Policy: Wireless Networking and Remote Access

Policy Details

Creation date:_____ Revision date: _____
Applies to: All employees and contractors
Approved by: _____

Purpose

To ensure that the risks of transmitting personal and health information are mitigated and that the information is accessible to authorized individuals for authorized purposes. This policy intends to include enough technical detail so that the clinic manager can discuss the recovery procedure with the IT professional who will implement it.

Clinic policies regarding wireless networking and information handling and security apply at the clinic and anywhere else the authorized clinic devices are used (E.g., home office, telework). These alternate work locations should be discussed with and approved by the system administrator before clinic devices are used.

This policy addresses common security considerations of both wireless and remote access.

Administrative Safeguards

The clinics shall make reasonable efforts to protect against human error or malicious acts.

The clinic's administrative safeguards related to remote access and networking are:

- Complete an inventory of all authorized wireless devices and update the documentation when necessary (recommendation: when devices are on-boarded and off-boarded and annually at minimum). This inventory should include all wireless devices, other hardware and peripherals connected to the network.
- Routinely check for rogue and unauthorized devices (system management).
- The System Administrator will periodically (at least once monthly) monitor any connectivity issues to ensure the integrity of the wireless network.
- Review and update all security and access policies, including Wireless Policies, quarterly to recognize that this technology and its inherent risks change quickly. Provide updates and training to wireless users as required.
- Remote access to the electronic medical record (EMR) outside of the clinic will be granted on a case-by-case or need-to-know basis.

Physical Safeguards

The clinic shall make reasonable efforts to protect against the risk of theft, water and humidity, fire, vandalism, and other external threats.

The clinics' physical safeguards related to remote access and networking are:

- The internet router is securely maintained in a restricted location in the clinic and is attached to a fixed object (i.e., wall) or maintained in a secure shelving unit.
- Uninterrupted Power Supply (UPS) for a router if business continuity and workflow is dependent on wireless connectivity.
- Access Points (AP) are located central to the building to reduce the strength of the signal leaving the building where possible to provide optimal strength to the equipment used in the building. (May need to consider reorganizing desk and equipment orientation in rooms to maximize signal strength.)

Technical Safeguards

The clinic shall make reasonable efforts to protect against network risks.

The clinics' technical safeguards related to remote access and networking are

Router

- Firewall has been installed, configured and tested.
- Passwords to the router have been changed from the default settings.
- Wireless access is password-protected using a minimum of 20 characters or greater alphanumeric passphrase not based on dictionary words.
- Scheduled scanning for rogue devices and updates for the wireless network devices is performed and drivers on the wireless devices are periodically updated.
- Disable Simple Network Management Protocol (SNMP).

Wireless access points are secure

- Wi-Fi Protected Access (known as WPA2) is implemented on the AP and wireless devices.
- Change the static Internet Protocol (IP) address on the AP from the default to a different number. Set a static IP address on the wireless clients so that they share the same numbers for the first three octets as the IP address just assigned to the access point, such as 192.168.47.x.
- Turn off administration over wireless (assuming you have at least one computer connected to the wireless access point using a network cable).

Other safeguards

- The System Administrator will lock the authorized client device (laptop) to only connect to predefined SSID's and device addresses.
- Enable the built-in windows firewall on the laptop. Each computer in the network has antivirus protection that is updated automatically and enable automatic updates from Windows and Microsoft office.
- Laptops and mobile devices (PDA's, memory sticks, etc.) require layered security protection. Clinic staff using laptops will be provided specific training on mobile computing to ensure that they understand the physical, administrative, and technical safeguards implemented. These include:
    - Ensure that the Administrator account has been renamed and given a strong password.

    - Never leave your laptop unattended, particularly overnight. Lock it in a desk drawer or cupboard.
    - Select laptops that have hard drive passwords and use these protection measures. Passwords on the hard drive boot are more secure than operating system user passwords.
    - Do not store personal or health information on mobile computing devices unless you need to. This must be limited to what is necessary, and the data may only be stored for as long as necessary to complete a task. Data must be permanently deleted from all computing devices such as tablets, phones, etc., once it is no longer required.
    - Data on the hard drive is encrypted as is data on all other mobile devices. Data encryption capability cannot be disabled by the user.
    - Access to physicians' EMR will be provided using the practice-owned computers.
- Ensure the laptop's network connection defaults are set to disable automatic roaming.
    - Mobile devices, including cellphones and memory devices, must each have, at minimum, unique password settings and, where possible, data encryption enabled.
- Wherever possible, an Internet connection will be gained using a wired network connection.
- When using wireless connections outside of the clinic is unavoidable, ensure it is a secure connection and not a public connection.
- Physicians, authorized clinic employees and vendors may be granted access to a wireless network and/or remote access to the clinic local install EMR. Access from outside of the primary site requires two-factor authentication (FOB and password) and a VPN tunnel.
    - Authorized wireless network and remote access users acknowledge that the clinic's policies and procedures (including wireless networking) and the clinic's security requirements also apply to the remote access sites (i.e., home offices).
    - When using remote access to the clinic's EMR, the user will access the Internet tools on the web browser to:
        - Delete history
        - Clear temporary files
        - Clear the cache in virtual memory
        - Clear cookies
        - Close the Internet browser

Questions?

If you have any questions about this policy, please contact the Clinic's Privacy Officer, _____.