Publication of Medical Mutual / Professionals Advocate®

DOCTORS Rx

Volume 27, No. 1

Spring/Summer 2019

WHEN CYBERCRIMINALS ATTACK

ARE YOU PROTECTED?

find out...

- What is a cyberattack?
- How does a cyberattack impact your practice?
- How can you protect yourself and your practice?

A LETTER FROM THE CHAIR OF THE BOARD

Dear Colleague:

Do you know how to protect yourself against cybercriminals eager to mine your patient data? This new edition of *Doctors RX* gives you the tools you need to understand the threats, protect your practice, and avoid becoming a statistic.

George S. Malouf, Jr., M.D., FACS
Chair of the Board
MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate Insurance Company

ISSUE HIGHLIGHTS

DOCTORS RX

Elizabeth A. Svoysky, J.D., Editor
Vice President - Risk Management

Dr. George S. Malouf, Jr., M.D., Chair of the Board
MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate® Insurance Company

CONTACT

Home Office Switchboard	410-785-0050
Toll Free	800-492-0193
Incident/Claim/ Lawsuit Reporting	800-492-0193
Risk Management Program Info	ext. 215 or 204
Risk Management Questions	ext. 224 or 169
Main Fax	410-785-2631
Claims Department Fax	410-785-1670
Web Site	mmlis.com proad.com

WHEN CYBERCRIMINALS ATTACK

Are You Protected?

THE ATTACK

It's early Monday morning, and you've just arrived at your office to review your notes from Friday and check your schedule for the day. You turn on your computer and a pop-up alert brightens your screen—one you've never seen before. It reads: "Your system is locked. You have no access. To unlock your system, you must pay 18,000 Bitcoin to CRYPT7ONIC."

Many thoughts enter your mind: What does this mean? How can I see patients without access to electronic medical records? Has data about my practice or patients been stolen? What is Bitcoin? Should I pay this "ransom" request?

You have just been the victim of a ransomware attack. It is an anxiety inducing event, but there are things you can do reduce your risk of experiencing this scenario. In this article, we will address the importance of cybersecurity and some options for how you can implement the right cybersecurity protections for your practice.

SECURITY BREACHES IN THE HEALTH CARE INDUSTRY

Medical records are the most valuable data on the dark web because these records usually contain a wealth of information about a patient.[1] Year after year, the number of health care related breaches reported to the United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) increases.

Breaches by Covered Entity Type

Year	Provider	Health Plan	Business Associate	Other	Total
2010	134	21	44	0	**199**
2011	137	20	42	1	**200**
2012	155	22	36	4	**217**
2013	199	18	56	5	**278**
2014	202	71	41	0	**314**
2015	196	62	11	0	**269**
2016	257	51	19	0	**327**
2017	288	52	19	0	**359**
2018	273	53	39	0	**365**

During 2018 alone, more than 6 million individuals were affected by a health care data breach, and the average cost of these breaches is estimated to be more than $400 per individual record.[2] Only HIPAA-covered entities that experience a breach affecting more than 500 individuals are required to report the incident to HHS immediately. Consequently, the reports to HHS are not inclusive of all health care breaches, but this should not leave you with the impression that your practice has a diminished chance of a data breach. Indeed, 58% of malware attacks—attacks involving malicious software like ransomware—were against small businesses.[3]

The Impact of a Breach on You and Your Practice

A data breach at your practice not only has the potential to severely harm your reputation and competitiveness, it could also take away valuable time treating your patients. According to one survey, patients stated that they are less likely to return to a provider that has

George Chambers *is the MEDICAL MUTUAL Director of Information Technology. George has spent more than two decades developing technology security strategies for the public and private sectors.*

Ashton Delong, Esquire *is an Associate Attorney for MEDICAL MUTUAL.*

Example of a Physician – Targeted Vishing Attack:

In March 2019, the Drug Enforcement Administration (DEA) alerted the public to an international phishing and vishing scam involving the impersonation of DEA agents. The DEA warned that customers, Physicians, and pharmacies were receiving emails or phone calls from individuals "stating that they [were] the subject of an investigation," threatened revocation of a Doctor's DEA number, and "demand[ed] money to clear up the matter." The caller(s) even referenced a Physician's state license number and/or National Provider Identification Number in an attempt to legitimize their request for information or payment. Full text of the DEA alert can be found at https://www.dea.gov/press-releases/2019/03/13/dea-warns-alarming-increase-scam-calls

experienced a data breach that could have been prevented by cybersecurity measures.[4] Financial consequences trail a breach as well because you may not have access to data needed to provide patient care leaving your practice in limbo.

