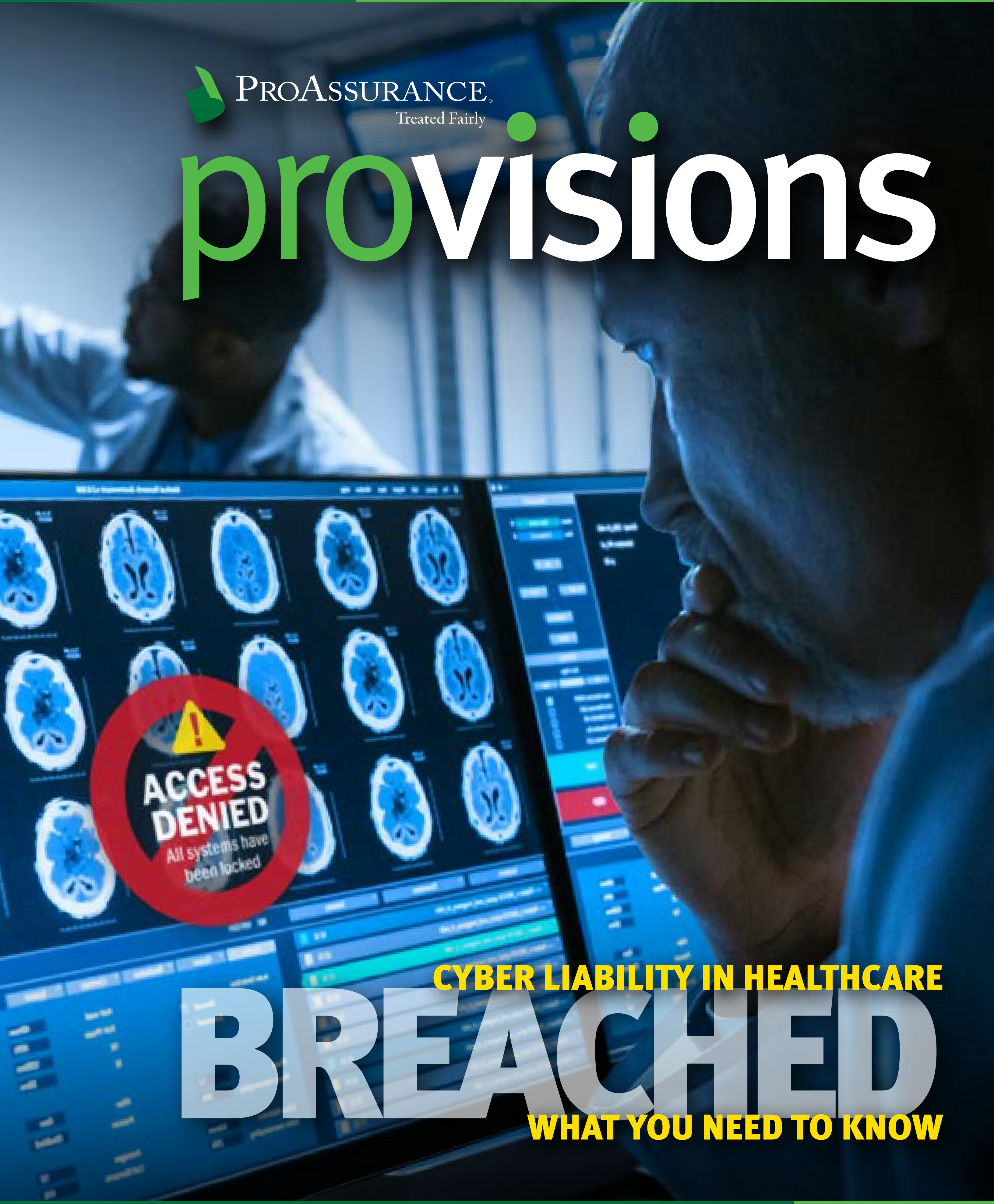
Monthly Insights for ProAssurance Agents

FEBRUARY 2020 | CYBER LIABILITY

ProAssurance®
Treated Fairly

provisions



CYBER LIABILITY IN HEALTHCARE

BREACHED

WHAT YOU NEED TO KNOW

> *"Taking the time to assess your firm's cybersecurity can prevent a breach. Do you conduct daily offline backups? Do you have a policy to notify parties of a breach? How does your company know that authentication is required to access case files? Regularly reevaluate your firm's status to address new risks."*
>
> **Michael Stoeckert**
> **Chief Technology Officer**
> **ProAssurance**

Hackers attack every

39 seconds.

On average, it took 7 months to identify a breach in 2019.

ProVisions is ProAssurance's monthly agent magazine. If you or your colleagues do not receive the digital version, email **AskMarketing@ProAssurance.com**. Please include names and email addresses for everyone who would like to subscribe.

A Word from the CMO

Staying on Top of Cyber

We're certainly no strangers to the talk of serious cyber issues in the healthcare industry. But as much talk as there is around cybersecurity options for medical entities, state of the industry reports have largely stayed the same.

Healthcare still ranks as one of the top targets for cyber criminals, and healthcare networks continue to have serious security weaknesses. The reliance on electronic health records, interconnected systems, and teleworking medical staff is ever growing. That provides even more opportunity for hackers to find an entry point and help themselves to valuable information. It's not "if" you get hacked. It's "when."

If you follow any industry publications, your inbox is probably flooded with tales of hospital systems paying out huge ransoms to get their systems back—followed by massive Health Insurance Portability and Accountability Act (HIPAA) fines for the data exposed during the incidents.

What doesn't make the news, but stays top of mind at ProAssurance, are the stories of smaller physician offices hit by the same threats. The loss amounts are not so jaw-dropping, but are more personally devastating.

HIPAA fines add up, and a physician might have to pay a ransom to get access to their data. Add in the time an office must remain closed while a data breach gets sorted out and the bill only gets worse. And, it's difficult to put a price on how having patient data exposed damages a physician's reputation.

Cyber liability insurance helps protect a physician from the long-lasting damage a cyberattack can have on their livelihood. In addition to providing a tool to manage the aftereffects, ProAssurance's cyber policy provides a key risk management component.

