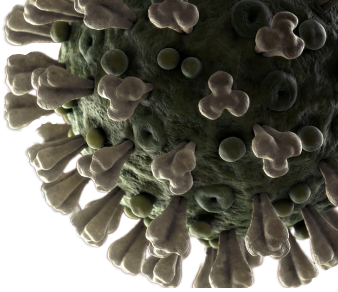
AMA AMERICAN MEDICAL ASSOCIATION

American Hospital Association™
Advancing Health in America



WHAT PHYSICIANS NEED TO KNOW

Working from home during COVID-19 pandemic

During the COVID-19 pandemic, many physicians are working from home, using their personal computers and mobile devices to help care for patients. Fortunately, technology can allow physicians and care teams to do much of what they could do at the medical office, remotely. Telemedicine is a powerful tool that spans a continuum of technologies and offers new ways to deliver care. Many electronic health record (EHR) systems allow you to connect over the Internet just as if you were in the clinic. While you are doing your part to help during the COVID-19 pandemic, the American Medical Association (AMA) and American Hospital Association (AHA) want to ensure you have resources to help keep your work environment safe from cyber-threats that could disrupt your practice, the hospital, or negatively impact your patients' safety and well-being.

Your Home Personal Computer (PC)

Your home computer, whether it be a Windows or Mac, laptop or desktop, is susceptible to cyber threats. It is important to take steps to keep your home office as resilient as your medical practice. We are learning of increased security threats to medical data due to the pandemic. Many cyber criminals are taking advantage of clinician interest in COVID-19 to infect practices', and hospitals' computers and networks with the hope of stealing or holding medical records for ransom.

To help protect you and your patients, the AMA has compiled a Checklist for Computers, which is a non-exhaustive list of **actions you should take immediately** to strengthen your home computer and network.

- Watch out for these common threats:
  - **E-mail phishing** is an attempt to trick you into giving out information using e-mail. E-mail cybersecurity should remain a top priority for clinicians and hospitals as a vast majority of cyber-attacks are initiated by clicking on a phishing e-mail containing malware (malicious software) or a malicious link appearing to be COVID-19 related from a legitimate organization. Additional information on e-mail phishing can be found at this resource on pages 16-17. The FBI has also issued several Public Service Announcements on business email frauds and CORVID-19 themed frauds and they can be found here.
  - **Ransomware** is a type of malware (malicious software) that attempts to deny access to data, usually by encrypting the data with a key known only to the hacker who deployed the malware until a ransom is paid. Paying a ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data. The FBI discourages paying the ransom as it may incentivize continued ransomware attacks and fund more serious crimes including violent crimes. Most ransomware attacks are sent in phishing campaign e-mails asking you to either open an attachment or click on an embedded link. Additional information on ransomware can be found at this resource on pages 18-19.
- Consider using a Virtual Private Network (VPN) and/or a cloud-based service, which are coming into widespread use as many organizations are encouraging staff to work remotely, even if not directly needed for patient care. 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. Your EHR vendor or telehealth service provider will have recommendations for using VPN or cloud-based technologies to support your work from home. When using these technologies, you should also consider:
  - Employing strong authentication and lockout parameters
  - Limiting remote access to only the necessary databases and systems in your office
  - Ensuring all VPN and cloud-based services' security patches are up to date

© 2020 American Medical Association. All rights reserved.

- Additional considerations:
  - Use multi-factor authentication for all personal and business accounts.
  - Enable, where available, lockout features for multiple incorrect login attempts.
  - Add "external origin" email caution banners on emails coming into your work email accounts.
  - Schedule regular forced password changes every 60-90 days—lengthy passwords using passphrases are best.
  - Establish verbal authentication procedures with a known person for any email request to change payment instructions, direct deposit information or requests for batches of sensitive data such as patient information, payment information, or W-2 information.
  - Add enhanced email system security protocols including advanced threat protection (ATP) to detect malware based upon behavior and known indicators.
  - Consider an application "whitelisting" strategy. A whitelisting strategy is one in which only safe, authorized and necessary applications can execute and run on computer systems or networks.
  - Prepare to defend against ransomware. Consider using the 3-2-1 rule to create secure backups:
    - 3 offline segmented backup copies of your data;
    - 2 different media types; and
    - 1 cloud-based backup.
    - Ensure direct and remote access to the backups is highly restricted and monitored

