Andrew N. Pollak, M.D.
CHAIRMAN

MARYLAND HEALTH CARE COMMISSION

Ben Steffen
EXECUTIVE DIRECTOR

Reducing Cybersecurity Risk

Overview

Electronic systems have revolutionized many aspects of health care delivery. Growing use and integration of these systems have also made the health care industry more vulnerable to malicious cyber-attacks. Increased cyber threats have resulted in a growing number of reported data breaches by providers with the majority resulting from hacking/information technology (IT) related incidents.[1] Consequences following a breach can include disruptions to operations, financial cost to recover and implement corrective actions, and reputational harm to providers impacting patient trust.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes requirements for the privacy and security of patient health information. HIPAA was amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 to, among other things, strengthen privacy and security safeguards, which included extending liability to business associates and business associate subcontractors. Updated requirements are detailed in the final HIPAA Omnibus Rule that went into effect on September 23, 2013. Today, evolving cyber threats that include targeted attacks to expose vulnerabilities in how people interface with technology demonstrate the need to implement additional security measures above the minimum requirements established by federal laws. This is evident with the increased threat of ransomware that is often instigated with a phishing scam (i.e., a fraudulent message attempting to manipulate an end-user of technology into divulging confidential information in order to gain system access). This scenario can lead to the alteration or shutdown of systems that are central to providing care.

A Scalable Response

Cybersecurity requires a proactive and ongoing approach by health care organizations to better detect, prevent, and quickly respond to a potential security incident. Cyber risks can vary depending on the nature of the services provided, to what end technology is integrated into care delivery, and organizational structure and policies. Implementing safeguards to protect software and operating systems is essential; equally important is changing behavior by end-users of systems to reduce the risk of a breach.

> "Cybersecurity is not limited to the cyber-environment, but encompasses the people, processes, policies, and technology that contribute to an organization's overall cybersecurity readiness."
>
> --*The Maryland Health Care Commission, Cybersecurity Self-Assessment Tool*

Here are some basic steps your practice can take that are free or have minimal cost:

1. **Ensure systems require staff to use strong passwords** that are at least 10 characters in length, include upper and lower case letters, numbers, and special characters, and are unique to each system accessed. Passphrases can help make passwords easier to remember. For example, start with a phrase such as, "Mom likes apple pie!". Then replace some of the letters with punctuation, special characters, and numbers to replicate the passphrase: "M0mlikes@p11epie!". This technique should be used by staff at all levels of the practice and for administrative accounts that are often initially set up with default login information.

2. **Implement multi-factor authentication** where users provide two or more credentials to gain system access. This can include entering a password and responding to security questions (e.g., what is the maiden name of your maternal grandmother?). It may also require that users possess a physical object like a key card or token (e.g., a personal identification number or PIN). Multi-factor authentication is a best practice in verifying user identities by creating multiple barriers for a hacker.

[1] Maryland Health Care Commission. *Health Care Data Breaches: How Maryland Compares*, December 2017. Available at: www.mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/AllStateBreaches_Final.pdf.

3. **Routinely train staff to increase awareness and education** about best practices including how to identify potential threats like phishing. Staff should be educated on how to identify cyber threats and encouraged to report them if they suspect they could have been targeted. Emphasizing specific areas of responsibility and assessing staff retention about security protocols can be beneficial and helps foster good cybersecurity best practices. Increasing cybersecurity awareness enhances prevention and detection capabilities and ensures staff is prepared to respond if a breach is suspected.

4. **Create an incident response plan** for detecting and managing suspected security incidents. Having a plan in place helps minimize the impact of a cyber-attack and protects the safety and security of your patients. An incident response plan should encompass processes to mitigate risks and potentially avoid a breach, including roles and responsibilities across the organization that can be reasonably understood and enacted. Plans should be updated regularly to account for emerging threat scenarios and changes within the organization.

Overall, creating an organizational culture that values risk-awareness and stewardship is a significant step towards improving security. Establishing a commitment among leadership to follow basic steps like those listed above is a good place to start. Reinforcement about best practices and reassessment of employees understanding will help ensure a strong security-minded organization.

Resources

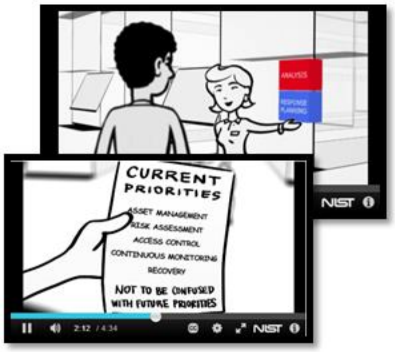
The Maryland Health Care Commission (MHCC) worked with stakeholders to develop the Cybersecurity Self-Assessment Tool.[2] This free tool can help practices identify gaps in cybersecurity readiness related to people, processes, policies, and technology. The MHCC has also released other publications that provide information about the current state of cybersecurity in Maryland.[3]

Other resources include:

- The Medical Group Management Association (MGMA) fact sheet, ***Cybersecurity in Medical Practices***: www.mgma.com/government-affairs/tools/cybersecurity-action-steps-for-medical-practices

- ***Top Ten Tips for Cybersecurity in Health Care*** from the U.S. Department of Health and Human Services: www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

- ***HITRUST Community Extension Program*** offering free in-person events across the country to promote education and collaboration about cybersecurity best practices. More information available at: www.hitrustalliance.net/community-extension-program/



Screenshots taken from National Institute of Standards and Technology (NIST) video, "The Cybersecurity Framework", available at: www.nist.gov/cybersecurity-framework.

In Summary

Some level of risk will always exist in a technology-dependent environment. The threat is especially real for the health care industry because of its unique access to personal information. Cybersecurity should be treated as a strategic critical asset that all health care organizations must proactively monitor and enhance. Continuous improvement of cybersecurity will help ensure strategies keep pace with emerging threats, prevent IT system intrusion, and reduce the risk and magnitude of a breach.

[2] MHCC, *Cybersecurity: A Self-Assessment Readiness Tool*, May 2017. Available at: www.mhcc.maryland.gov/mhcc/pages/hit/hit/documents/Cybersecurity_Self-Assessment_Tool.pdf.
[3] MHCC, Health Information Technology, Cybersecurity. Available at: www.mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/hit_cybersecurity.aspx.