Unsurprisingly, legal consequences also follow a breach. For example, a State Attorney General could initiate a HIPAA action completely independent of the HHS pursuant to the HITECH Act and such action could result in substantial fines. The HITECH Act further permits individuals who have had their personal health information lost, stolen, or inappropriately accessed to file a data breach suit against a health care organization. Not only can a breach result in regulatory action or civil lawsuit, but it also could give rise to a separate state action depending on the state in which you practice.

So, how do you avoid all of this mess in the first place?

UNDERSTAND THE THREAT

To understand how to prevent an attack that could result in a breach, it is important to understand the types of attacks you and your practice may be vulnerable to.[5] Generally, cybersecurity attacks are levied in two ways: (1) when an outside entity accesses your network remotely or (2) when an outside entity gains physical access to hardware like a company laptop. We will focus on some of the attacks levied in the former manner.

Phishing, Smishing, and Vishing Attacks

Phishing is "[a] technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person."[6] In other words, an attacker masquerading as a reputable person or company attempts to gain access to your system by sending emails to employees of your practice. Usually, these emails will ask an employee to click a web site link or download an attachment. When the receiver of this email clicks on the link or downloads the attachment, the attacker accesses the system. An alternative phishing tactic is for the email to contain a link that looks like a valid web site where the recipient has an online account but instead directs the recipient to a false web site. When the recipient logs into his/her account or changes a password using the link, the attacker obtains the recipient's username and password for later use.

Smishing is a relatively new form of attack with the advent of smartphones. Smishing is a technique that targets a victim by using text messages and often provides a link or phone number where the recipient can obtain more information.[7]

Below are some warning signs of a phishing and smishing attacks:

- The sender is unknown.
- The subject matter in the message is unexpected.
- There is a sense of urgency – i.e., you have been locked out of your account.[8]
- The message is sent at an odd time of day.
- The message contains spelling errors and/or poor grammar.
- There is a request to click a link, attachment, or call a specific number to learn more.
- If there is an offer, it seems too good to be true.

Vishing, on the other hand, is similar to phishing and smishing, but its method of attack is via phone call.[9] An attacker using vishing will call someone and attempt to extract information or payment.

Some warning signs of a vishing attack are as follows:

- The call is automated.
- The caller is aggressive and conveys a sense of urgency.
- The caller is defensive when you ask questions.
- The number is an unknown number.
- The caller asks for personal information or asks for payment.
- The caller offers you something too good to be true.

It is important to trust your instincts and investigate before complying with requests for information, clicking a link, downloading an attachment, or giving personal information. Indeed, attacks using the technique of providing a link or downloading an attachment exposes

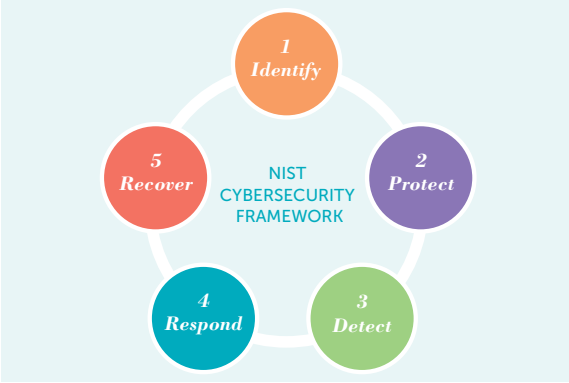
you and your practice by giving the attacker access to your network. Once attackers gain access to your network, the attacker can then download malicious software such as the one described in the next section.

Ransomware Attack

Ransomware attacks can be the byproduct of an attacker gaining access to your network through a phishing or smishing attack, but attackers can also download ransomware when you visit a particular web site.[10] HHS defines ransomware as "a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that destroys or exfiltrates data, or ransomware in conjunction with other malware that does so." [11]

DEVELOP A DEFENSE PLAN

The above attacks could be used to access data such as patient records, billing, or employee information, just to name a few.[12] The National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity" is a common example of a cybersecurity framework employed to aid in protecting data. The framework progresses through five stages: **identify, protect, detect, respond,** and **recover.**



The **identify** stage involves verifying the effectiveness of established controls you have in place concerning your network. The **protect** stage is comprised of the development and implementation of the appropriate safeguards to decrease your risk of an attack. The **detect** stage involves the implementation of processes and software to detect a breach. The **respond** stage entails the creation of an incident response plan for when a breach occurs. Lastly, the **recover** stage concerns planning for the continuation of the practice and recovering lost or compromised data.[13]

