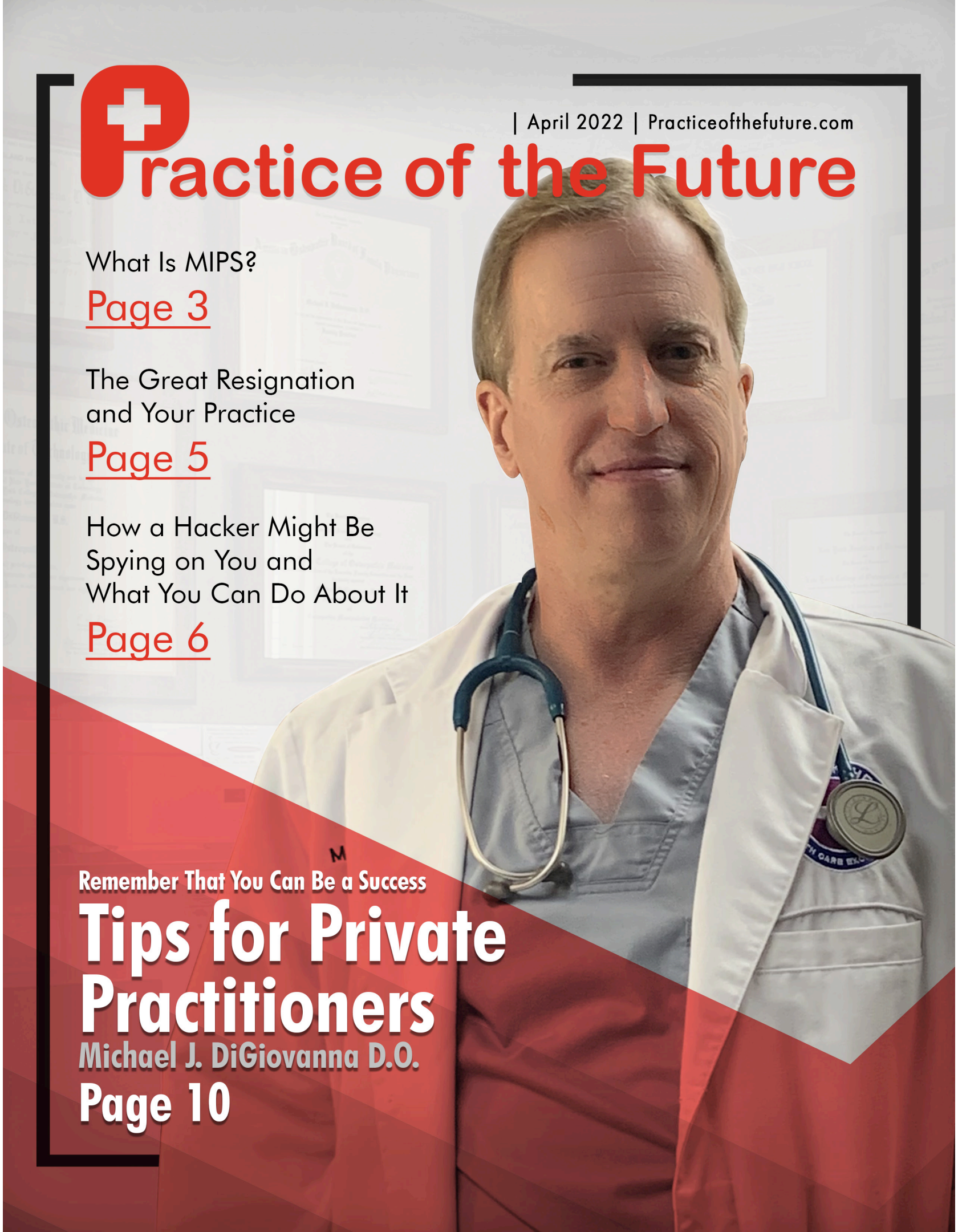
| April 2022 | Practiceofthefuture.com

Practice of the Future



Remember That You Can Be a Success

Tips for Private Practitioners

Michael J. DiGiovanna D.O.