If your business is hit with fraud and a misdirected payment has occurred, you should notify your financial institution immediately. There is a high probability of electronic fund recovery if you notify your institution within 72 hours. Also, report fraud to your FBI local field office and at www.ic3.gov; they will work with you and your financial institution to attempt to the recover funds. Again, there is a high probability of fund recovery if reported within 72 hours to your financial institution and the FBI.

Also, if you have cybersecurity insurance, review coverage and understand any limitations. Prior to suffering an incident, consider reaching out to your insurance company for references to forensics firms which may help you recover your data if needed. And again, contact the FBI. They will work with other agencies, including DHS, not only in the investigation of the attack, but also to assist you in possible decryption of the data, mitigation of the impact or negotiation with the ransomware perpetrators.

Your Phone or Tablet

Smart phones and tablets can now provide many of the same features and benefits as desktop or laptop computers. Some EHRs allow you to use applications (apps) to connect back to your office to order medications and tests and document your patients' care. There are also several apps that provide two-way voice and video and other telemedicine services. As you consider using a mobile device to help care for your patients, review the ideas below to help protect yourself from cyber threats.

- Settings to check immediately
  - Make sure that each of your iPhones/iPads and Android devices are running the most up-to-date version of its operating system software. Often these updates address security vulnerabilities or add new features.
  - Make sure your home's wireless network is protected with a strong password. For example, use a combination of numbers, upper and lowercase letters, and symbols.
  - Enable encryption on both your device and apps if possible. This is often found in the device's or app's settings.
  - Use multi-factor authentication where possible.
  - Enable lockout features for multiple incorrect login attempts.
  - Install anti-virus software on your device.
  - Consider using a VPN app.
- EHR and telemedicine apps
  - Check with your EHR vendor to make sure you are downloading the right app for your environment. Many vendors offer several different apps; while some have similar sounding names, they may be created by third parties and not endorsed by your EHR vendor.

© 2020 American Medical Association. All rights reserved.

- Review the list of apps and services the federal government has recommended for telemedicine. While these apps may not offer full integration with your EHR, they may offer voice and video communications services for both you and your patients.
- Enable all available encryption and privacy modes when using telemedicine applications.

Your Home Network

Think of your home office as a miniature version of your medical practice. With multiple devices like printers, phones, tablets, and computers sharing the same network, there is an increased risk one or more could be attacked—compromising your entire network. Weaknesses in your home network could be exploited and impact your patients' data. Where possible, your home environment should have the same protections as your medical practice. The AMA has developed a resource to help safeguard confidential information and patient records that can help protect both your practice and home networks.

Adequate broadband is needed to transmit high quality audio and video data as well as text and images. Telemedicine can increase the demand on your Internet connection. This may impact the reliability of your home network or affect patient care. For example, physicians using video conferencing to treat a patient may need to examine an abrasion or other physical symptoms carefully. Your broadband connection needs to be strong enough to support high quality video streaming so the patient can be viewed clearly. Consider reaching out to your Internet service provider (ISP) to learn more about speeds available in your area.

Working from my practice – maintaining cyber hygiene

The COVID-19 pandemic is impacting our lives in several ways. Cyber attackers are taking advantage of interest in the novel coronavirus. Ransomware and phishing emails are being designed to look like reputable information from trusted sources. Physician practices should exercise caution when clicking on links, opening email attachments, downloading files and installing new programs. The AMA has developed tips and advice on protecting your computers and network to keep your patient health records and other data safe from cyberattacks. These include:

- Steps to improve your cybersecurity practices;
- Cybersecurity checklists for your computers; and
- Advice on protecting your medical practice from cyber threats.