*All the steps in this framework are important to protecting your data, but for the remainder of this newsletter, we will focus on the **identify** and **protect stages**, and the steps you can take right now to mitigate your chances of an attack.*

THE IDENTIFY STAGE: A BRIEF OVERVIEW

The first step to mitigating your cybersecurity risk is to identify what type of network—hardware and software—you have in place at your practice.[14] Some questions you might ask yourself are as follows:

1. Do you have internet access? Do you have Wi-Fi?
2. Do you have computers and/or laptops?
3. Do you have a software program that facilitates remote access to work computers via cellphones, iPads, or other mobile device?
4. Do you have a patient portal?
5. Do you have electronic health records? Can those records be accessed remotely?
6. What type of operating system do you have (Microsoft, Apple iOS)?
7. Do you have in-house servers, routers?
8. Do you have firewalls, encryption, or other security software?[15]

Once you identify what hardware and software is in your network, it is important to determine how well your current security measures are working including any internal policies you may already have in place. For brevity, one way to do this is to partake in a risk assessment test[16] such as the one on our web site available at *https://www.mmlis.com/content/security-risk-assessment* For a more in-depth assessment, you might also consider consulting with a cybersecurity expert to better understand your network's vulnerabilities and to aid you in conducting more rigorous testing

Warning:

Attackers sometimes conduct extensive research on a target and then tailor an attack to exploit their target's interest. For example, an attacker may notice from your social media accounts that you enjoy taking cruises. An attacker could exploit this interest by sending you an email or sending a text message offering information on a new cruise line and providing a link to a web site.

such as penetration testing—a type of test for vulnerability that can include the simulation of attacks on your network.[17]

THE PROTECT STAGE: OPTIONS FOR IMPLEMENTATION

Protecting your patient's data is *your* responsibility. It is imperative that you have someone on your staff responsible for managing cybersecurity for your practice; this person could even be your already designated HIPAA security officer.[18] You and your assigned security staff member should consult with the vendors (EMR, IT) your practice already uses for managing electronic data to ascertain how these vendors can aid your practice in implementing cybersecurity protections. Depending on the amount of electronic patient data in your possession, you may also choose to consult with a cybersecurity expert or employ a cybersecurity expert(s) in your practice. If you decide to engage a cybersecurity expert, tips for choosing the right cybersecurity expert are provided at the end of this article.

In the meantime, below are *some* measures you and your staff can implement now and topics you may wish to discuss with a cybersecurity expert:

Awareness Training

Importance: Regardless of the investment in protective technology, an untrained staff can be considered the greatest vulnerability to an organization's data. Educating employees is vital and will provide you and your employees with the knowledge to recognize attacks such as phishing, vishing, and smishing.

Implementation:

- Cybersecurity Awareness Training: Training employees could take the form of in-person training, an online training program, or watching free online videos. Interactive training is a particularly good option because the training can require employees to answer questions at the end of the training to encourage retention of knowledge. Whatever option you choose, the training program should educate employees about what they can do to prevent a cybersecurity attack and the training should take place, at a minimum, annually.
- Education on Practice, Policies and Procedures: Educate your employees on what to do if they suspect an attack, including developing internal notification procedures and the consequences if an employee fails to follow security procedures.
- Alerts: Alert employees to current cybersecurity alerts from the FBI, DEA, HHS, and other federal and state government agencies via email or training.

Access Control

Importance: Access controls create secure access protections for authorized users while ensuring unauthorized users are not able to view, access, or alter certain data. This is an important protection measure because an attacker may not be able to access all of your data depending on the access controls of a particular employee.

Implementation:

- Internal Policies: You should consider creating a policy in which you identify which employees in your practice need access to certain data. For example, a physician assistant may not need access to your billing system, and therefore, you decline to provide physician assistants with login credentials for the billing system.

Data Security

Importance: Data security involves the protection of your network from attackers who attempt to infiltrate your network via the internet or email. This type of protection is important to aid in preventing all the threats described in this article.

Implementation:

- Antivirus software: Antivirus software is "[a] program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents."[19] Antivirus software

Awareness Training

Importance: Regardless of the investment in protective technology, an untrained staff can be considered the greatest vulnerability to an organization's data. Educating employees is vital and will provide you and your employees with the knowledge to recognize attacks such as phishing, vishing, and smishing.

could be provided to you at no cost depending on your operating system—Windows, iOS, etc.—or you could decide to purchase antivirus software within your budget.