Table of Contents

The Practice of the Future Team

Publisher and Founder:
Robert Gabriel

Senior Editors:
Andersen Silva,
Justina Kopec

Art Director/Design:
Sundas Aziz

Research Editor:
Monica Rivera

Featured Provider

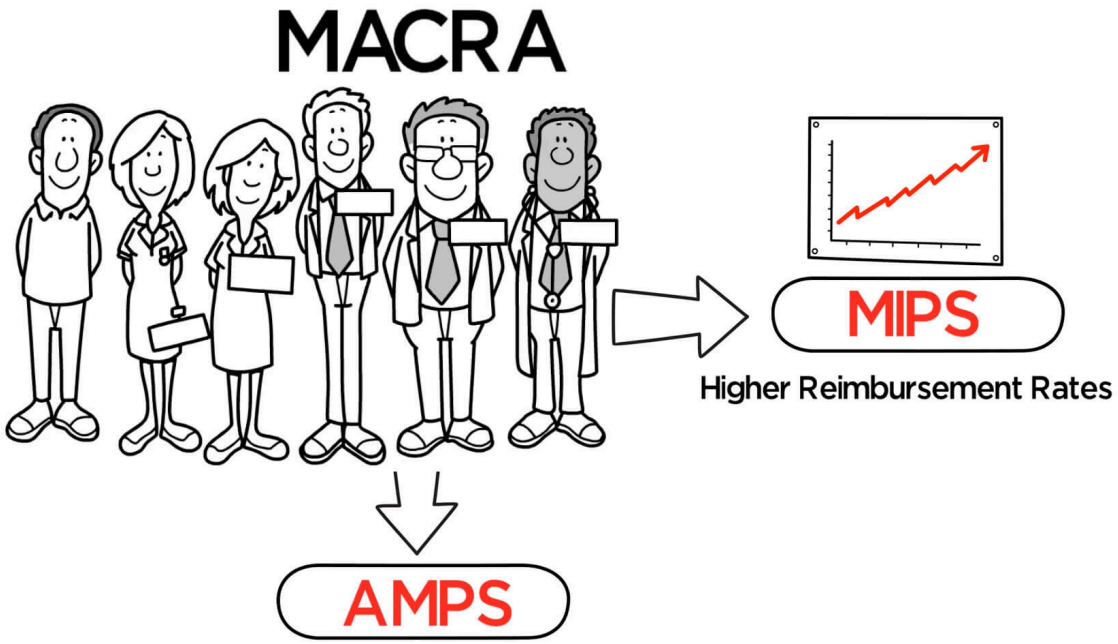
DiGiovanna Family Health

Michael DiGiovanna of DiGiovanna Family Health & Wellness Center discusses his experiences working within a larger medical group and then transitioning back to private practice, sharing some very useful tips for private practitioners.

Read full story inside:
Page 10

Get your practice featured in the next issue

practiceofthefuture.com/get-featured



What Is MIPS?

by Yasmin Yasser

MIPS and MACRA are terms that all doctors nowadays should be familiar with. Following is a quick explanation.

The Medicare Access and CHIP Reauthorization Act of 2015, or MACRA, is U.S. healthcare legislation that provides a new framework for reimbursing clinicians who successfully demonstrate value over volume in patient care. It used to go by the name PQRS until January 2017, when the Quality Payment Program went into effect and pay ment increases were no longer set for Medicare services by the Sustainable Growth Rate (SGR) law. The idea is to encourage and reward quality over quantity.

MACRA set up the Quality Payment Program, or QPP, with two payment tracks emhasizing value-based payment models. The Merit-Based Incentive Payment System, or MIPS, is the more popular track.

Prior to MACRA, clinicians used to have their payments adjusted according to the SGR formula. However, the MIPS program applies payment adjustments to the Medicare part B claims with incentives of up to 9%.