Everyone who has access to ProAssurance's secure services portal (SSP) can access cyber risk management resources from our partner for cyber liability policies, Tokio Marine, HCC (TMHCC)—the entity which acquired NAS Insurance Services last year. Sign in to the TMHCC CyberNET® portal for news and best practices. Get a glimpse of their offerings in more detail throughout this issue.

It's our hope that when someone inevitably decides to try to make their way into your system, you have a clear idea of how to proceed. And, you can pass those resources onto your clients.

Thank you for continuing to communicate this important issue during your sales conversations.

Thank you!

Jeff Bowlby
Chief Marketing Officer
ProAssurance

TABLE OF CONTENTS ...

PROASSURANCE.
Treated Fairly

ProAssurance Cybersecurity Coverage Options

CyberAssurance Plus

Most ProAssurance medical professional liability policies include CyberAssurance® Plus coverage at no additional cost. This endorsement helps to address the cyber risks physicians face every day as they interact with and store patients' medical and financial data.

These critical coverage enhancements include:

- **Multimedia liability**—including copyright/trademark infringement, libel and slander, plagiarism, and personal injury resulting from dissemination of media material.
- **Cyber extortion**—expenses incurred and extortion monies paid as a direct result of credible cyber extortion threats.
- **Cyber terrorism**—for income loss, business interruption expenses, and special expenses as a result of total or partial interruption of the insured's computer system due to an act of cyber terrorism.
- **PCI DSS assessment**—for claim expenses and assessments and fines imposed by banks and credit card companies due to noncompliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.
- **BrandGuard**™—for lost revenue as a result of an adverse media report or customer notification of a security breach or privacy breach.

ProSecure

ProSecure® acts as an extension to CyberAssurance Plus, offering higher cyber limits plus additional coverage for error and omissions and regulatory risk protection.

- **Network asset protection coverage**—Amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased, or corrupted.

  Also includes a sublimit for dependent business interruption loss—business income loss and interruption expenses incurred as a result of a total or partial interruption of a computer system operated by a business process outsource service provider or outsourced IT provider.
- **Cyber crime coverage**—Loss of money or securities incurred due to financial fraud; charges incurred for unauthorized calls resulting from use of the insured's telephone system; expenses incurred to notify customers of phishing schemes that impersonate the insured or the insured's brands, products or services, and the costs of reimbursing customers for loss they sustain as a result of such phishing schemes. Cyber crime coverage has a $100k sublimit and a $2,500 retention.
- **Bodily injury coverage extension**—Claims alleging bodily injury resulting from a privacy breach or security breach. Bodily injury coverage has a $250k sublimit and a $1,000 retention.
- **Privacy regulatory defense and penalties coverage**—Regulatory fines and penalties and/or regulatory compensatory awards incurred in privacy regulatory proceedings/investigations brought by federal, state, or local governmental agencies.
- **Breach event costs coverage**—Reasonable and necessary mitigation costs and expenses incurred as a result of a privacy breach, security breach, or adverse media report.

  Includes coverage for proactive privacy breach response costs—public relations expenses incurred in response to a privacy breach, but prior to the publication of an adverse media report.

Also includes coverage for voluntary notification expenses—expenses incurred in notifying affected parties of a privacy breach where there is no requirement by law to do so. Qualifications:

- › Available only to physicians with medical professional liability coverage through ProAssurance
- › Must not have experienced any cyber or privacy-related claims or incidents in the last five years
- › Must have a firewall and anti-virus system in place
- › Must be a solo physician practice or medical group

- **Security and privacy liability coverage**—Claims alleging liability resulting from a security breach or privacy breach, including failure to safeguard electronic or nonelectronic confidential information or failure to prevent virus attacks, denial of service attacks, or the transmission of malicious code from the insured's computer system to the computer system of a third party.

Contact **Melanie Tullos** via **email** or phone at **205-439-7967** if you have any questions related to CyberAssurance or ProSecure.

CYBER CLAIMS

Advise Your Clients to Report Cyber Claims Immediately

The sooner your clients report a cybersecurity problem, the more efficiently it can be resolved—hopefully avoiding a lot of downtime and extra expense. Advise your clients to report a cyber breach or HIPAA violation as soon as they suspect something is wrong.

Insureds can report a cyber claim through ProAssurance Claims or Tokyo Marine, HCC at these numbers:

- ProAssurance Claims Intake (8 a.m. to 5 p.m., CT) at 877-778-2524 or ClaimsIntake@ProAssurance.com.
- Tokio Marine, HCC (8 a.m. to 5 p.m., PT) at 818-382-2030 or email claims@nasinsurance.com.
- After hours or on weekends, call 888-627-8995 for assistance contracted by Tokio Marine, HCC.

How the CALIFORNIA CONSUMER PRIVACY ACT Affects Your Clients

The California Consumer Privacy Act (CCPA) took effect January 1, 2020. Any companies doing business in California—specifically those that collect consumer data online—will be affected by this law. While this is the first such act to be signed into law, other states are expected to follow suit.

The CCPA will protect over

$12B of personal information each year.

California DOJ

The CCPA has defined a set of consumer rights regarding how businesses collect, share, use, and store customer data.

- **The right to know what personal information is being collected**—Consumers can request that a business disclose the categories and specific pieces of personal information being collected by the business. Businesses must, at or before the time of collection, inform consumers what categories of personal information are collected and for what purposes they will be used. A business is prohibited from collecting more personal information beyond those purposes without providing notice to the consumer.
- **The right to know whether and to whom personal information is sold or disclosed**—A consumer may request that a business that sells or discloses the consumer's personal information identify the information collected about the consumer and the categories of information sold or disclosed to the third party.
- **The right to block the sale of personal information**—This is referred to as the right to "opt out." This right gives consumers the right to block a business from selling personal information.
- **The right to access and delete personal information**—A consumer can request that a business disclose the categories and specific pieces of personal information collected about the consumer. A consumer can also request that a business delete any personal information which the business has collected from the consumer. There are, however, limitations to this right. For example, a business is not required to delete information if the information is needed to complete a transaction with the consumer, detect security incidents, or protect against illegal activity.
- **The right to equal service and price regardless of whether privacy rights are invoked**—Businesses may not discriminate against a consumer who has exercised any rights under the CCPA. Discriminatory actions include, for example, denying goods or service and changing pricing.

