Doctors Technology Office (DTO): Technical Bulletin

Wireless – Reduce Risks and Improve Performance

DTO TB - #17-003	**Objective: (Updated)** To provide basic best practices guidelines regarding setting up a wireless network in your clinic for privacy, security and improved performance.

Brief Description:

Although no network can be 100% hacker proof, nevertheless, if you are concerned about privacy and security, you should make hacking your network as difficult as you can. By following a few basic steps, you can go a long way to hardening your wireless network. Another benefit you will notice is that your network will also be more stable and have better performance.

Potential Impact:

The impact can be summed up to time and materials; however, there is a significant difference when it comes to data breaches. Poor performance and inconsistent operations are annoying and impact daily workflow, but a data breach - depending on severity, may be considered an offence. Security breaches with patient records such as personal data and health history may not be solved by time and money.

Solutions to reduce impact:

1. Hire a professional technical IT.
    a. There really is no substitute for a competent professional technical IT, who understands your requirements, to setup your wireless network.

2. Use "Prosumer" or “small office” class of equipment.
    a. They are less expensive than professional equipment and are better quality than consumer hardware.
    b. They have added benefits such as more advanced security features.

3. Do not share your clinic's wireless network with your patients.
    a. The security configurations on their hardware devices - or lack thereof - can pose unforeseen security risks and consume a lot of your network resources.

4. Use 5GHz wireless setting instead of 2.4GHz.
    a. Most locations are already congested with other 2.4 GHz wireless networks. Many wireless routers near you are set to 2.4GHz. In addition, microwaves, cell phones, Bluetooth are also using 2.4GHz. We have found setting your wireless router to use 5GHz will greatly improve performance and stability. The down side is that 5GHz has a shorter range and does not penetrate solid objects as well as does 2.4GHz, but that should not be a problem for most offices. Please be aware that your computers’ wireless network cards must also be capable of using the 5GHz setting.

Author: Patrick Wong

Original Date Created: 2017-09-07

5. For those on the PPN, turn off DHCP (Dynamic Host Configuration Protocol)
    a. The wireless access point should be configured in "Bridge Mode" so security appliances within the PPN can identify infected computers.

6. Change the "Network Name" aka SSID. (Should I change my default SSID?)
    a. This name (SSID) is publicly broadcasted and makes it easier to identify your network.
    b. Other clinics in your area may have the same router, thus the same name.
    c. The default name provides hacker with information that can be used against you.
    d. Hackers may assume you have taken less care in setting up security and begin the attack.

7. Change your default Admin Username and Password immediately.
    a. Make the passwords complicated. (Creating complex passwords you can remember)

8. Deactivate Wi-Fi administration, remote 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 wireless professional IT agree.

9. Activate encryption (WPA2) - almost the single most important item to set.
    a. Select WPA2 type AES or better if you have a server, and avoid using the TKIP setting.
        i. If you don't have the WPA2 option, get a new router.
        ii. Create a complex password for users to connect to your wireless network.

10. Disable WPS (Wi-Fi protected setup) - or use with caution.
    a. This is the option where you can use a button or enter a PIN rather than a password. In short, people with physical access to your router would not need your password. Also to check out other security issues click this link? "Wi-Fi's Protected Setup Woes".

11. Configure "GUEST" accounts, networking or access.
    a. Only use "Guest Accounts" for peripheral wireless appliances such as wireless speakers.
    b. Turn off "Guest Accounts" if you provide patients with their own network as suggested.
        i. You should off-load non-business essentials such as wireless appliances here.

12. Double up on security. (Work with your professional IT).
    a. Turn on additional firewall setting, both software and hardware, if you have them.
    b. Turn on Win firewall or install firewall software on your computers. Some firewall software will monitor other software for sending data outbound.

13. Keep your router's firmware (software for hardware) updated.
    a. Like software, hackers find weaknesses in hardware devices, so keep it updated. Some routers have the ability to do this automatically, whenever new firmware is available.

14. Keep your computers wireless adaptors' firmware updated.

15. Monitor your wireless network for rogue devices.
    a. Some routers can provide a list of devices connected to your network; sophistication would depend on the quality of your router.
        i. Beware of rogue computers, rogue phones, rogue wireless access points (APs)

16. Turn off Wi-Fi Sense for Win10 users (How to turn it OFF)
    a. Win10 Wi-Fi Sense allows you and your **"Friend"** to share Wi-Fi connections without knowing each other's passwords. Though encrypted, the passwords are automatically sent to each other's computers to ease connections, but can be potentially hacked. "Friend" is defined as **EVERYONE** on your Facebook friend list, your Outlook contacts list and Skype contacts list - set to on by default.
    b. Microsoft tells us that "The password is also stored in Microsoft's database – in encrypted format so that no one can hack it".

17. Placement of your wireless router and access point.
    a. Restrict physical access from non-clinic personnel.
    b. Closets, ceiling and under a desk introduce heat, dust and signal interference.

18. Clinical Awareness
    a. Although this is placed at the end, if your staff are not aware, or are as concerned about security, the most talented professional setup would not amount to much. For example, it would not matter how strong the encryption is if passwords can be found under your keyboard or stuck to your monitor.
    b. Opening dangerous emails or visiting dangerous websites will render even the most powerful software virtually useless.
    c. You should be concerned with whom you have granted access to your network.

Background:

Wireless network can be cost effective when compared to wiring your office. Often, not only is it convenient to carry a wireless device around, the way some offices are, wiring may be next to impossible. However, wireless introduces another level of risks. In addition, wireless is never as fast or stable as wired. Also, be aware that any security is less convenient than no security, but that is the price we now have to pay to protect our data, thus ultimately ourselves. The good news is that once it's properly configured, there is little you will need to manage.

Note what your EMR software vendor's support model is when it comes to wireless.

Please do not attempt this on your own, but rather work with your local IT support vendor.

If you have any questions or would like more information contact:

Doctors Technology Office, 604-638-5841, dtotechsupport@doctorsofbc.ca