HTA POST

Volume 6
Issue 3
March 2022

Healthcare Technology Advice for the Modern Independent Practice

WHAT'S NEW

Free Webinar March 25
Cyber Security Update 2022

It's time to sharpen your pencil, clear your notebook, and settle in for some learning. In the upcoming webinar called **Cyber Security Update 2022**, presented by **Derrick Weisbrod** of **Healthcare Technology Advisors**, you will learn about the current threats that are most likely to affect your medical practice, the steps you can take to mitigate your risk, and how to plan for the future of technology in the medical field. For more information and to sign up: *htadvisorsllc.com/events*

UPCOMING EVENTS

Cyber Security Update 2022
March 25 12pm-1pm

See more at: *htadvisorsllc.com/events*

IN THIS ISSUE

Page 2 - Combating Burnout: Environment, Education, and Community

Page 3 - Top 3 Cyber Threats

Page 4 - When Compliant Doesn't Mean Protected
Tech Tip: Reduce Cyber Risk By 50%

Healthcare Technology Advisors

REFERRAL

Want to get up to $2,000 OFF your annual IT investment?

Learn more at:
htadvisorsllc.com/about-us/referral-program

This monthly publication is provided courtesy of Derrick Weisbrod, CEO, and the Healthcare Technology Advisors Team.

Our mission is to be trusted advisors guiding healthcare businesses through the complex IT and HIPAA landscape while providing a comprehensive service that always maintains a human touch.

Physician Burnout Isn't New, But Your Approach Can Be

"A study by the Archives of Internal Medicine found that out of 7,000 responding physicians, more than 41% reported experiencing at least one symptom of burnout."

This figure isn't likely to surprise anyone, as the pandemic has only increased pressure caused by bigger workloads, staffing shortages, and stress. In the 2020 **National Academy of Medicine** report, *Taking Action Against Clinician Burnout: A Systems Approach to Professional Well-Being* several key areas were illuminated that could immediately reduce stress and fatigue among physicians and providers.

Environment

Your workplace should reduce stress, not add to it! Whether you own your own practice, work in a group setting, or are a team member for a large hospital system, creating a safe and supportive work environment is vitally important. No matter your role, seek to collaborate and communicate with your colleagues to discover what systems will work best for your practice. Value the input from everyone on your team - you never know where a new idea may come from!

Education

Continuing education is a requirement for many healthcare professionals. Yet learning, growing, and evolving in one's understanding of healthcare can take place in many settings. Amidst a growing shortage of healthcare professionals, your team may find opportunities to give back by pursuing an education certificate. Could your practice take on teaching interns, whether in the medical or administrative fields? Perhaps working with a local high school or college can bring you in contact with individuals who can benefit from the experience and expertise of your staff in non-clinical settings. Being given the opportunity to teach and inspire others can change the way a professional sees their own role.

Community

Feeling alone and isolated are huge contributors to burnout. A good solution to this is to foster and engage with a community of peers. While a workplace can be a community of its own, it is also good to reach out to larger established organizations such as the **Medical Group Management Association (MGMA)** or the **St. Louis Metropolitan Medical Society**. These groups have a treasure trove of resources that can be levied for the well-being of your providers, including education opportunities and networking. Perhaps more important than the professional resources are the personal connections that can be formed with others who are facing the same issues and fighting the same battles. These communities can strengthen a person's resilience, thus reducing burnout by letting them know they are not alone.

DON'T FEEL ISOLATED!

Interact with Your Peers in the Medical Community

Join the Greater St. Louis MGMA

mgmastl.org

TOP 3 CYBER THREATS FOR SMALL MEDICAL PRACTICES THAT AREN'T RANSOMWARE

Ransomware is a good news topic - it's flashy, scary, and always evolving while creating new stories. So, we end up talking about it a lot! Today, let's look at the top 3 cyber security threats to your practice that aren't related to ransoms.

1. Social Engineering

This type of attack is hard to predict and difficult to spot, because it relies on deception. Much like phishing, a social engineering attack works by an attacker pretending to be a trusted entity. This is often a very targeted attack, and the bad actor will use personal information that they've learned from observations on social media or from a compromised email account. If the doctor is on vacation and sends a hurried email asking the practice administrator to approve the transfer of funds for the new hire coming on next week, **it will probably seem very plausible**. The doctor IS on vacation. There IS a new hire coming in, and there was some mention of needing to set funds aside... So, the administrator may believe all this and follow the directions her boss has sent her. The problem here is that it was a bad actor pretending to be the doctor and spoofing a look-alike email. The only way to prevent an attack like this is to have standard operating procedures that require checks and balances, and to never ever go around them for convenience.