CPPA Resources for ProAssurance Insureds

Tokio Marine, HCC provides resources on how to address CCPA at your agency or your client's healthcare organizations.

Tokio Marine, HCC resources are available to all ProAssurance agents and insureds through ProAssurance's SSP.

Their guide includes:

- Performing a data inventory across your organization
- Reviewing/updating your privacy policy
- Creating/modifying internal procedures to accommodate the rights above
- Reviewing service agreements with vendors with whom you share personal data
- Training your employees

To access resources, sign in at ProAssurance.com and select "Data Security Risk Resource & HIPAA" from the "Risk Management" menu.

82%

of surveyed healthcare organizations agree that digital security is one of their foremost concerns.

SI Consulting Group

What's the difference?

CYBER EXTORTION

Stealing money using the hacked person/business's computer, often by pretending to be them.

VS

CYBER TERRORISM

Using the hacked person/business's computer system to commit crimes/acts of terror.

THE HOMEPAGE

Multifactor Authentication Self-Serve Option

MFA Two Years Later

Two years ago signing into the ProAssurance secure services portal (SSP) became more secure, though a bit more involved for our users. As a necessary and responsible adaptation to the current cyber threat environment, we implemented multifactor authentication (MFA) on February 28, 2018. Since then, MFA has become mainstream and users have become accustomed to working through a more involved sign-in process, especially where finances or personal data are concerned.

First, a Recap

MFA means "we need two pieces of evidence verifying that a user is who they say they are." One of those is a "knowledge factor" (a password known only to you); the other is a "possession factor" (a code sent to your phone or some other device we know to be in your possession).

The first factor is your self-selected password.

For the second factor, users have a choice of three options:

1. **Text message**—You input your mobile number and we text you a six-digit code. Correctly entering that code into the sign-in screen grants you access.
2. **Automated voice call**—Instead of a text, an automated voice call tells you the six-digit code. This option works for folks who want to use their office phone.
3. **Google Authenticator**—Google provides a service supplying its own users' unique codes for other security services to use. You would enter the unique code provided by Google when signed into this Google application.

NOTE: Having the code emailed to you is not an option for security reasons.

As a convenience, you can select a checkbox on the sign-in page to bypass the entry of the second factor for 30 days.

New Self-Serve Option

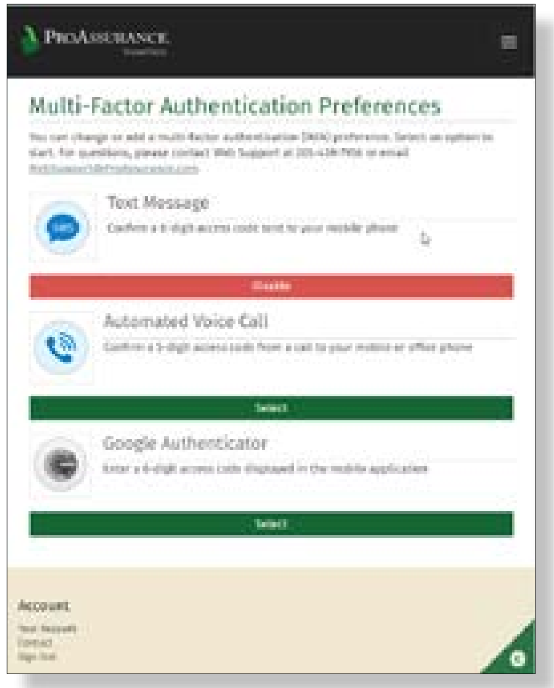
At implementation, the only support option for a user to add/remove/change an MFA option was offline: contacting the ProAssurance Web Support desk. This month we've enhanced the "Account Preferences" screen inside the SSP to enable users to self-serve.

The three MFA options are the same (call, text, or Google Authenticator). What's different is that online you can now:

- Enable or disable any MFA options
- Enable multiple options (rather than just the one you selected at set-up)
- Update your call/text number if your cell/office phone number has changed
- Relink your account to Google if you've had to reinstall the app

Steve Dapkus, *Vice President, Marketing*

Please note: *The Homepage is not an advice column. The purpose of The Homepage is marketing, communications, and business operations insights in the digital age.*



Multi-Factor Authentication Preferences

You can change or add a multi-factor authentication (MFA) preference. Select an option to start. For questions, please contact Web Support at 205-439-7956 or email WebSupport@ProAssurance.com

Text Message
Confirm a 6-digit access code sent to your mobile phone

Automated Voice Call
Confirm a 6-digit access code from a call to your mobile or office phone

Google Authenticator
Enter a 6-digit access code displayed in the mobile application

To access the MFA Preferences screen:

1. **Sign in to the SSP**
2. **Select the "Your Account" link from the top banner**
3. **Select the "Reset Multi-Factor Authentication Preference" button at the bottom of the page**
4. **Make your changes on the new MFA Preferences screen.**

We hope this change makes it just a little bit easier to manage the security of your clients' policy information. For additional questions or support with MFA issues, or any other SSP issues, please contact the Web Support team at 205-439-7956 or WebSupport@ProAssurance.com.

Two Communication Reminders…

1 New Commission Payment Notification Emails

On January 1, ProAssurance transitioned to Workday Financials for management of our back office financial processes, including commission payments.

The system sends email notifications of payments which you may inadvertently overlook or which may be routed to a spam folder by your email system until you identify the "from" email as a safe sender.

Please notify the person in your organization responsible for receiving/processing commission payments via ACH that the notification email:

- Has a "from" address of ProAssurance@Workday.com
- The subject line will begin "Remittance Release for Supplier…"
- The body of the email will begin "ProAssurance Payment Made"
- A statement for the payment will be attached as a PDF

There is no change to the payment schedule or any other processes. Other than potentially flagging ProAssurance@Workday.com as a safe email, no action is needed on your part. This is simply to notify you about a change in format for this new system-generated notification email.

If you have any further questions, please email our Accounts Payable team at Corporate@ProAssurance.com.