- Firewalls: Firewalls protect your network when communicating in a public network like the internet.[20] Firewall software can monitor both incoming and outgoing activity, and a firewall may already be included in your operating system. You also have the option of purchasing firewall software.
- Encryption: It is vital to encrypt personal health information especially when this information is connected to the internet, and when this information is sent outside your network via email or other communication method. Don't forget to include your patient portal in the equation. In determining the right encryption software for your practice, you may want to read the NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices for more information on the types of encryption available. This publication can be found at ***https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800111.pdf?language=es***[21]
- Data Backup: HIPAA requires that practitioners in possession of electronic protected health information implement a procedure to backup this data.[22] It is, therefore, imperative that you implement a process to backup your data such as the use of a cloud storage service that stores your data in an offsite server away from your practice. Even if you do not use a network that includes electronic protected health information, backing up your data pertaining to employee records or billing could aid in recovery of this data if your network is attacked by malicious software.[23]
- Multi-Factor Authentication: Multi-factor Authentication "prevents hackers who have obtained a legitimate user's credentials from accessing your system."[24] For sensitive data, multi-factor authentication should be a top priority.
- Wi-Fi Access: If you decide to provide Wi-Fi to your patients or guests, make sure this Wi-Fi connection is separate from the Wi-Fi connection that you and your staff use. All Wi-Fi should be password protected, and if you offer Wi-Fi to your patients, the password should be different than your staff Wi-Fi and available only upon request.[25]
- Extra layers of security: If you have a complex network of data that you keep in electronic form, you may want to discuss with a cybersecurity expert about the option of implementing several layers of security. For example, you may wish to install several different antivirus or firewall software that monitors different aspects of your network, i.e. email, e-personal health information, etc.

Maintenance

Importance: It is critical to stay up to date on software updates from the manufacturer because these updates may fix vulnerabilities the manufacturer has identified to be subject to attacks. It is also important to review your policies on access controls. Staying up to date on software and other internal policies are important to manage the risk of exposures to malicious software.

Implementation:

- Software updates: Allow for automatic or notification of all new updates for your systems, including your electronic health record software.
- Review of Access Controls: Periodically plan a time to review the individuals who are granted access to sensitive data and remove those who no longer need this access.

CONCLUSION

As with many things in life, there is no security measure that will 100% protect you from a cyberattack, but these suggestions will make your practice a harder target for attackers. Educating yourself and those in your practice on the threat of cyberattack is the first critical

Your MedGuard Coverage Includes Cyber Protection

MedGuard is a comprehensive coverage provided at no additional charge that works as a complement to an Insured's professional liability coverage. Included in your MedGuard coverage is our e-dataRESPONSE cyber protection to help you navigate the complicated legal response to a data breach and cover payment for out-of-pocket expenses including:

- *Legal services to respond to or defend an insured event*
- *Computer security consultant services to determine the cause and extent of a data breach for which the Insured has legal responsibility to provide notification or mitigation*
- *Fines or penalties by a government agency due to the privacy breach*
- *Fees and other expenses the Insured becomes legally obligated to pay to implement credit monitoring or other mitigation for persons affected by the breach of private information*

Cost

Though your assets are no less valuable to you than that of a large organization, the solution and service should be priced accordingly to the size of your network and the amount of data you are protecting.

FOR MORE INFORMATION, VISIT

MMLIS.COM/CYBER
OR
PROAD.COM/CYBER

step. Consult your insurance producer to see what coverage may be available to you for these situations. Be proactive in your cybersecurity and remember that you do not need to take this journey alone.

Selecting the Right Cybersecurity Partner

REPUTATION

Do they have a positive track record with former clients? Be careful when working with start-ups.

CERTIFICATIONS

Do they possess some combination of the following certifications?

- *Certified Information Systems Security Professional*
- *Certified Information Security Manager*
- *Certified Information Security Auditor*
- *SANS Certification*
- *Certified Ethical Hacker*

ABILITY TO EXECUTE

Are they able to provide layered solutions in a simplified manner?

DELIVERABLES

Are they able to provide outgoing evidence of vulnerabilities and blocked attacks?

FLEXIBILITY

Are they willing to work when it is most convenient for your schedule?

TRAINING

Are they willing to engage in ongoing information sharing for the purpose of mitigation breaches?