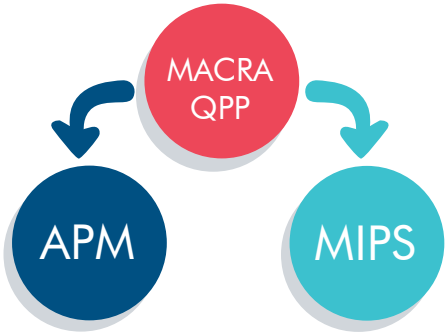
So, how do I get in on the game of incentives?

Well, you probably won't believe me when I tell you that you're probably already doing the work! All that you need is to document and report the right way!

The MIPS program is an annual program comprised of four categories:

- Quality: 30% of MIPS
- Improvement activities: 15% of MIPS
- Promoting interoperability (used to be known as meaningful use): 25% of MIPS
- Cost: 40% of MIPS

If eligible for MIPS reporting, you will need to decide on which measures to report on for each category and use your EHR software to obtain the reporting data. Ready to jump on the bandwagon yet?



Letter from the Editor

I was supposed to be an astronomer.

At least, that was the plan when I was in grammar school. I loved space and the stars, and signed up to get NASA publications on the Space Shuttle and Viking and Voyager missions (yes, I am that old). I loved the original "Cosmos" presented by Carl Sagan, I had my own telescope, and I was convinced that I'd end up working with the stars. No, not those stars.

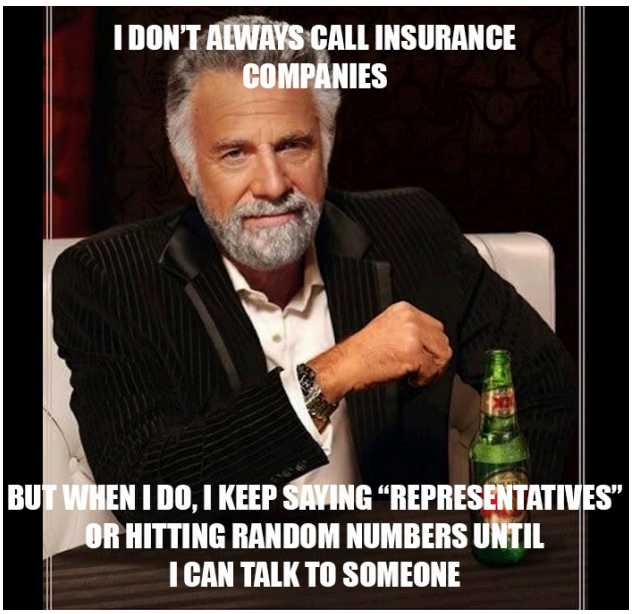
I still love to gaze at the night sky, and I'm thrilled to have seen planets and moons and comets and meteors, sometimes with the naked eye and sometimes with the help of additional lenses... but I ended up taking a different path. From a retail store's customer service area to a bank's bulk currency department to inventory control and then layout for an embroidery manufacturer, I gathered knowledge and experience and friendships.

And then I became an MIS manager, and hey, turns out I actually like working with computers and networks and data, and I'm not half bad at it, either. Now I'm involved in data services and tech support (and some IT and marketing, we like to wear multiple hats here) for Microwize Technology when I'm not working on this magazine. It's not stargazing, nor would I have ever guessed I'd end up here, but it is worthy and noble and fulfilling work. I help doctors and other medical professionals help patients, by keeping their systems and databases running and secure and accessible. Knowing that makes me feel proud and humble at the same time, part of a team of people that is doing good for other people.

I'm still looking forward to May's total lunar eclipse, though, hope you are, too. Thanks for letting me introduce myself!

Andersen (Andy) Silva, senior editor

Humerus Corner



The Great Resignation and Your Practice

by Robert Gabriel

Some people refer to it as the "Big Quit," while others call it the "Great Resignation."

