AMA
AMERICAN MEDICAL ASSOCIATION

American Hospital Association™
Advancing Health in America

LOOKING FORWARD

Technology Considerations for the Rest of 2020

In the months since the United States first declared a public health emergency due to COVID-19, hospitals and physician practices have learned many lessons. Notably, the pandemic quickly increased most Americans' reliance on digital tools, including digital health technologies like telemedicine, which brought increased industry focus on how physicians and hospitals keep patients' protected health information (PHI) private and secure. *Privacy and security are distinct, but closely interrelated. It is not enough for medical practices and hospitals to invest in one but not the other. Fortunately, the concepts are mutually reinforcing, meaning that many actions that are taken to bolster security of patient information will also better protect the privacy of that information.*

The American Medical Association (AMA) and American Hospital Association (AHA) have monitored a variety of technology issues associated with the novel coronavirus and developed a range of resources to assist their members, including our joint resource, What Physicians Need to Know: Working from home during the COVID-19 pandemic. Now, as practices reopen, and hospitals around the country prepare for a second wave of COVID-19 infections coinciding with cold and flu season, our organizations are providing this update on steps physicians should take to prepare for the coming months

Cybersecurity

Risks and Vulnerabilities Update

The COVID-19 pandemic has dramatically changed our way of life and that of the world, including bringing a greater number of people together virtually. However, there is one group that views the pandemic as an opportunity to exploit our virtual community for illicit purposes – cyber criminals.

At the onset of the COVID-19 pandemic, there was a dramatic increase in phishing email campaigns directed toward the health care sector. These emails are cloaked under the guise of important information related to COVID-19. They make fake promises of retailers selling N95 masks and raise false hope for lifesaving ventilators—but instead are often laden with malware and malicious links.

The pandemic also brought an urgent need to dramatically expand the ability for physician and their staff to work remotely and treat patients. Remote Virtual Private Networks (VPN), and other cloud telehealth services have quickly expanded to support telework, telehealth, and for remote monitoring of medical devices. However, this expansion also dramatically increased the "attack surface" for cyber adversaries who quickly adapted and began probing hospital and physician office networks.

Cyber-attacks that disrupt patient care service and pose a risk to patient safety, such as ransomware attacks, are of the greatest concern. Successful ransomware attacks can cripple a health care provider by preventing access to medical records and disabling mission critical systems, resulting in a delay of care for the patient. There are ramifications for the providers as well. Ransomware attacks cause an interruption and loss of revenue. Remedying and recovering from an attack can also be very expensive. Further, attacks create legal and regulatory exposure and reputational harm. Unfortunately, during the pandemic we have a seen a significant increase in successful ransomware attacks targeting small and large providers. With the onset of EHR and health information technology interconnectivity to support clinically integrated care, we have seen attacks on individual providers cause a disrupting ripple effect among many providers, including physician offices, hospitals, ambulatory surgery centers, labs, pharmacies, and imaging centers.

Compounding this issue is the fact that critical cyber vulnerabilities have been discovered in ubiquitous technologies such as network and firewall services used in many hospitals and medical offices. For instance, Palo Alto and the National Security Administration announced a major security flaw which would allow an attacker to bypass authentication on Palo Alto's firewall[1] and VPN services. Additionally, in July, Microsoft announced the discovery of a 17 year old vulnerability in its Domain Name System (DNS) servers that allowed an attacker to penetrate an organization's network with self-replicating malware that could take over the entire network[2]

Vulnerabilities like those mentioned above underscore that medical practices and hospitals should request routine updates from their health information technology vendors or security professionals. Network security requires the use of technology and policies to keep that technology up to date. Below, you'll find a list of questions to ask your vendors to help ensure you're staying on top of your network security needs.

