Physician cybersecurity vigilance and resources

Michael A. Cassidy, Esq.

The COVID-19 pandemic has exacerbated the already too prevalent public health information (PHI) hacks, providing a target rich environment of both businesses and individuals, and therefore medical practices, who are more susceptible to phishing attempts linked to providing test kits, PPE, pandemic information, etc. The data available through the hacking and other cyber crimes is highly valuable because it can contain significant PHI, i.e., name, birth date, account numbers, insurance numbers, phone numbers, addresses, social security numbers.

This threat is irrevocably intertwined with the increasing reliance on telehealth, because much of this information is being exchanged and stored via non-secure or less protected networks and through medical devices that do not have robust or effective cybersecurity protection, culminating in the following:

Continued on Page 392

From Page 391

- Increased remote telehealth interactions without appropriate additional security,
- Individual and institutional fears regarding pandemic issues have created more, susceptible targets, and
- A fragmented and outdated IT infrastructure, especially with individual physicians, small medical practices, and financially challenged hospitals.

Last month's article in the *Bulletin* entitled "Cybersecurity: Hackers Raise Stacks with Patient Safety and Provider Operations" by Beth Ann Jackson, Esq., was a timely prescient clarion call to physicians and medical practices to increase their cybersecurity vigilance. Recently, IT security publications have reported a majority of hospitals and more than 70% of all businesses have been victims of cybersecurity and ransomware attacks within the last twelve months.

This article is intended to provide physicians a basic understanding of the improved resources being made available to physicians in this area.

AMA: Working from Home White Paper

The American Medical Association (AMA) has published a short white paper entitled "Working from Home During COVID-19 Pandemic," which you can reach through the following link: https://www.ama-assn.org/system/files/2020-04/cybersecurity-work-from-home-covid-19.pdf.

AMA makes a number of recommendations, which are described in greater detail in the white paper, but include the following:

- Consider using a virtual private network (VPN) and/or a cloud-based service for your home connection, because they provide the ability to securely connect back to EHR/IT systems using a range of different devices.
- Inventory the devices you use to connect, i.e., home computer, smartphone, tablet, etc., and determine whether those connections are secure to your home network and whether your home network is secure.
- If you are using an EHR app as part of your home practice, you must verify that the app you are using is the most current version of that app for connection to the system's medical records.

The AMA white paper provides detailed recommendations regarding the following:

- Steps to improve your cybersecurity practices
- Cybersecurity checklists for your computers
- Advice on protecting your medical practice from cyber threats
- multifactor authentication and virtual private networks (VPNs) in relation to password strength.
- COVID-19 Cyber Threats (Update): https://www.hhs.gov/sites/default/files/covid-19-cyber-threats-update.pdf
- Social Media Attacks: https://www.hhs.gov/sites/default/files/social-media-attacks.pdf
- 5G Security for Healthcare: https://www.hhs.gov/sites/default/files/5g-security-for-healthcare.pdf

Resources to reinforce cybersecurity

- AMA –"Working from Home During COVID-19 Pandemic," https://www.ama-assn.org/system/files/2020-04/cybersecurity-work-from-home-covid-19.pdf
- HHS – Potential cyber threats, https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

HHS Threat Briefs

- Securely Teleworking in Healthcare: https://www.hhs.gov/sites/default/files/securely-teleworking-healthcare.pdf. NOTE: Section on

HHS launches physician cybersecurity website

The Department of Health and Human Services (HHS) Health Sector Cybersecurity Coordination (HC3) has recently launched a new website to help physicians and their medical practices be better informed about potential cyber threats at this link: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html.

One of the extremely useful resources accessible through this website is a series of "Threat Briefs," which HHS is publishing on a regular basis to provide detailed information regarding cybersecurity threats to physicians and their medical practices.

Although there are several dozen Threat Briefs existing on the website now, four of the most informative, in my opinion, are the following:

- Securely Teleworking in Healthcare: https://www.hhs.gov/sites/default/files/securely-teleworking-healthcare.pdf
- COVID-19 Cyber Threats (Update):

https://www.hhs.gov/sites/default/files/covid-19-cyber-threats-update.pdf

- Social Media Attacks: https://www.hhs.gov/sites/default/files/social-media-attacks.pdf
- 5G Security for Healthcare: https://www.hhs.gov/sites/default/files/5g-security-for-healthcare.pdf

The threat brief entitled "Securely Teleworking in Health Care" is very similar to the AMA website, and emphasizes critical cybersecurity defense such as multifactor authentication and virtual private networks (VPNs) that are structurally and inherently more secure than the "wifi" typically available from the commercial carriers.

The importance of multifactor authentication is grammatized recently by a report by Irongate Technology providing a visual graph of the time it would take a hacker to "brute force" your password.

- With passwords of four to six characters using numbers only, lower case letters only, upper case and lower case letters, any combination of all of those or any combination of numbers, upper and lower case letters, and symbols, the access time goes from "instantly to all of 5 seconds."
- Conversely, a 10-word password with numbers, upper- and lowercase letters, and symbols would take an estimated five years; an 11-character password would take 400 years; and a 12-character password would take 34,000 years. The time increases are exponential; a 15-character password with all of those combinations would take 15 billion years – considerably longer than any of our life spans!

Conclusion

HIPAA requires you to take reasonable steps to protect the privacy and security of your PHI data. Consulting these resources would be an appropriate next step.

Mr. Cassidy is a shareholder at Tucker Arensberg and is chair of the firm's Healthcare Practice Group; he also serves as legal counsel to ACMS. He can be reached at (412) 594-5515 or mcassidy@tuckerlaw.com.