If you missed the "60 Minutes" segment on Sunday, January 9th, it discussed why more Americans are quitting their jobs. Many businesses are having difficulties finding skilled workers to hire. To summarize the segment:

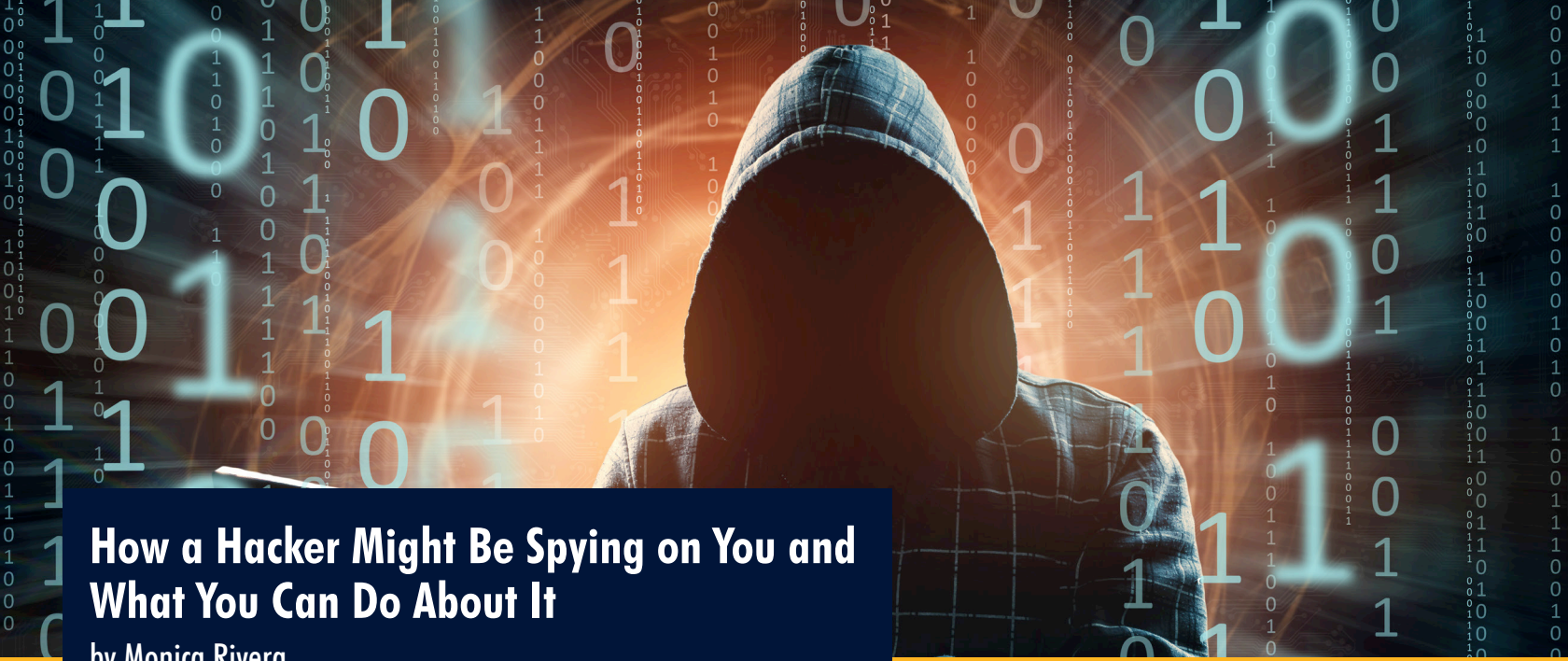
More and more "baby boomers" have decided to retire and not go back to work

Many moms decided to stay home and not go back to the workforce

Others relocated to areas with more affordable housing, safer communities away from the big cities, avoiding the hustle and bustle with the option to work remotely

Some people even seem to think the Great Resignation is the result of 'generous' stimulus and unemployment benefits from the government. The bottom line is, your practice needs to fill vacant positions and run your business in the most effective ways. Microwize has been helping practices and billing services with remote employees for any responsibilities that can be handled remotely. Microwize is offering virtual employees who can help your medical practice with front desk or back-office functions. These include answering calls and taking appointments, following up with accounts receivable, running reports, and printing patient statements.