2. Third Party Exposure

Third Party Exposure happens when a service your practice uses, such as your billing company or management software, suffers a breach and your data is exposed. While there is little you can do to prevent this from happening, there is a lot you can do to mitigate the risk. First, **always be sure to work with companies who are HIPAA compliant** and are ready to sign a **Business Associate Agreement (BAA)** with your practice. They should be able to supply you with some information on their security measures. Not only does a **BAA** give you some protection in the case of a data breach, but it also shows that the company is taking their stewardship of your patients' data seriously.

3. Patch Management

Operating systems, cloud software, phones, tablets, payment systems - all these services update to provide new features, extra security, or to smooth out glitches that slow down your system. While these updates may make everything run smoother, they are a pain to implement on each individual device, and if not handled properly can cause massive disruption to your workflow. **They also represent a serious security risk.** Many cyber attacks focus on exploits in common software, such as **Microsoft**, **Java**, or **Adobe**. They target known vulnerabilities - that is, problems in the software that have already been discovered and patched away. The attackers know that not everyone will have run that security patch on their system. This was demonstrated in 2018 when two large scale cyber attacks exploited a weakness in **Microsoft** that had been patched two months earlier. It was only due to a lapse in updating that any organization was affected - but these attacks caused millions of dollars in damages.

UNCERTAIN HOW TO PROTECT YOUR BUSINESS? LEARN MORE HERE!

Read the Article in the
St. Louis Metropolitan Medicine Magazine
The Health Care Industry Is Under Attack from Cybercriminals!
Written by **Derrick Weisbrod**, our CEO

https://slmms.org/wp-content/uploads/2022/02/SLMM_February_2022.pdf

SERVICE SPOTLIGHT: WHEN "COMPLIANT" DOESN'T MEAN "PROTECTED"

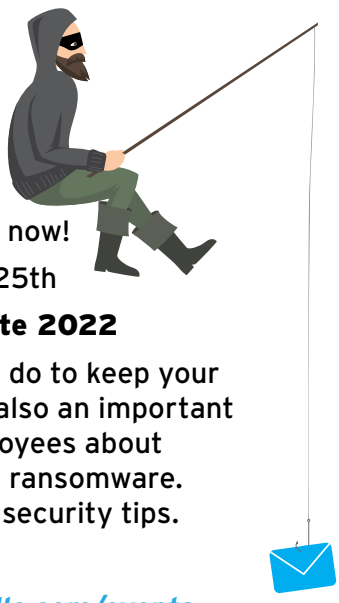
Maintaining **HIPAA** compliance is a huge part of the tech landscape for medical practices. It informs your purchases, training, and procedures as you make sure you meet the compliance standards. However, many businesses focus on such stringent compliance for only a brief time, such as an annual audit or risk assessment. According to **Verizon's PCI** Compliance Report, 80% of companies fail to maintain a passing level of compliance throughout the whole year.

Even weeks after being certified **Payment Card Industry Data Security Standard (PCI DSS)** compliant, some companies suffered data breaches. Meeting the standard of compliance is not always enough to adequately protect the data you've been entrusted with.

In order to maintain the level of protection needed, it is important to designate a person in your organization as the **HIPAA** Security Officer. In the same way, having a person chosen to oversee your cyber security compliance can make a big difference in how your practice operates on a daily basis. This person can be in charge of scheduling ongoing cyber security training sessions for your team.

Call **Healthcare Technology Advisors** to inquire about employee cyber security training BEFORE the next incident hits the news.

WHO'S PHISHING IN YOUR POND?



Protect your business now!

FREE Webinar March 25th

Cyber Security Update 2022

Find out what you can do to keep your business safe. This is also an important training for your employees about phishing, hacking, and ransomware. Learn essential cyber security tips.

Reserve your spot!

More info: *htadvisorsllc.com/events*
or call 314-312-4701

TECH TIP: REDUCE CYBER RISK BY 50%

Did you know that more than 60% of cyberattacks are attributed to insiders? An organization's employees can do as much damage as cybercriminals whether they mean to or not, and that could be a disaster for your business.

The primary way that insiders bring you risk is through human error like sending someone the wrong file or interacting with a phishing message. Of course, there's always the possibility that an employee is out to hurt your business intentionally. Malicious insider actions are responsible for an estimated 25% of confirmed data breaches.

But you can reduce your risk of an insider security incident with security awareness training. Security-related risks are reduced by 70% when businesses invest in cyber security awareness training. Employees that are educated in risk with a solution like **BullPhish ID** make fewer mistakes and spot suspicious behavior faster. Don't postpone putting this affordable and effective tool to work for your business today.

Call (314)312-4701 today to reserve your slot at our free webinar **Cyber Security Update 2022** or go to: ***htadvisorsllc.com/events*** for more information.