# Cyber Liability Insurance

*Tips for Small Practices*

## A CYBER-ATTACK TAKES PLACE...

Dr. Jones' owns a small practice with one other provider and three support staff. The receptionist receives an email pertaining to a past due invoice that appears to come from a software vendor. The receptionist clicks a link in the email and inadvertently launches ransomware,[1] a type of malicious software (or malware[2]) that locks access to computer files and systems while demanding payment (a "ransom") to gain access back to critical data. Practice operations come to a halt – the receptionist cannot schedule appointments, and Dr. Jones' is unable to access patient data in the electronic health record (EHR) system. Dr. Jones' is prepared to minimize downtime. She routinely conducts cyber drills (or walk-through exercises) with practice staff that simulate likely scenarios testing the practice's ability to detect and respond appropriately. The practice also has cyber liability insurance; Dr. Jones' promptly calls the carrier to assist with recovery.

## OVERVIEW

Cybersecurity is crucial to ensuring business continuity and protecting patient safety, health, and privacy.[3] Cyber-attacks occur daily and can prevent access to mission critical systems, including EHRs and practice management systems.[4] Practices of all sizes can be targets.[5] Phishing is the most common cause of cyber-attacks, resulting from human error (i.e., an unintentional action or a lack of action).[6, 7] Most often, what appears to be a seemingly legitimate email tricks a victim into clicking a link or downloading a file to launch a cyber-attack.[8] It is estimated that 90 percent of data breaches are launched through phishing.[9] Adequate cyber liability insurance can help protect practices against cyber threats like phishing.

## WHAT IS CYBER LIABILITY INSURANCE AND WHY IS IT SO IMPORTANT?

Cyber liability insurance provides practices with a combination of coverage options to assist with response and recovery, including data breach lawsuits, interruption in operations, recovery expenses (e.g., potential regulatory fines and penalties), network damage, and data breach lawsuits.[10] Coverage can offset costs associated with a breach, such as support staff to locate and fix the cause of a breach, a call center to answer questions from patients, public relations,[11] attorney fees, and patient notification and credit monitoring services.[12]

**Cyber liability insurance does not replace implementing cybersecurity best practices; having insurance helps enhance a practice's overall security posture[13] (i.e., the ability to detect, prevent, and respond to cyber threats).[14]**

## TIPS FOR SELECTING CYBER LIABILITY INSURANCE

- Align coverage with total liability at the practice[15]

  Identify how much and the type of electronic protected health information (or "ePHI") stored by your practice (e.g., number of unique patient medical records and credit card information) to understand the potential risk if ePHI is compromised in a breach[16, 17]

- Utilize the results of a cybersecurity risk assessment to understand risks and help prepare for and mitigate various cyber threats[18]

  Refer to MHCC's Cybersecurity Preparedness Self-Assessment Questionnaire

- Determine what amount of coverage, if any, is provided by your malpractice insurance carrier[19]

  Understanding coverage provided by your malpractice carrier can help you determine what coverage, or additional coverage, the practice needs[20]

- Make sure cyber liability insurance is personalized for your practice

  Use an insurance broker that is knowledgeable about health care cyber risks and can recommend appropriate coverage options based on practice risk

- Make sure questionnaires[21] required by insurance carriers are completed accurately

  Incorrect information may not be discovered until a claim is filed, which can result in denial of the claim, leaving your practice without funding and resources to help with recovery[22]

## CYBERSECURITY PREPAREDNESS SELF-ASSESSMENT QUESTIONNAIRE

The MHCC, in collaboration with stakeholders, developed the *Cybersecurity Preparedness Self-Assessment Questionnaire* (questionnaire) using the National Institutes of Standards and Technology (NIST)[23] Cybersecurity Framework.[24] The questionnaire consists of a series of self-evaluation statements, grouped by people, process and technology, intended to help users identify potential gaps in cybersecurity and prioritize areas for improvement. Cybersecurity preparedness is essential to maintain information technology system(s), sustain operations, protect against current and future cybersecurity threats, and respond to and recover from a cyber-attack. Complete the questionnaire at: mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/Cybersecurity_Self-Assessment_Tool.pdf.

## BUY MARYLAND CYBERSECURITY (BMC) TAX CREDIT

The BMC Tax Credit provides an incentive for Qualified Maryland Companies to purchase cybersecurity technologies and services from a Qualified Maryland Cybersecurity Seller. The incentive is for companies that have fewer than 50 employees in Maryland and are required to file a tax return in Maryland. Eligible companies can claim a tax credit for 50 percent of the net purchase price of cybersecurity technologies and services purchased from a Qualified Maryland Cybersecurity Seller. More information and a list of Qualified Maryland Cyber Security Sellers is available at: commerce.maryland.gov/fund/programs-for-businesses/buy-maryland-cybersecurity-tax-credit.

