HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

WIRELESS NETWORK BEST PRACTICES GUIDE FOR CLINICS

Summary

With personal health information being a high value target of cyber crime, it is important to ensure that the wireless network (Wi-Fi) of your clinic is appropriately configured to protect patient information. This guide describes best practices and helps clinics or their supporting local IT provider to configure wireless network and adhere to provincial privacy standards. These suggestions will generally also result in better network performance within the clinic.

> ***NOTE:***
>
> Clinics on the **Private Physicians Network (PPN)** may have additional considerations beyond the best practices suggested below. See the *Resources* section at the end of this guide for more information.

Wireless Network Security and Performance Best Practices

1. Hire a professional IT support provider.

a. A professional IT support provider should have experience with network equipment and standards in setting up wireless networks preferably in clinical setting. Ask for related certifications.

2. Use business-class equipment.

a. Devices like network switches and wireless routers should not be similar to what is used at homes but business-class for both security and performance reasons.

3. Use the appropriate network band setting for what you need. (5GHz vs 2.4GHz)

a. The 2.4 GHz band provides greater physical coverage but transmits data at slower speeds and may have congestion from other nearby networks and active network devices.

b. The 5 GHz band provides lesser physical coverage but transmits data at faster speeds. The range is shorter in the 5 GHz band because higher frequencies cannot penetrate solid objects, such as walls and floors.

4. **Disguise the wireless network name (Service Set Identifier or SSID).**

   a. The names of wireless networks are visible to the public and other nearby individuals can see them on their devices. Choose a name for your clinic wireless network that does not indicate to outsiders that the network belongs to a clinic.

   b. Having a custom network name immediately signals that your network has been configured and is less vulnerable.

5. **Change the default Administrator Account username and password after initial setup.**

   a. Using default account settings on wireless devices such as router may pose a security risk. Use personal username and strong unique password for the administrator account.

6. **Do not use remote administration or Wi-Fi administration for your network device.**

   a. There is no need to "administer" your Wi-Fi using a wireless computer; especially if you have at least one computer connected using a network cable.

   b. Only use remote administration if you and your IT support staff identify it as necessary.

7. **Use appropriate wireless encryption protocol settings.**

   a. Set the wireless encryption protocol setting to Wi-Fi Protected Access II (WPA2) or better. This setting includes the Advanced Encryption Protocol (AES) standard.

8. **Disable Wi-Fi Protected Setup (WPS).**

   a. The Wi-Fi Protected Setup setting may be turned on by default in the router. Disable this feature.

9. **Use caution with Guest Accounts on the wireless network.**

   a. Only use “Guest Accounts” for peripheral wireless appliances such as wireless speakers.

10. **Public access Wi-Fi) must be separate from the clinic network.**

    a. Some clinics decide to provide access to wireless network (Wi-Fi) to patients. This public access should be managed entirely on a separate network reserved for non-business use only.

    b. The insufficient protection and unknown software installed on public devices can pose security risk and consume network resources.

11. Ensure local firewall is enabled.

a. If available, use a hardware or software firewall to protect your local networks on the workstations (Windows Firewall) and on any network equipment like the router.

12. Keep network device firmware up to date.

a. Ensure network devices like the router are scheduled to have their firmware versions regularly checked and updated as needed.

b. Keeping firmware up to date on network devices ensures that newly discovered vulnerabilities are secured.

13. Monitor the wireless network for suspicious devices

a. Wireless access points such as routers may allow the ability to see all of the connections on your wireless network.

b. Use this ability to monitor for unauthorized devices that may have gained a connection to your wireless network.

14. Disable the Wi-Fi Sense feature on Windows 10 workstations.

a. The Windows Wi-Fi Sense feature allows you and your "friends" to share Wi-Fi connections without knowing each other's passwords. Windows identifies "friends" as anyone in your Outlook or Skype contacts, or optionally, your Facebook contacts.

b. This type of automatic access sharing is not appropriate for the business-use network at a clinic and should be disabled.

15. Ensure wireless router and other network access points are properly placed.

a. Physical access to the network ports or devices should be restricted to clinic staff only.

b. Consult with your IT support provider for other technical considerations when setting up these devices or access points to provide the best coverage while preserving security

Resources

IT Support Selection Checklist for Clinics	Guidance to physicians on specific questions to ask your local IT support. This is a great conversation starter and provides tips on what questions to ask your local IT.
Physician Office IT Security Guide	This guide is meant to help physicians, clinic managers, staff, and IT support start on the path to achieving best practices for protecting clinics from information security risks.

DISCLAIMER

This document provides general guides and approaches only. We strongly recommend that you retain a knowledgeable and qualified professional to regularly assess and maintain your clinic's technology.

For more information, guidance, or support please contact:

Doctors Technology Office
604 638-5841
DTOinfo@doctorsofbc.ca
www.doctorsofbc.ca/doctors-technology-office