With the right features and proper security, your network can improve your practice's efficiency and make your job easier.

Demystifying Computer Networks for Small Practices

Glen Stream, MD, and Justin Fletcher, PhD

Small practices are becoming increasingly reliant on computer applications, such as practice management systems and electronic health record (EHR) systems, making them frequent topics of discussion for family physicians. Amid these technology discussions, however, physicians often fail to consider the computer networks on which these applications run. Planning and maintaining a computer network in a practice requires a number of important considerations. Failing to adequately account for these can result in an improperly functioning network with potentially serious consequences, such as security violations. This article will review the major decisions you must make to ensure that your computer network is an asset and not a liability to your practice.

If you're just getting started, you will likely need to hire a technology consultant to perform the actual network implementation. Make sure the consultant is aware of the special requirements of a medical practice and holds certifications such as Cisco Certified Internet Expert or Juniper Networks Certified Internet Expert. You should also ask for references or seek recommendations from your colleagues who have been through this process and can offer advice from their experiences.

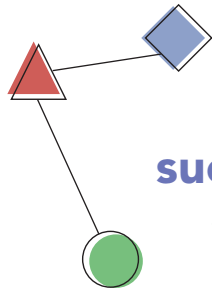
Wired vs. wireless

Both wired and wireless networks come with their own set of pros and cons. Wired networks are generally easier to implement and maintain. They also tend to be faster, more reliable and able to transmit greater amounts of data than wireless networks. The obvious disadvantage of wired networks is that they require you to pull cable to outlets throughout your office at every site where you wish to place a computer. This may be easy or difficult depending on the layout of your building. (Consult with a computer cabling installer early in your network planning to determine the amount of work involved.)

Wireless networks eliminate the need to pull cable to each computer location and allow you to use mobile computing devices. Many physicians find the mobility of a laptop or tablet PC to be an enormous workflow advantage. You can carry a device wherever needed in the practice and maintain a network connection. Wireless networks also eliminate the need to place a computer in each exam room. This reduces the security risk and damage risk posed by patients left alone in the exam room with a computer.

But wireless networks can create significant challenges:

ROBIN JAREAUX



Large amounts of metal or water, such as a refrigerator or even a fish tank, will completely block a wireless signal.

Careful planning will help you set up a computer network that functions properly and meets your practice's needs.

First, you must choose between a wired or wireless network; a wired network is faster and easier to maintain, but a wireless network allows greater mobility.

Wireless networks create additional challenges, including placing access points to avoid interference and securing the network from outside users.

Access points. Deployment of a wireless network involves the placement of base stations with antennas, also called access points, which connect to a wired network. Small offices may require only a single access point, but most practices will require access points throughout the office. Effective placement of the access points is a combination of art and science, and it will help you avoid interference.

Interference. If your practice is in a building with, or simply near, other offices with wireless networks, there can be interference. With the rapid deployment of wireless local area networks, this is an increasingly common occurrence. One means of avoiding interference is to select a non-overlapping channel, which is a configuration option on the access point.

Interference can also be caused by other wireless devices, such as certain types of cordless phones. If you get interference from another device, it may help to change the position of either the device or the access point. You can also change the channel used for wireless transmission.

The physical layout of a building and the materials used in its construction can also cause interference. Inside doors with glass can have some effect on the signal, while double-glazed windows, concrete and brick allow only a small amount of the signal through. Large amounts of metal or water, such as a refrigerator or even a fish tank, will completely block a wireless signal. In these cases, you can install additional access points, adjust the antenna orientation, add a wireless repeater or add a signal booster. Of course, the stronger the signal, the greater the possibility that someone else will be able to pick it up.

Security. Security is a major consideration for wireless networks. Wireless computers and access points broadcast their radio signals beyond the boundaries of your building, so you will need encryption in your wireless network to protect the privacy of your patients' health information. Various levels of encryption are available, and your choice will depend on several factors, such as how much you can afford to spend and how concerned you are about hackers attempting to access your network. The simplest way to encrypt your wireless network is to enable encryption on your access points. Modern access points will provide a variety of settings; you'll want to use the strongest you have available that is supported by your computer system.