## OTHER RESOURCES

**10 Practices to Protect Your Organization from Cyber Threats**
Infographic highlighting 10 practices to mitigate cyber threats.

**Top 10 Tips for Cybersecurity in Health Care**
ONC provides information and additional resources for reducing cyber risks.

**HIPAA Safe Harbor Bill: Understanding What It Means for Your Practice**
Summary of the HIPAA Safe Harbor Bill.

## Questions?

Contact: Justine Springer, Program Manager
justine.springer@maryland.gov

---

[1] Trellix. *What is Ransomware*. Available at: www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html.
[2] Malware is a program or code that is launched on a computer system with the intent to cause harm. More information is available at: www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-cyberattacks/#:~:text=Malware%20is%20the%20most%20common,software%20in%20a%20malicious%20way.
[3] WHiMA. *Best Practices for Cybersecurity in Healthcare*. Available at: www.whima.org/cybersecurity-a-comprehensive-risk-management-approach-for-healthcare/.
[4] GlobalSign. *The Impact Felt in Healthcare Breaches*. Available at: www.globalsign.com/en/blog/impact-felt-healthcare-breaches.
[5] In 2017, 8 in 10 doctors reported experiencing a cyberattack at their practice. Health care records have a lot of information that has monetary value on the dark web and a low tolerance for downtime, which makes health care appealing to cyber criminals. Health care records include information such as date of birth, place of birth, credit card details, Social Security number, address, and emails, which can be used to steal a person's identity. Health care practices also cannot have downtime, which can disrupt patient care; so, it is critical to get systems back up, and practices may be more willing to pay ransoms to have systems restored. More information is available at: www.ama-assn.org/practice-management/sustainability/8-10-doctors-have-experienced-cyberattack-practice.
[6] Tessian. *Must-Know Phishing Statistics: Updated 2022*, January 2022. Available at: www.tessian.com/blog/phishing-statistics-2020/.
[7] It is estimated that 70 percent of cyber-attacks involving ransomware target health care organizations with fewer than 500 employees. More information is available at: www.fiercehealthcare.com/practices/hackers-target-small-hospitals-practices-for-ransomware-attacks.
[8] Crowdstrike. *The 14 Most Common Cyber Attacks*, September 2021. Available at: www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-cyberattacks/.
[9] It is estimated that 90 percent of data breaches are launched through phishing attacks. More information is available at: www.tessian.com/blog/phishing-statistics-2020/.
[10] Medical Economics. *What Physicians Need to Know about Cyber Liability Insurance*, May 2021. Available at: www.medicaleconomics.com/view/what-physicians-need-to-know-about-cyber-liability-insurance.
[11] Ibid.
[12] Insureon. *Cyber Liability Insurance*. Available at: www.insureon.com/small-business-insurance/cyber-liability.
[13] Centraleyes. *Cybersecurity Insurance Alone Isn't Enough: Here's Why*, June 16, 2022. Available at: www.centraleyes.com/cybersecurity-insurance-alone-isnt-enough-heres-why/.

[14] AppDynamics. *Seven Steps to Strengthen Your Security Posture*, October 26, 2022. More information is available at: www.appdynamics.com/blog/security/seven-steps-to-strengthen-your-security-posture/.
[15] Maryland Health Care Commission. *Cyber Liability Insurance: What Practices Need to Know about Risk, Selecting Coverage, and Avoiding Common Pitfalls*, February 2022. Available at: mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/Cyber_Liability_Insurance_Webinar_Slides_20220218.pdf.
[16] Ibid.
[17] Between 81 and 100 percent of data is stored digitally at small and large practices. More information is available at: www.helpnetsecurity.com/2022/04/05/cyberattacks-healthcare-providers./.
[18] HHS. *Security Rule Guidance Material.* Available at: www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[19] See n. 15, *Supra*.
[20] Ibid.
[21] Cyber liability insurance carriers have questionnaires that a practice is required to complete in order to purchase insurance. These include, but are not limited to, questions on the technical infrastructure, cybersecurity controls, PII held at the organization, and training. More information is available at: www.csoonline.com/article/3619877/17-cyber-insurance-application-questions-youll-need-to-answer.html.
[22] See n. 15, *Supra*.
[23] NIST was established by Congress in 1901 to create a measurement infrastructure for technology. NIST works across all industries in which technology plays a role. Their core competencies include measurement science, rigorous traceability, and development and use of standards. A wide variety of industries, including health care, rely on NIST technology standards, measurement and standards that enhance economic security and improve quality of life. www.nist.gov/about-nist.
[24] The NIST Cybersecurity Framework uses globally recognized standards for cybersecurity to provide a common structure for a variety of approaches to cybersecurity that can be utilized by organizations regardless of size, cybersecurity sophistication, or degree of cybersecurity risk to improve their cybersecurity infrastructure. More information is available at: nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.