Your EHR vendor can also act as a source of technical assistance, offer educational resources, or even provide supplemental cybersecurity training. Reach out to your customer support representative or helpdesk for additional information.

Adequate broadband is needed to transmit high quality audio and video data as well as text and images. Just like at home, telemedicine can increase the demand on your Internet connection at your practice. This may impact the operation of other health IT systems in your office network or effect patient care. For example, physicians using video conferencing to treat a patient may need to examine an abrasion or other physical symptoms carefully. Your broadband connection needs to be strong enough to support high quality video streaming so the patient can be viewed clearly. Consider reaching out to your Internet service provider (ISP) to learn more about speeds available in your area or business-class services tailored for health care facilities.

© 2020 American Medical Association. All rights reserved.

Working with medical devices

Medical devices can introduce additional and significant cybersecurity risk to a physician practice or hospital—risk that must be managed because of the possible threat to patient care and patient safety. Phishing emails can contain malware which may exploit the cyber vulnerabilities of medical devices. Medical device cyber vulnerabilities are often exploited by cyber adversaries to launch high impact ransomware and malware attacks against physicians and hospitals. Consider the following steps when identifying and mitigating cyber risk associated with medical devices:

- Establish a formal process of coordination and communication between clinical, biomedical engineering and information security teams for the procurement, acquisition, maintenance and proper use of medical devices and biomedical technology.
- Have a dynamic process to maintain an accurate inventory of medical devices, distinguishing which devices are network connected, network capable or stand alone.
- Maintain an inventory of the operating systems, firmware and software applications contained within your medical devices. You should ask your manufacturers and vendors to provide a software "bill of materials" (similar to a list of ingredients) for your devices to help ensure you know and can update the operating systems, firmware, and software your tools use.
  - If the medical device manufacturer or vendor provides a software "bill of materials," as some are starting to do, incorporate this into the inventory listing of that device.
  - This inventory should include remote patient monitoring devices, implanted medical devices such as pacemakers, and telemetry systems used to monitor and report patient information.
- Prioritize devices by criticality to life support, patient care and their potential impact on patient safety should they be rendered inoperable or malfunction due to a ransomware or other malware cyber-attack.
- Prioritize installation of updates and cyber vulnerability patches of network connected and network capable ventilators, and other mission-critical life support medical devices.
- Define who is responsible for maintaining patches, how often and for how long. Is this function included in the contract you or your organization has with the manufacturer, the vendor, or another third-party, or is it up to you? If it is your responsibility, consider outsourcing this function if you or your organization lack the internal capability or capacity to maintain updates and patches.
- Monitor updates and patch status of all software and firmware contained within the devices. Medical devices may contain dozens of firmware and software programs, including many third- and fourth-party embedded applications. Useful links to track medical device vulnerabilities can be found at US Cert and at the FDA.
- Deploy network segmentation strategies. Seriously consider disconnecting vulnerable medical devices—meaning those that cannot be patched—from internal and external networks. With the expiration of technical support for Windows 7, many medical devices may be running an unsupported operating system. Microsoft is offering a paid extended security update service for Windows 7 until January 2023.
- Ensure proper access controls, password protection and encryption where feasible to help mitigate cyber threats to medical devices.
- Purge unnecessary patient information stored on medical devices. Many medical devices are capable of storing large quantities of information, which may not be purged after the information is transferred to EHR systems. Cyber criminals are aware of this vulnerability and recognize that these devices may be an easier target from which to steal patient information than the EHR system.
- For additional information, the U.S. Department of Health and Human Services provides an overview of medical device cybersecurity and best practices for physicians and hospitals which can be found in Section 9 of its Cybersecurity Practices Technical Volume 2, found here. The Healthcare Sector Coordinating Council Cybersecurity Working Group also provides valuable resources to assist physicians and hospitals in enhancing medical device cybersecurity found here.

© 2020 American Medical Association. All rights reserved.

20-444412:04/20