Questions to Ask About Your Network Security

- Are network components or services still in place in my practice that potentially create vulnerabilities? (I.e., use of personal mobile devices or home computers, out-of-date VPN or firewall technology, etc.)
- Are we running legacy devices or systems that utilize Windows 7 as the operating system? Support for Windows 7 expired on 1/14/2020 and is out of support for security updates, unless the extended security update (ESU) service is purchased. The ESU is only available through 2022. This is an extremely critical issue as most medical devices currently in service use Windows 7 as the base operating systems and thus will be either totally out of support in 2022 or very expensive to replace.
- Do we need to maintain newly added components or services? With continuing concern of a second COVID-19 wave in the coming months, many providers are rightly reluctant to remove some of their newly adopted networks and devices. Physicians and hospitals should make sure network devices that are retained are resilient and hardened against cyber-attacks.
- Many individuals, and perhaps outside parties and vendors, may have been given network access or company mobile devices during the "heat of the battle" where the priority focus was rightly on treating patients and saving lives. Do these individuals and outside parties still need access to your network or use of your mobile devices? If so, do they have the right level of access? Can it be limited to the minimum amount of access based on their current role?
- For the vendors that were provided network access, have they all signed proper business associate agreements (BAA)? Physicians and hospitals should consider including updated cybersecurity requirements in their BAAs to match the level of cybersecurity risk associated with the vendor's role, the amount of data they hold, and the sensitivity of the data and/or access they have been provided. The AMA offers a sample BAA for your reference.
- Where is protected health information (PHI) located now? Are there PHI and payment information on company or personal computers? Is it being sent using unencrypted emails, or stored in medical devices? Some medical devices and office equipment, such as imaging devices or photocopiers, can store thousands of patient records. Consider requesting that your medical device vendors review their data management policies and ensure PHI access is limited to only fulfill their roles and responsibilities. Also, when you purchase or upgrade new medical devices or office equipment, ensure that all PHI is properly removed from your older equipment by the vendor.

Privacy

Physicians are responsible for the privacy and security of PHI under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Among other things, HIPAA requires the physicians and hospitals to comply with following requirements:

- Enter into BAAs with third-parties using, storing, transmitting, or otherwise managing PHI on behalf of the physician or hospital to ensure PHI is appropriately handled by the third-party

[1] https://security.paloaltonetworks.com/CVE-2020-2021
[2] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

- Conduct a Security Risk Analysis to identify and evaluate what may expose PHI to inappropriate use or disclosure and take steps to address vulnerabilities
- Develop and implement policies and procedures to help ensure proper confidentiality and security of PHI

Preparing to come into compliance with HIPAA when the Public Health Emergency (PHE) declaration ends

Early on in the pandemic, the Office for Civil Rights (OCR) announced that it would use discretion in enforcing HIPAA violations for physicians and hospitals who, in good faith, utilized telemedicine platforms and applications to connect with their patients. While this was critical to helping clinicians quickly adopt telemedicine, physicians and hospitals should start planning now how they will come into compliance with HIPAA when the PHE declaration ends. Patient trust is central to the physician-patient relationship. While HIPAA compliance may seem onerous and burdensome, it is a necessary ingredient to the long-term, continued use and success of telemedicine technology. Physicians and hospitals should do all they can to assure their patients that they prioritize the privacy and security of their patients' health information—even during a pandemic. We encourage physicians and hospitals to have discussions with their telemedicine vendors about entering into a BAA and start taking steps to conduct or implement their security risk analysis of the telehealth platform.

We also suggest asking your vendor about their privacy practices, intended data use, and security protocols. Many physicians do not realize that a telemedicine platform or application may be low-cost or free because the vendor's business model is based on aggregating and selling patients' data. If possible, consult with your legal team to clarify how video, audio, and other data are being captured and stored by the vendor and who has access. You can also ask whether the vendor will share results of third-party security audits, including SOC 2 or HITRUST, in addition to the results of their penetration testing.

Whether you have been using telemedicine for many months or have just recently adopted the technology, we encourage you to be open with your patients about the potential privacy risks associated with use of telemedicine platforms and applications. We also recommend enabling all available privacy and security tools available when using such applications and using platforms with end-to-end encryption, as using unencrypted audio-visual platforms to communicate may result in third-parties being able to intercept the communications and "tap into" the conversation between a physician and patient.

Additional Resources:

- AMA's Physicians' Guide to Reopening: https://www.ama-assn.org/delivering-care/public-health/covid-19-physician-practice-guide-reopening
- AMA's Telehealth Implementation Playbook: https://www.ama-assn.org/system/files/2020-04/ama-telehealth-playbook.pdf
- AMA HIPAA Privacy and Security Resources: https://www.ama-assn.org/practice-management/hipaa/hipaa-privacy-security-resources
- AHA Cybersecurity Resources, Government Bulletins, Briefings and Articles https://www.AHA.org/cybersecurity
- CISA Ransomware Resources: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf
- How and where to report cyber-attacks:
    - Federal Bureau of Investigation Cyber Task Force
      https://www.ic3.gov/default.aspx;
      www.fbi.gov/contact-us/field
        - U.S. Secret Service Cyber Fraud Task Force www.secretservice.gov/investigation/#field
    - Cybersecurity and Infrastructure Security Agency
      https://us-cert.cisa.gov/forms/report