Four Ways to Mitigate COVID-19 Cyber Risks

by John Riggi, Senior Advisor for Cybersecurity and Risk, American Hospital Association, 3/25/2020

As COVID-19 progresses, cyber criminals seek to exploit health care infrastructure

As the nation's hospitals and health systems, physicians, caregivers and staff treat and care for patients and our communities, there are others in the world seeking to exploit the COVID-19 pandemic for financial gain. Particularly, cyber criminals.

We here at the AHA are closely monitoring government cyber bulletins and threat information from the field. We believe a hospital and health systems cybersecurity programs' first priority is to mitigate cyber risk affecting patient care and patient safety.

Ventilators and other life support medical devices are critical in the battle against COVID-19. In the most serious cases, life-saving mechanical breathing assistance is required for patients. Thus, we highly encourage:

- Formalizing coordination and communication between clinical engineering and information security teams
- Having a dynamic process to maintain an accurate inventory of medical devices
- Focusing on the update and cyber vulnerability patch status of network connected and network capable **ventilators, and other mission critical life support medical devices**.
    - This includes checking updates and patch status of all software and firmware contained within the devices.
- Deploying network segmentation strategies and disconnecting vulnerable medical devices, which cannot be patched, from internal and external networks. With the expiration of support for Windows 7, many medical devices may be running an unsupported operating system.

In addition, both the FDA and the Healthcare Sector Coordinating Council provide valuable resources to assist in enhancing medical device cybersecurity.

Email cybersecurity should also remain a top priority as a vast majority of cyber-attacks are initiated by an unsuspecting staff member clicking on a phishing email containing malware or a malicious link, which may appear to be COVID-19 related from a legitimate organization. In addition, we have seen a number of financial frauds based upon "spoofed" or impersonated emails purporting to be from health care related organizations seeking to divert pending legitimate payments. In the worst-case scenarios, we have seen adversaries actually penetrate legitimate emails systems through compromised passwords or social engineering techniques. Once in, the criminals use the compromised email account to send emails directing the diversion of legitimate payments to the criminals' accounts, steal information or distribute malware to address book contacts. To mitigate this risk we highly recommend:

- Staff awareness and education including routine phishing tests
- Multi-factor authentication starting with remote account access
- Lockout feature for multiple incorrect login attempts
- External origin email caution banners
- Regularly scheduled forced password changes every 60 – 90 day—lengthy passwords using passphrases are best
- 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 PHI, PII, payment information or W-2 information
- Heightened email system security protocols including advanced threat protection (ATP) to detect malware based upon behavior and known indicators
- Domain-based Message Authentication, Reporting, and Conformance (DMARC) to reduce risk of email spoofing
- Consider an application "whitelisting" strategy. A "whitelisting" strategy is a strategy in which only safe, authorized and necessary applications are allowed to execute and run on systems

If you are aware of a compromised email account in your organization or an email phishing campaign targeting the field, please contact John Riggi, senior advisor for cyber and risk at jriggi@aha.org. We will assist you, warn the field and leverage federal resources to mitigate the threat. In addition, we would also recommend reporting a breach to your local FBI field office and at www.ic3.gov.

Virtual Private Networks (VPN) and cloud-based services are coming into widespread use as many organizations are encouraging staff to work remotely, if not directly needed for patient care. The use of encrypted VPNs and clouds services, although fairly secure, does not come without cyber risk as the U.S. government has recently warned. The referenced bulletins identify several critical VPN and cloud-based service vulnerabilities identified over recent months. These vulnerabilities are actively being exploited by cyber criminals and nation state actors. When using VPNs and cloud-based services we would encourage organizations to:

- Employ multi-factor authentication and lockout for multiple incorrect attempts
- Limit and monitor international access
- Set download limits
- Limit remote access to sensitive databases
- Ensure all VPN and cloud-based services security patches are up to date

Please see attached links to government bulletins related to VPN and SharePoint vulnerabilities.

Telehealth is a necessary and vital capability for care delivery, especially to rural areas and for remotely triaging patients exhibiting COVID-19 symptoms. On March 17, 2020, HHS granted permission for providers to use every day, non-public facing technologies, such as FaceTime or Skype, during the COVID-19 public health emergency. HHS stated that their regulatory enforcement component, the Office of Civil Rights (OCR), "will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency[i]."

However, the guidance does not provide a blanket exemption for hospitals to use any communication platform. The notice specifically states that, "Facebook Live, Twitch, TikTok, and similar video communication applications are public facing, and should not be used in the provision of telehealth by covered health care providers." The notice goes on to state that the following platforms provide HIPAA-compliant video communication products, and that they will enter into a HIPAA Business Associate Agreement:

- Skype for Business
- Updox
- VSee
- Zoom for Healthcare
- Doxy.me
- Google G Suite Hangouts Meet

It is clear from the above recommended communication platforms that they exhibit similar characteristics: they are all known entities with proven track records, and all claim to offer some level of end-to-end encrypted communications.

HHS's practical and necessary telehealth HIPAA waiver is a recognition of how necessary and vital telehealth capability is for safe delivery of care, especially in rural areas or to remotely triage patients exhibiting COVID-19 symptoms.

The exercise of these capabilities during this national emergency will no doubt demonstrate the value of telehealth as a fundamental component of care delivery. This will likely further the expansion of the connected medical device ecosystem and the introduction of new technologies such as 5G and augmented intelligence (AI), which also greatly accelerate telehealth growth and capabilities. As such, we strongly encourage members to be cognizant of the potential cyber risk created by the telehealth landscape and to ensure proper security by design features are in place. This includes encryption in transit, and at rest and multi-factor authentication to mitigate risk to patient safety, security and privacy of patient data. The National Institute of Standards and Technology provides useful resources to assist members in this effort now and in the future.

For any questions on this or other cybersecurity and risk issues, please feel free to contact John Riggi, Senior Advisor for Cyber and Risk, and former FBI cyber executive, at jriggi@aha.org or 202-626-2272.

---

[i]