COST

Though your assets are no less valuable to you than that of a large organization, the solution and service should be priced accordingly to the size of your network and the amount of data you are protecting.

references

[1] CBS News, Hackers are stealing millions of medical records – and selling them on the dark web, Feb. 14, 2019, available at https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/

[2] Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, 9, available at https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

[3] Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, 8, available at https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

[4] TransUnion, Nearly Seven in 10 Patients Would Avoid Healthcare Providers That Experience a Data Breach, March 2015, available at newsroom.transunion.com/transunion-survey-nearly-seven-in-10-patients-would-avoid-healthcare-providersthat-undergo-a-data

[5] For a list of the most common types of cyberattacks: Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, 18, available at https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

[6] NIST Glossary, Phishing, available at https://csrc.nist.gov/glossary/term/phishing

[7] FCC, Avoid Temptation of Smishing Scams, available at https://www.fcc.gov/avoid-temptation-smishing-scams

[8] 2018 Public-Private Analytic Exchange Program, Vulnerabilities of Healthcare Information Technology Systems, available at https://www.dhs.gov/sites/default/files/publications/2018_AEP_Vulnerabilities_of_Healthcare_IT_Systems.pdf

[9] FBI, Smishing and Vishing, available at https://archives.fbi.gov/archives/news/stories/2010/november/cyber_112410/cyber_112410

[10] FBI, Cyber Crime, available at https://www.fbi.gov/investigate/cyber

[11] HHS Fact Sheet: Ransomware and HIPPA, 1, available at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf; Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, 18, available at https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

[12] Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, 16, available at https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

[13] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[14] This article will not address all the facets of the identify stage of the NIST framework. For more information: National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[15] See American Medical Association, Protect you practice and patients form cybersecurity threats, available at https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/government/advocacy/network-security.pdf; American Medical Association, Checklist for office computers, available at https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/government/advocacy/computer-security-checklist.pdf

[16] NIST has a HIPPA Security Rule Toolkit that is available at https://csrc.nist.gov/projects/security-content-automation-protocol/hipaa

[17] See NIST Glossary, Penetration Testing, available at https://csrc.nist.gov/glossary/term/penetration-testing

[18] See 45 CFR § 164.308; HHS, Summary of the HIPPA Security Rule, available at https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

[19] NIST Glossary, Antivirus Software, available at https://csrc.nist.gov/glossary/term/Antivirus-Software

[20] https://csrc.nist.gov/glossary/term/firewall

[21] NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices, available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800111.pdf?language=es

[22] 45 CFR § 164.308(a)(7)

[23] American Medical Association, Protect you practice and patients form cybersecurity threats, available at https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/government/advocacy/network-security.pdf

[24] Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol1-508.pdf

[25] American Medical Association, Protect you practice and patients form cybersecurity threats, available at https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/government/advocacy/network-security.pdf

CME TEST QUESTIONS

1. Warning signs of a vishing attack include all but the following:

   A. The message contains spelling errors and/or poor grammar.
   B. The message requests you to click a link or attachment
   C. The sender is known to you
   D. The message is sent at an odd time of day

2. Only Federal law is triggered by a breach of patient data

   A. True B. False

3. Ransomware attacks can be a result of visiting a particular web site

   A. True B. False

4. Ransomware attacks cannot access billing or employee information, only patient information

   A. True B. False

5. The NIST Framework includes the following stages: Identify, Protect, Detect, Respond, Recover

   A. True B. False

6. Practices should have policies in place to identify which employees require access to certain data

   A. True B. False

7. Multi-factor authentication allows hackers who have obtained a legitimate user's credentials access to your system

   A. True B. False

8. Phishing attackers may do extensive research on a target to tailor the attack to exploit a particular interest of the target

   A. True B. False

9. Even if attackers gain access to your system, they would be unable to download malicious software

   A. True B. False

10. Firewalls protect your network when communicating in a private network

    A. True B. False

Instructions – to receive credit, please follow these steps:

Read the articles contained in the newsletter and then answer the test questions.

1. Mail or fax your completed answers for grading:
   Med•Lantic Management Services, Inc. | Fax: 410-785-2631
   225 International Circle | P.O. Box 8016 | Hunt Valley, Maryland 21030
   Attention: Risk Management Services Dept.
2. One of our goals is to assess the continuing educational needs of our readers so we may enhance the educational effectiveness of the *Doctors RX*. To achieve this goal, we need your help. You must complete the CME evaluation form to receive credit.
3. Completion Deadline: August 31, 2019
4. Upon completion of the test and evaluation form, a certificate of credit will be mailed to you.

CME Accreditation Statement

MEDICAL MUTUAL Liability Insurance Society of Maryland is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for Physicians.

