AMA
AMERICAN MEDICAL ASSOCIATION

# Protect your practice and patients from cybersecurity threats

Protect your office network to safeguard the confidential information and patient records of your medical practice.

## Network security

Your practice handles sensitive health information and financial data every day. Cybersecurity involves protecting this data both "at rest" (in a database) and "in transit" (moving across a network). To protect your data and entire information technology (IT) network from threats, you must take steps to implement good system hygiene.

## Connected devices mean risk

"At risk" IT systems extend well beyond electronic health records (EHRs), practice management systems and patient portals. Part of what makes technology so useful but also vulnerable, is the ability to network—or connect—different devices.

Many physician office networks are made up of a combination of personal computers (PCs), servers, tablets, smart phones, printers, scanners, Internet connections and Wi-Fi networks. As technology continues to evolve, even office phones, credit card readers and security systems may become part of this network. If a practice incorporates telemedicine, additional equipment and network devices may have to be considered.

Networks typically differ by the devices included within them, as well as each device's capabilities and manufacturer. However, networks also share commonalities and risks. Here are some best practices to safeguard your office network against cybersecurity threats.

## The Internet connection

Many offices have a broadband (high-speed) Internet connection. Keep in mind that this type of connection has access that's always "on." Therefore, the computers—and any network the computers are part of—are exposed to threats at all times.

To prevent unwanted access, install a device that monitors and controls network traffic (a "firewall") between the practice's internal network and the Internet. Typically, the "router" (the device that forwards data between digital devices or larger networks like the Internet) also acts as a firewall. This device may have already been installed by your Internet Service Provider (ISP) or you may have purchased it online or in a consumer electronics store.

The proper configuration of a firewall depends on the structure of the network; depending on network complexity, a network professional may need to be involved.

## Wi-Fi hotspots need protection

The Internet router can also act as a Wi-Fi hotspot or "switch" (which connects multiple devices together to form a network). Most small networks have only one router but can have multiple switches depending on the number of devices.

Because of the importance of the router in the network, it must be protected with a strong password. Usually the preinstalled password can be guessed easily by others, allowing them to control the device, and monitor or record data and communications to and from the Internet. As such, it is critical that the password be changed as soon as the router is installed. Each router is different, but typically this can be done in a web browser on one of your office computers.

Some office networks have separate devices that act as routers, firewalls, switches and Wi-Fi components; make sure to change the administrative password for each of these devices. Also, many of these components run software that can be periodically updated. If needed, consult with a network expert to make the appropriate changes and update the software.

## Operating systems firewall settings

If your office computers use a modern version of the Microsoft Windows operating system, they probably have a software firewall available. You should also ensure this is enabled.

Each version of Windows is different, but typically the firewall setting is under the "Control Panel." If you are running another operating system, or if you need further help, you can take a look at the **American Medical Association's office computer checklist**, check online or consult with a network expert.

## Securing Wi-Fi access

Many routers can facilitate more than one Wi-Fi network. This can be used to provide patients with a public network in the waiting room, separate from the network in the clinic. Security for both networks is critical.

Set the wireless access point so that it does not broadcast its Service Set Identifier (SSID), which is the name of the wireless network. Provide patients with the Wi-Fi login credentials on request. Try not to use an identifiable name (e.g., Dr. Smith's Wi-Fi) for either the public or private network, as it may draw unwanted attention to your network.

In addition to masking the identity of the SSID, also create strong passwords for both the public and private Wi-Fi networks. Remember, the public network can be accessed even outside the clinic's walls; anyone who has the SSID and password can connect at any time. When setting up the SSID, be sure to encrypt the Wi-Fi networks. This step is important because it helps protect office data from electronic eavesdroppers. The current recommended setting is the Wi-Fi Protected Access 2 (WPA2) protocol, using the Advanced

Encryption Standard (AES) for secure encryption. WPA2 and AES work together to help create a secure Wi-Fi connection.

Also consider setting an access schedule for the public Wi-Fi. Within the router's menu, time frames can be set to allow or disable Internet access for network devices. For instance, if the office is closed on Sundays, access can be disabled to keep people from using it.

Check the router owner's manual or consult with a professional for help in making these changes. Note that the Wired Equivalent Privacy (WEP) option is not considered secure and should not be used for securing wireless traffic.

## Remote access and VPNs

One of the most widely used methods to access information remotely is through a Virtual Private Network (VPN). VPNs provide the ability to securely connect back to your office using a range of devices. Over a VPN connection, you can use a tablet, PC or smartphone to securely access your practice management system and the patient records and diagnostic images stored in your office's EHR.

You may already have the technology to support a VPN. Make sure you talk to your EHR/practice management vendor or consult with an expert on how to securely use your office's network capabilities.

## Modern printers/copiers store data

Many medical offices lease modern copy machines and multifunction printers. These devices contain hard drives similar to computers and automatically store a copy of every document that is printed or copied. Since these documents may contain protected health or other sensitive information, practices must ensure that the data stored on the devices' hard drives is removed or destroyed before the machines are returned to the vendor. Consult with vendors and legal counsel to ensure appropriate contractual assurances of data destruction.

## Backup and disaster recovery plans

Even with good system hygiene, there are instances in which patients' data are compromised or lost, such as a system hardware failure or natural disaster. There has been a recent increase in attack activity targeting the health care community utilizing cryptography to render the office systems data unusable unless a fee is paid to the attackers. These attacks have been called Cryptolocker or Ransomware attacks. Having a current backup of the office data could potentially

help to recover this information without having to pay the ransom fee. To prepare for the worst, develop and test backup and disaster recovery plans that anticipate how to recover any lost medical and practice records. A variety of software and hardware solutions exist, but the most appropriate option may depend on the location of the data.

Many physician offices manage their own servers on site, with equipment located at the physical office location. However, with the growth of cloud computing and co-locating services, applications like EHRs, practice management systems and/or other health IT components like a telemedicine service may be located off site or managed by a third party.

Either way, make sure your health IT vendors support backups and that appropriate processes are in place to protect your data.

This is intended to provide a jumpstart in improving physician practice cybersecurity but should not be considered exhaustive.


17-181372:PDF:12/17