AAP News™

Health care providers not immune to cyberattacks during COVID-19 pandemic

May 20, 2020

Srinivasan Suresh, M.D., M.B.A., FAAP

Article type: Health IT Trends

Topics: COVID-19, Health Information Technology, Infectious Diseases

Editor's note: *For the latest news on COVID-19, visit* https://www.aappublications.org/news/2020/01/28/coronavirus.

Health systems, hospitals and office practices have been relying more on technology and digital tools during the COVID-19 pandemic in ramping up telehealth and engaging staff in teleworking.

Making technology more convenient brings an inherent risk of reduced security. In health care settings, this can result in a breach of protected health information or financial information. There are reports of cybercriminals using certain types of documents (coronavirus coverage maps) on nonsecure websites to plant malware on computers that access those sites. There also are reports of targeted email scams promising personal protective equipment and COVID-19 treatments.

Cyberattacks can be extremely disruptive in health care settings. They can harm patients by interrupting continuity of care and making health data inaccessible to providers, patients and guardians. Hackers may steal and sell, or hold for ransom, personal information such as names, addresses and Social Security numbers. These attacks put children at particular risk because it may be years or even decades before anyone is aware a child's identify has been stolen.

Pediatricians and health care systems can take steps to prevent cyberattacks and security breaches during the COVID-19 pandemic. Though not an exhaustive list, following are some best practices that may help individuals and practices keep their systems and information secure.

General security

- Make sure your information technology (IT) system's spam protection is up to date and that the latest antivirus software is installed on all systems and devices.
- Antivirus software should always be running in the background.
- All work should be done on your company's secure virtual private network (VPN), even when working remotely. This will add an extra layer of security when working with personal information.
- If possible, enable two factor or multifactor authentication on any personal or work-related accounts (email, web meetings, etc.). This extra security will help minimize any potential hacking or exploitation of accounts by requiring you to enter a code typically sent to your cellphone to prove it is actually you accessing your account.
- Better safe than sorry! If something seems like it's not right, trust your judgment. Contact your IT support staff and ask them to check it out.

Email security

- Open emails only from trusted sources and be aware of the sender's email address. Even though an email may display the name of someone you work with, verify that the email address is associated with that individual. Cybercriminals may attempt to "spoof" an email to make it appear it is from a legitimate source when it is not. If you are unsure, reach out to that individual in another manner (phone call, text, etc.) to verify the person sent the message.
- Do not click on links provided in emails, especially if you do not know the sender or did not expect to receive the information described in the email. Manually type web addresses into your web browser.
- Check to make sure any links or websites included in emails are associated with a legitimate business or agency. Check for misspellings or incorrect domains in links (for example, anything from the Centers for Disease Control and Prevention will end in .gov not .com).
- If you do click a link or enter confidential information in an unknown or malicious site, contact your IT department immediately so it can assist with changing your password and scanning your computer to verify no malicious software or viruses are installed.
- Never provide the following information in the text of an email:
    - usernames,
    - passwords,
    - date of birth,
    - Social Security number/employee ID number,
    - financial data such as account numbers or
    - personal information.
    - Be aware of email red flags:
    - unexplained urgency,
    - last-minute changes in instructions, especially instructions related to finances or protected information,
    - last-minute changes in communication platforms or contact information,
    - refusal to communicate by phone and
    - requests for advanced payment, especially when advance payments have not been required previously.

Web meeting/conference security

- Make sure all meetings, especially employee meetings and virtual health care visits, are private by requiring a password for all patients/attendees or use the "waiting room" feature to approve participants who can enter the meeting.
- Provide meeting links to specific participants (i.e., in a personal email invitation or portal message).
- Manage options for screen sharing. Set up your meetings so that only the host can share a screen, and the host must grant others screen-sharing privileges.
- Make sure all participants are using the most up-to-date version of remote meeting tools.
- Make sure that you are developing and implementing telework policies that include guidance and expectations for physical and information security.

Dr. Suresh is a member of the AAP Council on Clinical Information Technology Executive Committee.

Related Content

- Information from the FBI on COVID-19 email phishing against health care providers
- Information from the FBI on COVID-19 online extortion scams
- Information from the National Security Agency on selecting and safely using collaboration services for telework
- Information from the Health Sector Cybersecurity Coordination Center on video teleconferencing exploitation during the COVID-19 pandemic
- Information from the Health Sector Cybersecurity Coordination Center on COVID-19 cyber threats
- Additional Health IT Trends columns