2 ProAssurance Email Encryption

In Q2 2019, ProAssurance began using transport layer security (TLS) to encrypt emails containing sensitive information. That might include social security numbers, credit card data, and medical information. Ninety-eight percent of ProAssurance email recipients have systems that support TLS. If the email recipient's mail server does not support TLS, the message is delivered using the secure services portal (SSP) at ProAssurance.com—just like it was under the old system.

What has changed for email recipients?

If the email recipient's server supports TLS, the recipient will not have to go to ProAssurance.com to receive their message. The email will arrive in their inbox and include [TLS Encrypted] in the subject to let them know it was secured in transit. If the email was delivered via the SSP, [SECURE] will appear in the subject line.

What do you need to do?

If your ProAssurance clients need more info, communicate what each of these designations mean. If the client is used to using the SSP to get encrypted messages, it may look like they are receiving sensitive information that isn't protected.

If you have additional questions, please contact Security@ProAssurance.com.

241 Day AMCA Breach Affects Millions

The American Medical Collection Agency (AMCA) was breached from August 1, 2018 to March 30, 2019 when the breach was finally discovered. The organization began informing their impacted clients the next day. In that time, it's estimated that approximately 20 million people had their personal, financial, and health data exposed.

AMCA's clients include several prominent vendors in the healthcare space, such as Quest Diagnostics, LabCorp, and BioReference. The company provided billing and collection services for medical tests for these organizations. As a result, over 20 million patients had their personal information exposed. This is considered to be one of the largest healthcare data breaches in history.

The hack gained access to AMCA's web payments page, which houses patient names, birth dates, addresses, phone numbers, social security numbers, and bank account/card information.

As a result of the fines for the various liabilities and fines resulting from the breach, AMCA filed for Chapter 11 protection. Additionally, dozens of hospitals and healthcare facilities who used AMCA's clients as a vendor were hit with HIPAA violations. This highlights how vulnerabilities with third-party vendors can leave a healthcare organization exposed both to cyber dangers as well as the associated liabilities.

Sources:

Lindsey, Nicole, "AMCA healthcare data breach could set a new precedent for health IT security," CPO Magazine, June 26, 2019 https://www.cpomagazine.com/cyber-security/amca-healthcare-data-breach-could-set-a-new-precedent-for-health-it-security/

"24.4M patients, 21 companies now say they were affected by AMCA data breach," Advisory Board, August 13, 2019 https://www.advisory.com/daily-briefing/2019/08/13/data-breach

7 Cybersecurity Threats That Can Sneak Up on You

Written by David Nield, Wired Magazine.
Reprinted with permission with Wired's copyright.

From rogue USB sticks to Chrome extensions gone wild, here is a quick guide to some basic risks you should look out for.

There's a certain kind of security threat that catches the headlines—the massive data breach, or the malware that hijacks your computer for a ransom—but it's also important to keep your guard up against some of the lesser-known attacks out there too.

These threats may not have the same high-level profile as an unfixable iOS bug, but they can still do some serious damage as far as your data and privacy goes. Here's what to look out for, and how to make sure you aren't caught out.

1 Rogue USB Sticks

A small USB stick may not look very dangerous, but these portable drives can carry a major threat—particularly if they've been specially engineered, as some are, to start causing havoc as soon as you plug them in. You should be very, very wary of connecting a USB drive to your computer if you're not absolutely sure where it's from.

Even if the USB stick isn't configured to release some kind of payload as soon as it's attached, it can carry disguised viruses as easily as email attachments—and experiments have shown that we're often far too curious when coming across USB sticks we don't know the origin of, so apply some common sense.

Besides being cautious, the usual rules apply to stay safe against this sort of threat: Keep your computer operating system right up to date, make sure effective security tools are installed, and keep them updated as well. If you're not sure about files on a USB drive, run a virus scan on them before doing anything.

2 Zombie Accounts

In this fast-paced, hyperconnected age, it's all too easy to forget about all the social media, language-learning, job-finding apps and sites that we've downloaded and used. But every account you leave behind gathering dust is another one that could potentially be hacked into.

As we've previously explained in detail, it's important to take the time to shut down these accounts rather than just uninstalling the associated app from our phones and then forgetting about them. If any of them should then suffer a data breach, for example, your data won't be included if you've scrubbed the account.

It's also worth running a regular audit on the third-party apps and services linked to your main accounts, like dating apps you might have hooked up to Facebook, or email apps connected to your Google account. These give hackers more targets to aim at, which is why you should regularly disconnect and delete the ones you aren't actively using.

3 Bogus Online Quizzes

You've probably seen friends and family take quizzes on Facebook to find out which Hogwarts house they'd get into, or which celebrity they're most like, and so on. They may seem like harmless fun—and some are—but they can also be used to harvest personal data that you don't really realize you're giving away.

These quizzes can and have been used to build up more detailed profiles of people and their friends, collecting not just the answers to the quizzes themselves but also other information stored in the linked Facebook accounts. Note too how often these fun quizzes ask for personal data, like the first road you lived on or the name of your pets, which could be used to impersonate you in some way.

Be wary of anything that requests personal information or personal photos from you—like the recently viral FaceApp app—or that requires a connection to one of your social media accounts: Knowing which president you're most like probably isn't worth it.

4 Untrusted Browser Extensions

The right browser extensions are able to add useful functionality and features to your daily window on the web, but these add-ons need to be vetted like any other piece of software—after all, they have the privilege of being able to see everything you're doing online, if they want to.

Pick the wrong extension and you could find it selling your browsing data, harassing you with pop-up advertising, or installing extra software that you don't actually want. We'd recommend keeping the number of browser extensions you have installed down to a minimum, and sticking only with the extensions you know and trust.

Identify safe extensions the same way you would identify safe apps: Look into the background of the developers, check the permissions that they ask for, read up on reviews left by other users, and stick to extensions that are actually useful.

5 Leaky Photo Uploads

There's nothing wrong with posting photos to your favorite social channels, but think twice about the information that other people can glean from any pictures you make public—particularly the places where you might live and work.

