighborhood Health Center
240 Shotwell Street San Francisco, CA 94110 - Phone: (415) 552-1013 - Fax: (415) 431-3178
info@mnhc.org - www.mnhc.org

POLICY AND PROCEDURE

Policy Name: Virtual Private Network (VPN) and Remote Access
Original Date: August 1, 2012 Revision Date: September 15, 2014, April 19, 2018, July 15, 2019, January 29, 2024
Department(s)/Site(s):
Document Owner: Chief Operating Officer
Approved By: Chief Executive Officer/Executive Director
Relevant Law / Standard:

Purpose:

The purpose of the VPN and Remote Access policy is to ensure the integrity of and protect the MNHC computer network system and patient health information (PHI) from potential data loss.

An application process is required for employees who use MNHC-owned laptops to access the network remotely.

The following classifications of employees at MNHC are allowed VPN and remote access after review by IT department and approval by the Executive Director:

1. Medical providers providing after hours coverage on evening, weekends, and holidays,
2. Executive management,
3. Other approved staff, based on health center needs.

Policy:

It is the policy of MNHC to require an application to the IT Department and approval of the Executive Director before the VPN installation onto an MNHC-owned laptop assigned to a staff person.

Only medical providers providing after hours coverage on evenings, weekends and holidays, executive management and other approved staff, are eligible for VPN and remote access.

Medical providers providing after hours coverage will use an MNHC provided laptop for purposes of accessing systems via VPN or remote EHR.

Laptops will have secure, encrypted VPN and EHR access. EHR is only accessible via VPN, and MFA is required to comply with HIPAA regulations and as a protection for MNHC electronic patient health information (ePHI).

Procedures:

- Eligible staff must complete the relevant application attached to this policy.

- MNHC's IT vendor/department is not responsible for support of employees' personal computers and home networking, equipment, including but not limited to router, switches and broadband devices.

  MNHC employees with VPN privileges are responsible to ensure no unauthorized users access the MNHC network or applications.

- MNHC provided laptops are for business and after-hours medical provider coverage use only. No personal software is to be installed on MNHC supplied computers. Unauthorized access by non-MNHC users is prohibited.

- Users will receive a web link and instructions on how to access the VPN via web browser. This does not require the installation of any software on the computer. If needed, VPN software can be installed on the computer by MNHC's IT department. If you need the VPN program installed on your computer or need assistance or have questions regarding installing the programs, contact DAS Health to schedule a time to receive help.

- In the event of your laptop/tablet being stolen, lost or misplaced, it is mandatory that you **immediately** report the occurrence to Itelagen's support phone line or email address in order to turn off the existing VPN and prevent MNHC data from being compromised. The loss must also be reported to the Executive Assistant to the Chief Executive Officer at x2225.

- As with all MNHC equipment and services, network and server updates are required. Users might need to log off or disconnect from their VPN session if they receive a message (pop-up) from the network administrator informing them that maintenance is taking place. Please log off accordingly; users who are not compliant will be disconnected 15 minutes after the message is sent and MNHC will not be responsible for data loss on projects that were not saved on time.

- All VPN and network passwords are to be kept confidential. Under no circumstances should a user password be shared with others or saved on the same computer that has the VPN installed on it.

- VPN connections will be automatically disconnected after 30 minutes of inactivity; save your work periodically to prevent data loss.

- All requests for VPN and Remote Access to the MNHC network must be reviewed by the IT Department or vendor and approved by the Chief Executive Officer. IT Support Specialists on an annual basis will audit who has access to VPN and delete inactive users.

ATTACHMENT A

Hardware Laptop Agreement- Access to Medical Records

- MNHC provided laptops are for business use only.
- Saving and storing PHI are prohibited.
- No personal data may be saved on the company provided laptop.
- No unauthorized installation of software or hardware.
- MNHC laptops are for use by employees only. Unauthorized access by individuals other than MNHC staff is prohibited.
- MNHC staff must not leave screens unattended while connected to the VPN.
- MNHC laptops must be securely in the possession of the provider and cannot be left in cars.
- Lost or stolen laptops must be reported immediately to DAS Health and the Executive Assistant to the CEO x2225. DAS Health contact information: support@dasmsp.com; (415) 813-774-9800 x4

All MNHC laptop users must read this policy and sign the below acknowledgement.

I, _____, have received and read MNHC VPN and remote access policies on_____ and agree to abide by the policies as noted.

_____ _____
Printed Name and Signature Date

_____ _____
Reviewed by IT Department/Vendor Date

_____
– Anna Robert, RN, MSN, DrPH - Chief Executive Officer
Date

Signed copy will to go to HR personnel file

ATTACHMENT B

MNHC Staff and Contracted Individuals VPN and Remote Access to EHR

MNHC systems are for business use only.

MNHC systems are for use by MNHC employees and contracted staff only. Unauthorized access is prohibited.

Saving and storing PHI on the local equipment are prohibited.

No personal data may be saved on the company systems.

MNHC staff must not leave screens unattended while connected to the VPN.

EHR is only accessible via VPN and MFA is required to comply with HIPAA regulations and as a protection for MNHC electronic patient health information (ePHI)

All off-site users must read this policy and sign the below acknowledgement.

I, _____, have received and read MNHC VPN

and remote access policies on _____and agree to abide by the policies as noted.

_____ _____
Printed Name and Signature Date

_____ _____
Reviewed by IT Department/Vendor Date

_____
- Anna Robert, RN, MSN, DrPH Chief Executive Officer
Date

Signed copy will to go to HR personnel file