CME Designation Statement

MEDICAL MUTUAL Liability Insurance Society of Maryland designates this enduring material for a maximum of one (1) *AMA PRA Category 1 Credit*.™ Physicians should claim only the credit commensurate with the extent of their participation in the activity.

CME EVALUATION FORM

Statement of Educational Purpose

Doctors RX is a newsletter sent twice each year to the insured Physicians of MEDICAL MUTUAL/Professionals Advocate.®
Its mission and educational purpose is to identify current health care-related risk management issues and provide Physicians with educational information that will enable them to reduce their malpractice liability risk.

Readers of the newsletter should be able to obtain the following educational objectives:
1) Gain information on topics of particular importance to them as Physicians
2) Assess the newsletter's value to them as practicing Physicians
3) Assess how this information may influence their own practices

CME Objectives for "When Cybercriminals Attack – Are you Protected"

Educational Objectives: Upon completion of this enduring material, participants will be better able to:
1) Understand how cyberattacks can occur in a practice
2) Identify risks to your practice through ongoing security assessments
3) Prepare a defense plan to prevent a cyberattack from happening

---

	Strongly Agree				Strongly Disagree
Part 1. Educational Value:	5	4	3	2	1
I learned something new that was important.	❑	❑	❑	❑	❑
I verified some important information.	❑	❑	❑	❑	❑
I plan to seek more information on this topic.	❑	❑	❑	❑	❑
This information is likely to have an impact on my practice.	❑	❑	❑	❑	❑

Part 2. Commitment to Change: What change(s) (if any) do you plan to make in your practice as a result of reading this newsletter?

_____

_____

_____

Part 3. Statement of Completion: I attest to having completed the CME activity.

Signature:_____ Date:_____

Part 4. Identifying Information: Please PRINT legibly or type the following:

Name:_____ Telephone Number:_____

Address:_____

_____

_____

_____

RISK MANAGEMENT NEWS CENTER

WE'RE HERE TO ANSWER YOUR LIABILITY QUESTIONS

Did you know that you can call our Risk Management department to ask about any liability concerns you have? Our Risk Management department includes experts with extensive medico/legal backgrounds, ready to give you instant advice and answers about liability questions. Contact us today at 410-785-0050 or toll free at 800-492-0193.

PHYSICIAN WELLNESS

MEDICAL MUTUAL is proud to be unveiling a brand new risk management education program this year on Physician Wellness for MEDICAL MUTUAL Insureds. This important program will address the unique challenges that health care professionals face and will include interactive activities, resources and daily coping strategies. Maryland Doctors can sign up today for this very valuable program at *mmlis.com* – coming soon to Professionals Advocate!

EHR WEBINARS

We offer free EHR webinars, conducted by a variety of EHR vendor professionals, that focus on patient engagement, portal use, security and helpful "tips and tricks" on EHR optimization. These webinars, while not for CME credits, contain valuable and timely information for medical practices of all types! Both Physicians and office staff are encouraged to attend these important sessions. You can check *mmlis.com* or *proad.com* for more information.

OPIOID PROGRAM

Our online Opioid risk management education program meets the two-hour requirement in both MD and VA– and it even meets the CDS license requirement in Maryland! Participants will also receive their RM discount upon completion. This course provides necessary information concerning the prescribing of opioids to treat pain, the laws governing opioid prescribing and how to limit risk for both you and your patients. Register now at *mmlis.com* and *proad.com*

MEDICAL MUTUAL and Professionals Advocate offer a variety of online tools and resources that are specially designed to help Doctors identify and address preventable issues before they escalate into potentially serious legal action.

MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate® Insurance Company

Home Office: Box 8016, 225 International Circle
Hunt Valley, MD 21030 • 410-785-0050 • 800-492-0193

DOCTORS Rx

Publication of MEDICAL MUTUAL / Professionals Advocate®

PRACTICE SELF-ASSESSMENT SURVEY

IS YOUR CURRENT PRACTICE PROTOCOL LEAVING YOU VULNERABLE TO RISK?

MEDICAL MUTUAL and Professionals Advocate provide a short self-assessment survey for your convenience, designed so that you can better determine which areas within the non-clinical aspect of your practice may be leaving you open to a lawsuit. Examples of non-clinical aspects include medical record documentation, patient scheduling, prescriptions and patient communications – all of these can affect the likelihood of a claim. Take our quick, two-part survey and know within minutes what your practice can do to improve risk prevention! This important resource can be found at *mmlis.com* or *proad.com* and touches on many topics, including patient privacy, telecommunications and more!