While a lot of apps, like Instagram and Facebook, automatically strip out the location data saved with photos, some, like Google Photos, can keep this data embedded in the file after it's been shared. Plus, whether you keep the original location data with the image, an associated check-in on social media can add the location right back in.

How is this dangerous? Well, information such as knowing where you work or which road you live on can help someone run an identity theft scam, or get past security questions on your online accounts, or visit you in person when you'd rather not see them. The less your public photos say about you, the better.

6 Smart Home Snooping

Our homes are getting smarter, which gives hackers and malware peddlers a whole new set of devices to try and target—the end result could be doors that don't stay locked or home security camera footage that's viewed by more people than you'd like.

Keeping your smart home secure starts with what you buy: It's a good idea to stick to well-known, established brands with a strong track record in hardware, as much as possible. After that, make sure both your smart home devices and your router—which acts as a gateway to them all—are kept up to date with the latest software. Most reputable smart home devices do this automatically, another good reason to stick with brands you trust.

If your smart home devices and accounts do need passwords, make sure you don't stick with the default. Instead, pick a long and difficult-to-guess password that you aren't using anywhere else, and turn on two-factor authentication, if available, as an extra layer of protection.

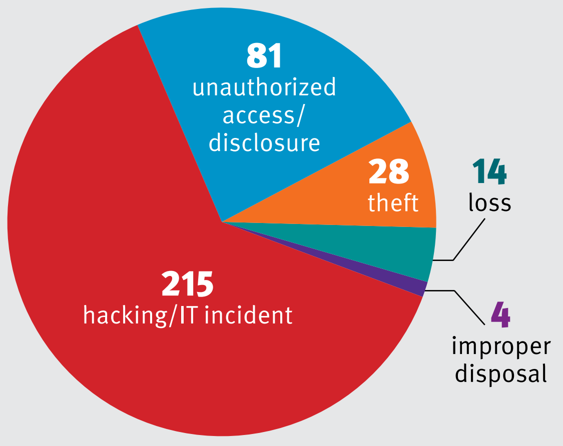
7 Malicious Charging Cables

The standard charging cables that come with your gadgets are designed to power them up, and perhaps sync some music when needed—but specially engineered cables that look very similar can do much more than that.

Take a look at these fake Lightning cables now capable of being mass-produced, cables that look just like the genuine products but which can give hackers remote access to a device once they're plugged in. All that the end user has to do is use a doctored cable, then agree to "trust this computer," a common alert that's easy to dismiss without a thought.

The fix is to only use the cables that come with your devices, or from reputable sources—something you should do anyway for the well-being of your gadgets. As with USB sticks, don't assume any cable that you find lying around is legit.

Return to **Table of Contents**



2019 HIPAA CASES UNDER INVESTIGATION

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) keeps a list of all breaches affecting over 500 individuals. In 2019 the OCR listed 342 healthcare providers in a total of 45 states. Texas was the hardest hit with 46 entities.

Of the 342 breaches, there were:

- 81 unauthorized access/disclosures
- 28 thefts
- 14 losses
- 4 improper disposals
- 215 hacking/IT incidents

In total, 22,588,461 individuals were affected by the incidents on the list. As of January 31, 2020, the OCR already has 29 entities listed for 2020.

Visit the OCR breach portal to view cases currently under investigation.

CYBER ACRONYMS EXPLAINED...

Internet of Things (IoT)

The networking capability that allows information to be sent to and received from objects and devices (such as fixtures and kitchen appliances) using the internet.

Operating System (OS)

Software that controls the operation of a computer and directs the processing of programs (as by assigning storage space in memory and controlling input and output functions).

Merriam-Webster, accessed February 14, 2020.

Recommended Cyber Articles

Instead of our usual healthcare industry article roundup, here are articles to support your knowledge of cyber liability trends. Please let us know if there are other topics you would like us to monitor at AskMarketing@ProAssurance.com.

1. **Number of data breaches jumped 17% in 2019: 3 things to know**—Most breaches in 2019 were from cyber hacks, but unauthorized access to information was not far behind. Written by Mackenzie Garrity, Becker's Health IT & CIO Report, January 29, 2020.
2. **Government issues warning over a critical medical device**—Computer programs used to monitor patient vital signs could be vulnerable to cyber attacks. Written by Dick Uliano, Washington's Top News, January 27, 2020.
3. **Ransomware targeting health systems in more "sophisticated" ways**—It is becoming more common for hackers to evaluate vulnerabilities at specific hospitals and create a customized attack. Written by Jessica Kim Cohen, Modern Healthcare, January 24, 2020.
4. **How fast can a new internet standard for sharing patient data catch fire?**—Technology companies and healthcare entities are working together to develop Fast Healthcare Interoperability Resources to make it easier to share health information across platforms. Written by Janet Rae-Dupree, Kaiser Health News, January 22, 2020.
5. **Cybersecurity impact of Microsoft's end to Windows 7 support**—56 percent of healthcare entities still use Windows 7; failing to upgrade to a supported system could leave these organizations open to serious cybersecurity threats. Written by Jessica Davis, Health IT Security, January 13, 2020.
6. **Five ransomware facts you need to know about**—Fourteen cyber experts were interviewed for their opinions on ransomware attacks. A majority agreed the problem is getting worse, and establishing preventative protocols is essential to keeping your organization safe. Written by Dane Greisiger, Risk & Insurance, December 9, 2019.
7. **Is blockchain a cure for healthcare data breaches?**—Blockchain technology allows data to be viewed but not copied. This may help healthcare organizations keep data secure without losing the ability to share essential health information amongst providers. Written by Jia Jen Low, TechHQ, January 29, 2020.
8. **Five healthcare tech trends to watch in 2020**—Technology is rapidly being incorporated into preventative medicine and primary care, but physicians still struggle to decide which tech tools are worth the investment. Written by Kevin Joy, HealthTech, December 19, 2019.
9. **Cybersecurity in 2020: IoT medical devices, ransomware, legacy OS**—Large scale data breaches, increased penalties for HIPAA violations, and a noticeable increase in ransomware attacks dominated cybersecurity discussions in 2019, including issues with Internet of Things (IoT) medical devices and legacy operating systems (OS). They project serious concerns for data security in 2020. Written by Jessica Davis, Health IT Security, December 12, 2019.
10. **Which employees pose the biggest cybersecurity risk? You might be surprised**—The common "tech-savvy" stereotypes are wrong—younger generations have more of a cybersecurity education gap than their older counterparts. Written by Courtney DuChene, Risk & Insurance, December 10, 2019.
11. **Lessons learned from a targeted ransomware attack**—A strong response strategy is every bit as important as taking preventative measures against ransomware attacks. Written by Robert Garrett, Modern Healthcare, December 20, 2019.
12. **Healthcare cybersecurity market—industry trends and manufacturing requirements studied in a new report**—Cybersecurity technology is largely growing due to increasing threats, which are becoming increasingly damaging and sophisticated. Dagoretti News, January 21, 2020.
13. **So far, under California's new privacy law, firms are disclosing too little data—or far too much**—The CCPA is considered the most far-reaching online privacy law, and companies and consumers alike are struggling to understand how to adapt to it. Written by Greg Bensinger, The Washington Post, January 21, 2020.