A fully qualified, medical billing certified and HIPAA-trained employee is ready to join your team and hit the ground running. Whether you need coverage for someone on a leave of absence or workforce augmentation, a Microwize remote employee is your best choice. At only $525/week for a full-time employee + a part-time supervisor, it is the best thing you will do for your practice. Never worry about payroll, sick time, vacations, medical or dental insurance, or the Great Resignation… a Microwize remote employee is an amazing option. Don't compromise, go Microwize.



How a Hacker Might Be Spying on You and What You Can Do About It

by Monica Rivera

Today, hackers can gain access to your smartphone through downloaded apps or Wi-Fi networks, and this allows them to monitor your activities. Learn how to protect yourself and prevent hackers from stealing passwords, spying on you, and collecting your personal data.

10 Tips That'll Keep Your Data Safe in Cyberspace

1. Keep your operating systems up to date.
Keeping your operating system and apps up to date is one of the best things you can do for your computer's security. Whenever Microsoft or Apple fixes a vulnerability, it's critical that you apply the update as soon as you can. If you're one of the many who wait weeks or months, then you're putting yourself in harm's way.

2. Create strong, unique passwords.
Create strong and unique passwords to access your devices, operating system, and applications. It's a basic step in the process of keeping your devices secure, but most people don't do it. You should use capital letters, symbols, numbers, and different kinds of characters to make them stronger, and most importantly, don't use one password across multiple (or all!) accounts. Keeping track of so many accounts and passwords is tedious, so we recommend using LastPass, a free and secure way to manage all of your passwords in one place.

3. Use MFA (multi-factor authentication).
Use multi-factor authentication wherever possible as an added level of protection when you're signing in and out of your accounts. This is where you receive a code via text message or E-mail or authenticator app (like those from Microsoft or Google).

4. Pay attention to installation screens.
It's here that you'll find important information regarding third-party software that may also be installed – things like toolbars, add-ons, or adware. This seems like a minor step, but can be critical. Be sure to keep an eye out for this before you move on or click "Next."

5. Avoid using peer-to-peer (P2P) file-sharing.
Getting files from BitTorrent could be putting your computer at risk. Downloading items such as movies or TV series in this manner exposes your computer to all machines that are also downloading the same files you are. This information exchange exposes you to keygens, cracks, worms, and other harmful viruses that compromise your data, privacy, or both. As an alternative to BitTorrent, using UseNet or BBS (Bulletin Board Systems) is a better way to accomplish the same thing.

How A Hacker Might Be Spying On Your Computer Right Now And What You Can Do About It

by Monica Rivera

6. Use a browser-based content blocker.
Content blockers such as Browser Guard, AdGuard, or DuckDuckGo can help to reduce ads, phishing, trojans, or any other content that an antivirus alone may not detect.

7. Slow down.
Take a moment to think about what you're clicking on or when you're reacting to unexpected messages.

8. Be alert for people trying to trick you.
I'll never forget the day I received an email from "IKEA" asking me to confirm sensitive information by clicking a link. As soon as I saw that it was IKEA, I immediately realized it was a scam, and knew not to click on any links. A trusted company will never ask you to verify sensitive information by clicking an external link the same way the IRS will never call you to verify your Social Security number. Thankfully, I had also educated myself on social engineering tactics, so the ploy to gain access to my computer so they could steal private data or take an unsuspecting victim for money failed.

