How to 'cybersecure' your practice

Kaustubh G. Joshi, MD

Dr. Joshi is Associate Professor of Clinical Psychiatry and Associate Director, Forensic Psychiatry Fellowship, Department of Neuropsychiatry and Behavioral Science, University of South Carolina School of Medicine, Columbia, South Carolina.

Disclosures
The author reports no financial relationships with any companies whose products are mentioned in this article, or with manufacturers of competing products.

doi: 10.12788/cp.0239

Discuss this article at www.facebook.com/MDedgePsychiatry

The health care sector is not immune from cybersecurity attacks (malicious attempts to access or damage a computer or network system). Between October 2019 and October 2021, 857 data breaches were reported to the United States Department of Health and Human Services.[1] The 3 main types of breaches reported were theft, hacking/IT incident, or unauthorized access/disclosure.[1] Health care has become a common target due to the availability of valuable patient information (health, personal, and financial), the industry's financial stability and resource capacity, and network susceptibility.[2] The top 2 cybersecurity threats facing physician practices are:

- **ransomware attacks**, in which an external party uses a type of malicious software (malware) that prevents you from accessing your computer files, systems, or networks, and demands you pay a ransom for their return.
- **employee-related threats**, such as the theft or destruction of sensitive information by a disgruntled employee.[3]

The financial implications of health care–related cybersecurity threats coupled with exposure to potential litigation associated with breaches of confidentiality result in a need to "cybersecure" your practice.[2] In this article, I outline steps to take to protect your practice against such threats. Although the recommendations I provide will increase your practice's cybersecurity fortification, they are not exhaustive, and you may need to consult with an IT specialist to help protect your data and network.

Improve your network protection. A broadband internet connection is always operating, which makes it continuously susceptible to cybersecurity attacks. Install a firewall (a network security system that monitors and controls network traffic and permits or blocks traffic based on a defined set of rules) between your practice's internal computer network and the internet.[4] For maximum protection, enable all available firewall settings in your operating software.[2] Prevent unauthorized access by ensuring that all network passwords are strong (ie, they include a combination of uppercase and lowercase letters, numbers, and symbols). Consider using different networks for online communication and for storing sensitive information.[2] Create separate Wi-Fi networks for your practice and for your patients, and use unique passwords for each that are not easily guessed.[4] If you or your employees use a virtual private network (VPN) to remotely access your practice's network, ensure that all devices used to do so (cell phones, tablets, etc) are encrypted and secured with strong passwords.

continued on page 19

Pearls: Cybersecurity

continued from page 12

Reduce employee-related threats. Not every employee in your practice will need to access to your patients' clinical or financial data. Limiting employee access to sensitive clinical or financial data can reduce the risks of employee-related cybersecurity threats.[3] In addition, restrict an employee's ability to install software on computers and other devices that belong to your practice.[2]

Frequently incorporate cybersecurity training, such as teaching your employees about the risks of clicking on links and attachments in emails and how to identify phishing attacks (in which an individual sends a fraudulent communication that appears to come from a reputable source in order to trick the recipient into revealing financial information, system credentials, or other sensitive data).[2,3] Use multifactor authentication to verify an employee's login identity, and change passwords often. Reinforce these policies at staff meetings and educate new employees about this process.[3] If you need to fire an employee, consider deploying cybersurveillance software to monitor the behavior of all employees before the employee is terminated.[3] Once the employee has been terminated, change all logins and passwords.

Restrict an employee's ability to install software on computers and other devices that belong to your practice

References

1. U.S. Department of Health and Human Services. Office for Civil Rights. Breach portal: Notice to the Secretary of HHS breach of unsecured protected health information. Accessed December 26, 2021. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
2. Umali G. How to safeguard your practice from cybersecurity threats. Psychiatric News. 2021;56(12):23.
3. Cryts A. Top two cybersecurity threats facing physician practices. Physicians Practice. March 13, 2020. Accessed December 26, 2021. https://www.physicianspractice.com/view/top-two-cybersecurity-threats-facing-physician-practices
4. American Medical Association. Protect your practice and patients from cybersecurity threats. 2017. Accessed December 26, 2021. https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/government/advocacy/network-security.pdf