MEDICAL PROFESSIONAL LIABILITY

Market Dynamics 2020

As part of our efforts to monitor ongoing market conditions, we have curated the following recent industry articles.

1. **Change in Diagnosis**—"Observers say the medical liability market is beginning to harden as higher jury awards, eroding tort reform sink in." Industry leaders, including ProAssurance's CEO Ned Rand, weigh in on the state of the market. Written by Timothy Darragh, Best's Review, February 2020.
2. **Reinsurance prices set to increase: Fitch**—Fitch Ratings, Inc. reports that April and June reinsurance renewals are likely to see additional price firming, though there were limited increases in January. Written by Matthew Lerner, Business Insurance, January 22, 2020.
3. **Social inflation adding pressure on loss costs for insurers: Analysts**—Analysts from Credit Suisse estimate that the impacts of litigation finance are adding over $3.8 billion in additional costs annually to the U.S. court system. Written by Luke Gallin, Reinsurance News, January 27, 2020.

SPOTLIGHT ON RISK RESOURCE
NEW 2020 Live Loss Prevention Seminar for Physicians

Registration has already begun for this year's live loss prevention seminars in 12 states and D.C. Our new seminar for physicians, *Hindsight 2020*, discusses factors influencing juror decision-making in medical malpractice lawsuits.

The medical professional liability industry is currently experiencing an increase in the severity of jury verdicts. Jurors are instructed not to base their verdicts on what was learned or discovered after the incident. While jurors are not permitted to use hindsight in arriving at their decisions, they often do.

Participation in this seminar will better enable attendees to:

- Understand factors that influence juror decision-making in medical professional liability lawsuits
- Identify risk issues that may increase the likelihood of a high verdict

Physicians who attend the full session are eligible for 2.0 AMA PRA Category 1 Credits and may qualify for a five percent premium credit at policy renewal. Certain exclusions from premium credit eligibility are noted in the physician seminar brochure.

We will send brochures and schedules to insured physicians and previous attendees approximately eight weeks in advance of their state's first seminar date.

Your clients can view seminar dates and register at ProAssurance.com/Hindsight.

2020 Schedule

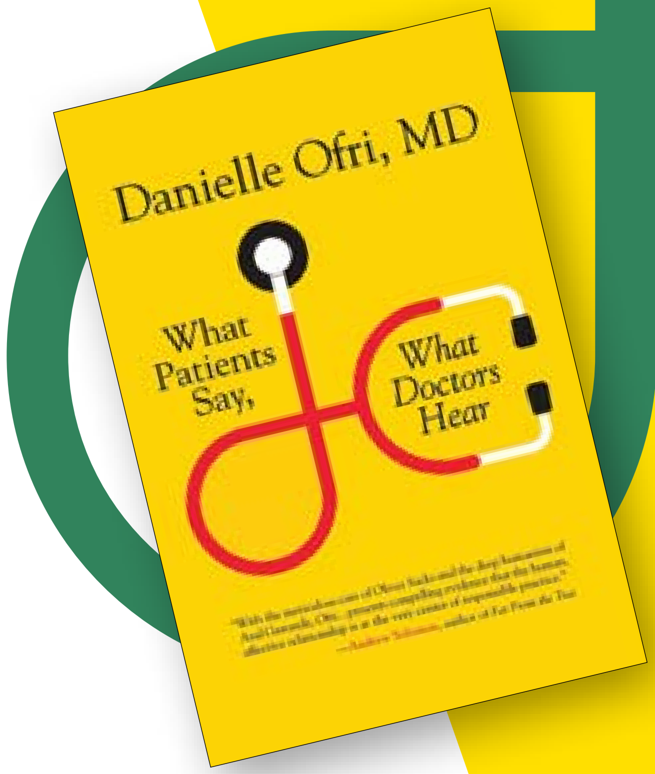
Location	Brochure Mailing Date	First Seminar
Alabama	January 17	March 10
Florida	January 31	March 26
Illinois	January 31	March 26
Indiana	February 28	April 21
Kentucky	May 29	July 21
Michigan	April 10	June 3
Mid-Atlantic Region (DC, DE, MD, VA)	February 7	April 2
Missouri	March 13	May 7
Nevada	March 20	May 14
Ohio	February 7	April 2

Retention Campaign Targets Insureds at Renewal Time with Complimentary Book Offer

Each year we send retention mailings to MPL insureds* the quarter before their renewal date in an effort to share knowledge, support patient safety, and retain superior relationships.

Mailings typically offer insureds a chance to request a complimentary resource with tips for avoiding risk. This year's we're offering the choice of a paperback or audiobook copy of *What Patients Say, What Doctors Hear* by Danielle Ofri, MD.

* *Excluding Certitude insureds.*



About the book...

What Patients Say, What Doctors Hear

The single most powerful diagnostic tool is the doctor-patient conversation, which can uncover the lion's share of illnesses. However, what patients say and what doctors hear are often two vastly different things.

Patients, anxious to convey their symptoms, feel an urgency to "make their case" to their doctors. Doctors, under pressure to be efficient, multitask while patients speak and often miss the key elements. Add in stereotypes, unconscious bias, conflicting agendas, and the fear of lawsuits and the risk of misdiagnosis and medical errors multiplies dangerously.