9. Never open unexpected attachments.
Before you do, first check the sender's email and make sure the address matches the trusted company's address exactly. Second, beware of emails with generic introductions such as 'dear customer.' Spelling or grammatical mistakes are also a sign that the email is a scam. No matter who you think it could be from, always be suspicious of an email that asks for your personal information or has unexpected attachments. Contact a colleague or someone from your IT department for a second opinion if you're not sure.

10. Back up your data frequently.
Backing up your computer to an external hard drive or solid state drive (SSD) is a good practice, but it's only as good as the backup. If your backup is incomplete, fails frequently, and cannot be properly restored, it won't help you if you lose your valuable data. A successful backup strategy will also save you time and money in the unfortunate event that your data is lost.

For most of us, it's impossible to be 100% certain that our systems will never fail. However, by applying common sense and taking some reasonable precautions, you can keep your data secure and limit the impact from any threats that do occur. In addition to the common practice of backing up files and documents on a regular basis, there are a few additional steps and best practices you can take up to protect yourself against the most common security risks. Remember, forewarned is forearmed!

Vulnerabilities Impacting Many Medical Devices

by Andersen Silva

Two separate reports this March note security vulnerabilities affecting medical and other "Internet of Things" devices. Forescout's Vedere Labs and CyberMDX announced the discovery of seven vulnerabilities, three rated critical by CISA. These Access:7 susceptibilities affect Parametric Technology Corporation's Axeda agent. PTC's Axeda platform is used to remotely access and manage over 150 devices from more than 100 IoT vendors.

The list of affected devices includes many related to healthcare, making the threat more severe. Attackers exploiting the Access:7 vulnerabilities could obtain sensitive information, shut down the Axeda agent, or even control and run commands on a device. Bad actors could modify patients' records and test results. PTC has released patches for the affected older versions (below 6.9.3) of the Axeda agent. The company also favors the ThingWorx platform over Axeda now; however, many customers continue to use Axeda.

Vulnerabilities in Infusion Pumps

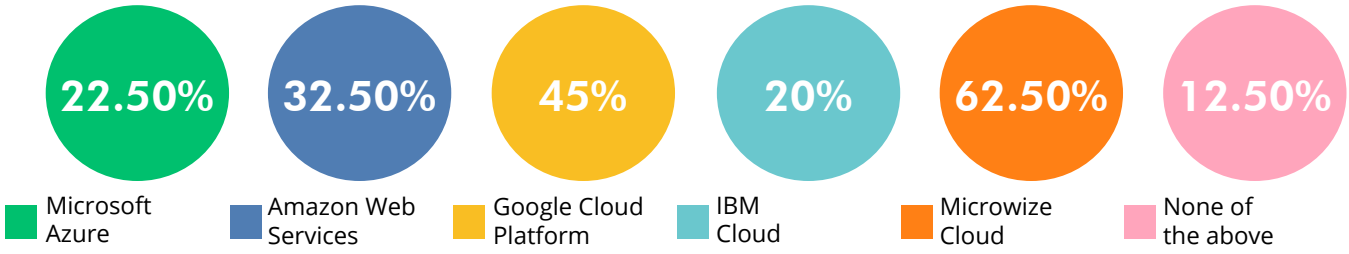
Separately, Palo Alto Network's Unit 42 threat intelligence team released a report regarding security flaws impacting infusion pumps. They examined more than 200,000 pumps used in hospitals and other healthcare organizations with Palo Alto's IoT Security for Healthcare. 75% of these infusion pumps were discovered to be "at heightened risk of being compromised by attackers." More than half were susceptible to two vulnerabilities disclosed in 2019, one rated critical and one high.

Infusion pumps administer fluids like medications and nutrients into a patient's body in controlled amounts. Healthcare organizations use them widely, but many of these IoT connected devices are older and unable to receive relevant security updates. Because of this, attackers could access sensitive information or cause a device to stop responding. Malicious actors exploiting these vulnerabilities could severely impact patient care and operations at hospitals and clinics.

Healthcare organizations must remain diligent about security software and updates to devices and firmware. Cybercriminals constantly seek vulnerabilities and backdoors to exploit. Microwize offers healthcare cybersecurity services to help secure networks and devices.