Other simple measures will significantly improve the security on your wireless network. These involve changing the default settings listed below. To make these changes, you will typically use a Web browser to connect to the access point, authenticate yourself and then change the settings through the browser. Usually the vendor will provide instructions for changing the settings.

1. Service set identifier (SSID). Changing the default SSID (e.g., "linksys") to a name your staff members will recognize helps ensure that users connect to the proper network.

2. Internet protocol (IP) address and subnetwork. Your Internet service provider, which we will discuss shortly, will provide you with a range of IP addresses. These are the only public addresses you should use. There are private address ranges reserved for internal use. These can be used freely inside any private network; however, to connect to the outside world, these addresses need to be translated by the border router to your public addresses. Using the proper IP address will make it less likely that

About the Authors

Dr. Stream is medical director of clinical information services at the Rockwood Clinic in Spokane, Wash., and a member of the AAFP Board of Directors. Dr. Fletcher is a senior software engineer at Vyatta and an adjunct assistant professor at Oregon Health & Science University in Portland, where he is an instructor for the computer networks course. Author disclosure: Dr. Fletcher discloses that he is employed by Vyatta, a company that specializes in open-source networking solutions.

users will find out the specific make and model of your access point. This will make it more difficult for hackers to break into your system.

3. Account name and password. Assigning new account names and passwords is a critical security measure. If you fail to change the account name and password, anyone who successfully connects can change the configuration.

4. SSID broadcast. The SSID broadcast is what allows your network to show up in a wireless computer user's list of possible networks to select. This feature is usually turned on by default. Disabling the SSID broadcast means that a typical user has to know the network's name in order to connect to it.

5. Media access control (MAC) address filtering. Enabling this feature ensures that only specific computer systems can connect to your network. It can be a challenge to maintain, though, as you have to add an entry every time you bring a new computer into the network.

Connecting to the world

To get the most out of your office computer network, you will want to connect it to the Internet through an Internet Service Provider (ISP). Your local phone company and cable television provider are likely ISPs. Other companies may also provide Internet access, especially high-speed or broadband access.

ISPs vary in the spectrum of services they provide, so consider what other telecommunication services your office needs before choosing one. For example, you may desire to have your ISP host your practice's Web site or provide phone service. It is worthwhile to obtain bids from several ISPs so you can identify the one that offers the best value for services provided. If your office has mission-critical applications (such as a practice management or EHR system) operating with an application service provider, you may decide to use two ISPs so that your Internet access will be maintained should one of the ISPs have a service outage.

You also need to determine how much data will be going across your Internet connection so that you can select the appropriate type of connection. If you attempt to transmit a large volume of data over a small bandwidth connection, you will likely experience frustrating delays. For example, if you will be accessing picture archiving and communication systems (PACs), which involve the transmission of radiology images, you will likely need a high-capacity connection, such as a T1 line or fiber-optic connection. On the other hand, if you work in a small office and you're mostly sending e-mail and browsing the Internet, a digital subscriber line (DSL) connection from your phone company or a cable Internet connection from your local cable company can often provide adequate bandwidth.

Remote access

Access to your practice's data, especially patient information in your EHR, from your home or the hospital can provide substantial convenience and efficiency. However, remote access requires an evaluation of the benefits versus the risks. The benefits are clear: You can access patient data while on call, which can translate to better and more efficient patient care that is easily documented. Medical care provided with incomplete patient data is a frequently cited cause of medical errors,[1] and remote access can help prevent this. If your network is set up for remote access, you can be home with your family for dinner and remotely access your EHR to complete your daily chart work.

Data security risks are the downside of using remote access. When set up incorrectly, remote access can allow unauthorized persons to access your sensitive data. If you choose to enable remote access, make sure your office network is secure by encrypting your home connection via a virtual private network (VPN) or other similar technology. When accessing the network remotely, such as from home, always log off from office applications when your work is completed. This will prevent others from inappropriately seeing or accessing confidential information.