Though the gulf between what patients say and what doctors hear is often wide, Dr. Danielle Ofri proves that it doesn't have to be.

Reporting on the latest research studies and interviewing scholars, doctors, and patients, Ofri reveals how refocusing conversations between doctors and their patients can lead to better health.

© 2017 Danielle Ofri, MD • 248 pages

New this year

Instead of sending two different promo offers, we are offering one book and sending reminder mailings to nonrespondents.

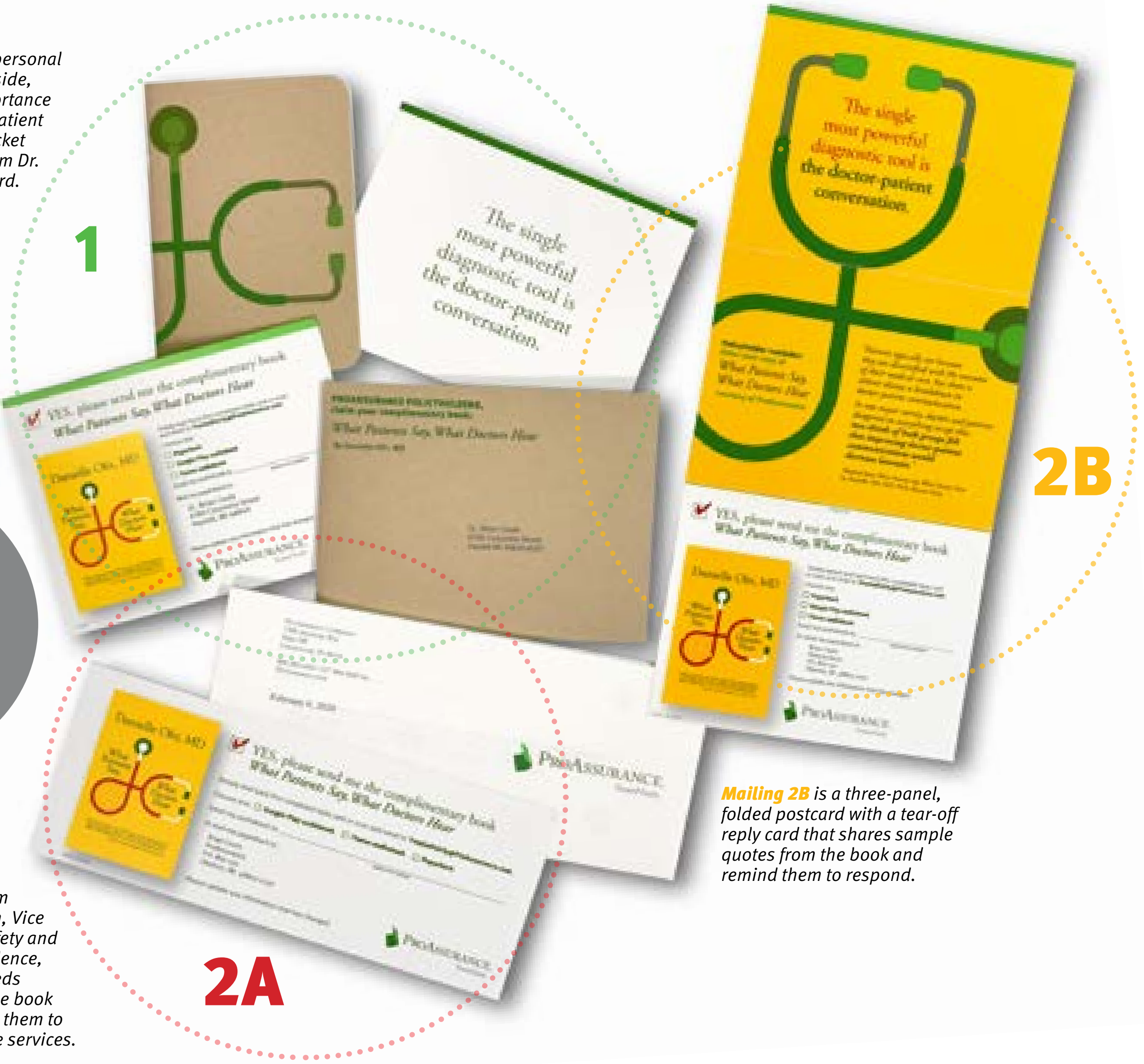
We'll be monitoring results of each stage of the mailings and adjusting the campaign as we see the effectiveness of each method. We will also compare responses to actual renewals numbers to determine the correlation.

Note: We are no longer sending agent bulletins for each mailing. Instead, please review the samples in the Agents' section of the SSP under "Insured Communications."

Campaign at a glance

The first mailing stage uses a proven format from prior years—a small brown envelope with a folded note from ProAssurance's Chief Medical Officer Dr. Hayes Whiteside, a reply card, and a custom pocket note. The second mailing is an A/B test of two direct marketing approaches. A final reminder email will conclude the campaign.

The mailings go out approximately one month apart—once someone responds, they are removed from the follow-up mailings.


1
2A
2B
The single most powerful diagnostic tool is the doctor-patient conversation.
ProAssurance

Mailing 1 includes personal note from Dr. Whiteside, reinforcing the importance of effective doctor-patient communication, pocket note with quotes from Dr. Ofri's book, reply card.

Mailing 2A is a letter from Lisa VanDuyn, Vice President Safety and Service Excellence, asking insureds to reply for the book and referring them to Risk Resource services.

Mailing 2B is a three-panel, folded postcard with a tear-off reply card that shares sample quotes from the book and remind them to respond.

The first mailing went out to March/April/May renewal dates on January 13 and has already exceeded projections with a ***14.2 percent response rate*** (10 percent is considered very good).

Please email **AskMarketing@ProAssurance.com** if you would like:

- To be on our retention mailing list
- A copy of the book *What Patients Say, What Doctors Hear*
- A list of your clients who respond to the mailing

Thank you for all you do to retain and engage our insureds.

WHAT'S THE BIG QUESTION?

A place to share your thoughts and expertise regarding industry issues.