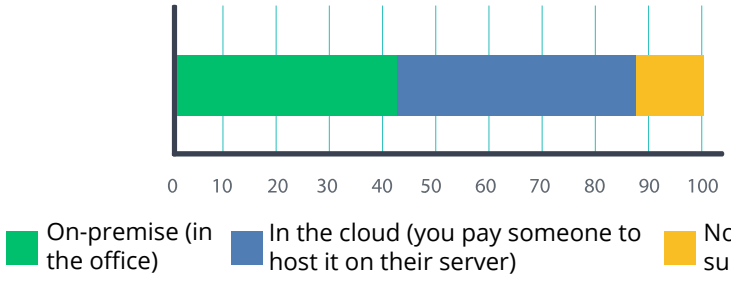
4 Questions About Cloud Based Services

Q1: Which of the following cloud services have you heard of? (select all that apply)



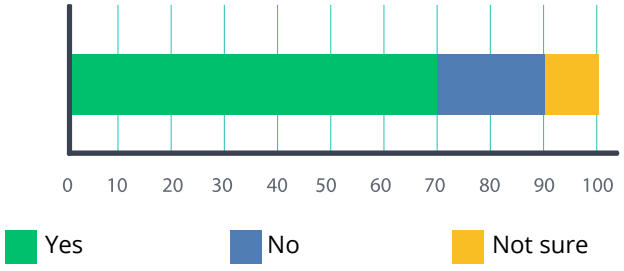
62.50% of healthcare providers are most familiar with Microwize Cloud

Q2: Where is your practice management and/or EHR software hosted?



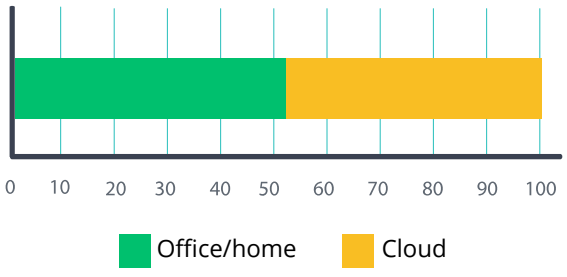
45% of healthcare providers have their practice management/EHR software hosted in the cloud

Q3: Do you use, or have you used, any applications or services that are cloud-based?



70% of healthcare providers have used applications or services that are cloud-based

Q4: Do you think protected, confidential data is more secure in your office or home, or in the cloud?



51.28% of healthcare providers think that their confidential data is more secure in the office/home

7 out of 10 surveyed providers use or have used cloud-based applications or services, and almost half are using cloud-based practice management/EHR software. 51% feel their data is less secure in the cloud, but really your data's security depends less on where it's stored, and more on the systems and protocols in place to safeguard it and back it up, and who is monitoring and maintaining them.

Tips for Private Practitioners

Featured Provider: Michael J. DiGiovanna D.O.

We spoke with Dr. Michael J. DiGiovanna at DiGiovanna Family Health & Wellness Center in Massapequa, NY about his experiences with joining a hospital-owned group, and then going to a private practice!

Q: What is the most rewarding aspect of practicing medicine as an independent physician?

A: The most rewarding aspect of practicing medicine as an independent physician is the autonomy. As an independent physician, I am able to be very flexible and adapt to the ever-changing environment in medicine. I am able to purchase equipment or tests quickly, as needed by the current climate. I am able to hire and terminate employees to better serve the practice and patients. I can make all my own decisions and not have several layers of administration to deal with.

Q: What was the deciding factor for you to leave the hospital-owned medical practice?

A: I was with a larger medical group for about 2 1/2 years, and after the "honeymoon period," found working with them to be cumbersome, unrewarding, and made me unhappy in my everyday practice. All decision-making was taken away from me, and I was scrutinized in every aspect of my daily medical practice, having to achieve targets with artificial parameters and try to satisfy competing priorities.