Network security

Network security involves physical, technical and administrative safeguards, all of which are important.

Physical safeguards. These are safeguards that defend your network from physical contact by unauthorized persons. To physically secure your network hardware, keep it in a locked room or closet accessible only to authorized persons. Repair and maintenance persons should be properly credentialed, and all parties should sign

Securing a wireless network begins with enabling the encryption on your access points and changing all default settings.

Consider your bandwidth requirements before choosing an Internet service provider.

Remote access allows you to access your network from outside the office, but you will need a secure connection to protect patient data.

a Health Insurance Portability and Accountability Act (HIPAA) Business Associate Agreement. Computer screens should be positioned so that unauthorized persons cannot easily view them.

Technical safeguards. A properly sized and configured firewall is a critical protection between your office network and the outside world. A basic guideline for firewall configuration is to permit network access only to known addresses and required services, and to deny all others.

Unique log-in names and strong passwords should be required for all network users. Strong passwords consist of at least eight characters, are alphanumeric and are not the log-in name or a word from the dictionary in any language. Network access should be given only to those individuals who need it to perform their duties, and even they should have access only to specific applications. Network users should lock their workstation if leaving for more than a very short period of time. The auto-logoff feature should be enabled on all computers so that a workstation inadvertently not locked will lock itself after a chosen period of time. Select the time-out interval based on your assessment of risk.

To safeguard your network from unauthorized persons, keep network hardware in a locked room.

Firewalls, strong passwords and secure Web sites are essential technical safeguards for a network.

Creating network policies and procedures for office staff will protect your network from internal violations.

If you have a Web server, the default access via hypertext transfer protocol (HTTP) is not encrypted. If sensitive material can be exchanged on the Web site, encryption is required. To provide encryption, you must allow only secure access to the site. Any requests that are not secure should be forwarded to the secure server's address. Your consultant should be able to help you with this process.

For extra protection, if you have a Web site that provides an e-mail address for others to contact you, list the e-mail address in a way that makes it difficult for other computers to read. For example, replace "@" with "at" and "." with "dot." This would change "physician@provider.com" to "physician at provider dot com." Spambots continually search the Internet for e-mail addresses to add to unsolicited bulk e-mail mailing lists, better known as spam. Some spam can contain viruses that will damage your computer. Educate staff on identifying and deleting suspicious-appearing e-mail attachments.

Administrative safeguards. You will need to create network security policies and procedures and hold all users accountable to them. Most computer security experts agree that the weakest link in the security chain is the system's users, and busy physicians are often the worst offenders. Physicians must set a good example for staff. Clear written policies about security breaches must be in place, including how you will notify those whose personal information has been exposed and what disciplinary actions will be imposed on those who committed the violation.

Writing down or sharing passwords is the most common breach and should be strongly discouraged. Staff accessing information they have no legitimate need to access is another common violation. You will also need to decide whether to allow network users to install software on their computers, either downloaded from the Internet or uploaded from CDs. Such software may introduce security weaknesses or other malicious programs into your computers and network. This includes benign appearing software, such as screen savers and games. Instant messaging is another Internet application that can invite malicious content into your network.

Finally, your office should have policies about the appropriate use of the network. Your network is a valuable and limited resource. Non-business uses can have a significant impact on network performance. Listening to Internet audio, watching streaming video and downloading large files of any kind can choke your Internet connection. Web surfing and using work e-mail for personal purposes consume employee time more than network resources, but you should still have policies about accessing inappropriate Web content and inappropriate e-mail content.

Investing in your practice

A computer network is the central nervous system for your practice. As such, it should be designed to meet your current demands and anticipate the need for growth as the use of computers in medical practices increases. It should also be equipped with ample security protection. With help from a qualified network specialist, you can successfully navigate the complexities that small practices face. It will be well worth the investment. FPM

Send comments to **fpmedit@aafp.org.**

1. Committee on Quality of Health Care in America, Institute of Medicine. *Crossing the Quality Chasm: A New Health System for the 21st Century*. Washington, DC: National Academy Press; 2001.