Each month, The Big Question asks the ProAssurance community for input on timely medical professional liability topics. Our goal is to provide our agents, insureds, colleagues, and professional connections with a place to share anecdotes and resources that make it easier to discuss the complexities of MPL market dynamics and insurance solutions.

We're interested in your answers and comments to each monthly question and would like to know what questions you would like to see asked. Submit both at ProAssurance.com/BigQuestion.

The Big Question

February 2020
Cyber Liability

Have you or your clients ever experienced a ransomware attack or similar event?

Keeping "Cyber Vigilant"

At SilverStone Group, we have spent the better part of a decade building a culture of safety and awareness around cybersecurity. Cyber liability insurance consulting has been an area of expertise for us for the past 11 years. Many, many clients have come to us for coverage and guidance: some because they were hacked, others because they wanted help quantifying or understanding their exposures. We help clients see the full picture, including where insurance is and isn't the solution.

Many of our insured clients have also experienced cyberattacks, and, luckily, cyber insurance helped them recover from their losses. The interruption to daily operations is always more than anyone expects.

Cybercrimes are a moving target. As soon as you get one social engineering scheme identified, criminals are figuring out a new one. They are becoming increasingly strategic. Many are going after the mission critical companies that our healthcare clients depend on—electronic medical record (EMR) vendors and record storage services—instead of the healthcare organizations themselves. If a supplier with multiple healthcare clients is breached, more records are potentially exposed.

Just as you can't delegate managing patient data in your EMR, you can't delegate away your responsibility for cyber security to third parties and software. Your people are your first line of defense against cyberattacks. You have to constantly train and reinforce the importance of caution to help prevent threats from taking hold. It takes time and continued vigilance because the threat is always changing.

John Marshall, Principal

SilverStone Group, a part of HUB International

AI Concerns

Artificial Intelligence has disrupted the healthcare space. As an example, in a 2019 study from Google and Northwestern Medicine, their newly-developed deep learning system was able to outperform radiologists in detecting malignant lung modules. But like all technology, AI is not perfect and has its limitations. Some risk management concerns include cybersecurity risk. When testing this radiology AI technology, it was discovered that hackers could alter the images of the radiology scans; moving pixels could make nodules undetectable, or create an inaccurate cancer diagnosis. The concerns and safety implications of this issue are significant.

Mario Giannettino, Esq.

Mario Giannettino is a partner at Kaufman Borgeest & Ryan LLP in the firm's Medical Malpractice, General Litigation, and Nursing Home and Long-Term Care practice groups. He recently spoke at ProAssurance's annual Risk Resource Conference in Las Vegas, Nevada. See more about the conference and Mario's presentation in next month's issue.

The Next Big Question

March 2020
Conferences

What life hacks do you have for attending conferences?

Please submit your observations by visiting **ProAssurance.com/BigQuestion**.

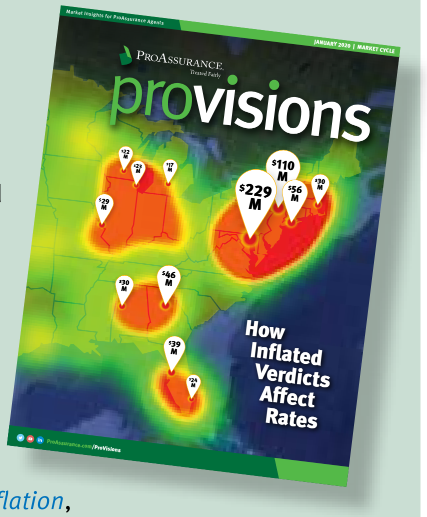
Is Your Practice Cyber Secure?

Risk Resource's latest issue of its *Medical Risk Resource Advisor* newsletter is available at ProAssurance.com/Newsletters. This newsletter for ProAssurance-insured physicians provides insight into the cyber risks today's medical practices are facing.

In Case You Missed It...

January 2020 *ProVisions*

Did you receive your email copy of the "Market Cycle" *ProVisions* issue last month? One of our most popular issues, it tackles changing market conditions and provides tools you can use to help your clients understand how the hardening market affects them. Top articles include *The Homepage: MPL Market Dynamics 2020 Explained*, *Shock Verdicts Fuel Social Inflation*, and *Tales from Prevous Hard Markets*.


Market Insights for ProAssurance Agents
JANUARY 2020 | MARKET CYCLE
ProAssurance
Treated Fairly
provisions
$22 M
$23 M
$17 M
$29 M
$110 M
$229 M
$56 M
$30 M
$30 M
$46 M
$39 M
$24 M
How Inflated Verdicts Affect Rates
ProAssurance.com/ProVisions

To read any of these articles or the full newsletter, visit ***ProAssurance.com/ProVisions*** and sign in.

Telemedicine Today—How are we Doing so Far?

ProAssurance's Gina Harris, Regional Vice President, Claims, was recently featured in *Inside Medical Liability* discussing the state of telemedicine.

"While the evolution of telemedicine takes shape, healthcare providers must remain cautious and careful, and pay close attention to the unique opportunities and challenges brought about by this fascinating new way to provide quality healthcare."

View Gina's excerpt at **MPLAssociation.org**.

PROASSURANCE LEADERSHIP CIRCLE

OCTOBER 4-7, 2020

Streamsong Golf Resort, Bowling Green, Florida

Doctors' Day was created to establish a dedicated time to say thank you to physicians for the vital work they do. Don't forget to reach out to your physician clients!

ProAssurance
Treated Fairly

provisions

Looking Ahead

Upcoming *ProVisions* themes include:

- **Conferences (March)**—An inside report on ProAssurance's Risk Resource and Claims conferences in February 2020.
- **Crisis Communications (April)**—This issue will contain a full guide to setting up a PR plan following negative events like a high malpractice verdict, cyber breach, inclement weather, and more you can share with your physician practice and hospital clients.
- **Ratios (May)**—Insurance is a ratio-driven industry. ProAssurance leaders will discuss the ratios they watch closely, and what is important about them.

Email your suggestions for future themes to **AskMarketing@ProAssurance.com**.

To subscribe or see previous issues, visit ProAssurance.com/ProVisions.