Q: What would you say to physicians on the verge of joining a hospital-owned group?

A: Think very carefully and do all of your due diligence before joining any hospital-owned group. Speak to other physicians and practitioners in the group and see what their opinion is. Do all the work upfront before you join. And make sure you negotiate a reasonable exit strategy in case the deal does not work out for you.

Q: Is there a difference in the care you are able to provide to your patients since the transition?

A: There is a huge difference in the care I am able to provide since the transition. I am able to work closely with my front desk to fine-tune all aspects of appointment-making and message-taking to satisfy my patient population. With a large and disconnected call center, I had no control over overbooking, the way they spoke to my patients, booking rules, and corresponding with me when a patient needed to be seen and there was no room in my schedule.

Q: What was the most difficult part of your transition back to private practice?

A: Ease of access to capital is the most difficult part of the transition back to private practice. Most banks look askance at independent medical practices and consider them too risky. Cash flow is often slow or difficult to manage due to vagaries in insurance billing cycles. This makes handling the most expensive part of most medical practices, payroll, difficult to manage at times.

Q: How did you ensure that your practice would successfully operate as a business?

A: In order to ensure the long-term viability of my independent medical practice, I stay very involved in every single aspect of the running of the practice. I review every bill that goes out, every explanation of benefits that comes in, I try to negotiate with and work with the best vendors I can find from IT to payroll processing to medical and office supplies, and everything in between.

Q: What advice would you give to physicians on the verge of practicing on their own?

A: If you are thinking about going into private practice on your own, do your homework first. Every successful business starts with a good plan, followed by proper execution and a lot of hard work and owner involvement. Surround yourself with good infrastructure, and be prepared to put every ounce of effort into your venture. Remember that you can be a success if you believe you will be a success.

EMR vs EHR?

Understand the Difference

by Monica Rivera

EMR vs EHR? To begin differentiating between the two, it's important to understand the shift in the medical industry. The growing advancements in the medical field within the past 50 years have tremendously improved our medical knowledge, as well as transformed research and development for treatment options. Because of this, those with chronic conditions have been living much longer. While this is good news, it posed a need for addressing the way doctors have access to medical charts and other information: electronic medical records (EMR).

Adopting electronic medical records (EMR) systems was extremely beneficial to the healthcare industry and the way healthcare providers can view and exchange information about their patients. An EMR is simply a digital version of the paper charts in a doctor's office. Primary care providers can now view data collected over time as a report and easily note and identify any alarming changes. Disease management and chronic disease outcome have dramatically improved quality of care and screening rates for preventative measures.

EMRs have raised the quality of care, but they've also helped physicians' workflows. Adopting an EMR system has numerous benefits for any practice. Clinicians can manage their time efficiently (reducing time searching for paper results and reports) and access lab results more quickly. They can also grant remote access to patient charts and receive medication error alerts. They can even get reminders for preventative care such as mammograms or colonoscopies.

While an EMR is a digitized medical chart, an EHR system is a little different. An EHR (electronic health records) system is a digitized system of all types of health information. It provides a holistic view of a patient's records and is easily accessible by different providers. An EMR, on the other hand, is used within individual practices and not meant to be shared. Cloud technology supports both EMR and EHR systems. It provides practically unlimited storage capacity for records for extended periods of time. This technology also ensures that there is no data loss and that patient information is protected from any natural or artificial disasters.

Adopting an EMR/EHR system improves both quality of care for patients and information exchange between providers, a positive impact on all sides. Medicare and Medicaid offer an EHR incentive payment on the condition that there is meaningful use. There's no need to "pick a side" in EMR vs EHR. Sharing information in a secure way makes it much more powerful; after all—healthcare is a team effort!

Microwize Technology
1 Kalisa Way #101
Paramus, NJ 07652

Get a digital copy of this magazine
and never miss any issue at
www.practiceofthefuture.com

SCAN ME