HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

WIRELESS NETWORK BEST PRACTICES GUIDE FOR CLINICS

Summary

Wireless networks are prime targets for a cyber-criminals and with personal health information also being a high value target of cyber crime, it is important to ensure that the wireless network of your clinic is appropriately configured to protect your clinical practice. This guide provides best practice guidelines for clinics or their supporting local IT provider to use when configuring their wireless network to help best protect patient information that may be accessed within that network and adhere to provincial privacy standards.

> ***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

The impact of privacy breach of information may be severe but by following the best practices for wireless network configuration and usage suggested below, a practice can be assured that this important component of their clinic infrastructure is well protected and focus on other areas of security that require more active management like user account maintenance. These suggestions will generally also result in better network performance within the clinic.

1. **Hire a professional IT support provider.**

   a. There is no substitute for a competent, professional IT provider who understands network equipment and standards to setup your wireless network.

   b. Your IT support provider should generally have some certifications related to specific network devices and common networking practices.

2. **Use business-class equipment.**

   a. For both security and performance reasons, business-class network equipment is highly recommended. This includes devices like network switches and wireless routers.

3. **Public access wi-fi must be separate from the clinic network.**

   a. If choosing to provide any public access to wi-fi services at your clinic, it should be managed entirely on a separate network from that of your business and reserved for non-business use only.

b. The unknown software installed and state of security on public devices can pose security risks and consume network resources.

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

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

b. The 5 GHz band provides shorter 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.

5. Disguise the wireless network name (SSID).

a. The names of wireless networks are broadcast publicly. Choose a name for your clinic wireless network that does not indicate to outsiders that the network belongs to a clinic as health information is a high value cyber crime target.

b. Setting the name to something other than the default also immediately signals to potential threats that your network has been configured and is less vulnerable that a network that still shows a default network name.

6. Change the default Admin username and password after initial setup.

a. Certain default settings on wireless devices may pose a security risk if not changed after the initial setup.

b. Changing the username and password of the administrator account for the wireless router with a personal username and strong unique password is highly recommended.

7. Do not use remote administration or wi-fi administration.

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.

8. Use WPA2 protocol setting (or higher) for the wireless network.

a. Set the wireless encryption protocol setting to Wi-Fi Protected Access II (WPA2) or better which will include AES encryption.

9. Disable Wi-Fi Protected Setup (WPS).

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

10. Use caution with Guest Accounts on the wireless network.

- **a.** Only use “Guest Accounts” for peripheral wireless appliances such as wireless speakers.
- **b.** Any other personal guest usage of wireless should be on a separate network from the rest of the business.

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 that supports it like the router.

12. Keep workstation and network device firmware up to date.

- **a.** Ensure both workstations and other 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 new vulnerabilities found by hackers are secured as soon as possible.

13. Monitor the wireless network for suspicious devices

- **a.** Routers and access points may allow the ability to see all of the connections on your wireless network.
- **b.** Use this ability to help monitor or periodically check 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.

15. Ensure wireless router and other network access points are placed to provide the best coverage while still placed as securely as possible.

- **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.

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