

WHAT'S NEW

HTA offices are opening back up for business! After two months of working remotely, our team is getting the option to come back into the office. We'd like to send a big shout-out of thanks to Derrick, who scoured several counties to come up with enough cleaning supplies to enable proper sanitation.



MVP of the quarantine-sanitizing goes to Greg Thompson of St. Louis Rheumatology, who graciously ordered us extra toilet paper through his supplier so that we could all come back to the office!

UPCOMING EVENTS

Wednesday,
June 17th

Greater Kansas City MGMA
Monthly Meeting: *Litigation Issues
for Practices*



See more at:
htadvisorsllc.com/events

IN THIS ISSUE

Page 2 - Client Spotlight: : Advanced Endoscopy Center

Tech Tip: Reduce Downtime and
Increase Efficiency!

Page 3 - Leading Through Empathy and Flexibility

Page 4 - The True Cost of Ransomware



Healthcare
Technology
Advisors

REFERRAL

Join the HTA
Advisory Committee!



Have a coffee on us, and get a chance at a
FREE iPad.

With our new referral rewards program, every
qualified referral enters you into a drawing
for a new iPad. Don't miss your chance to win
this quarter!

This monthly publication
provided courtesy of Derrick
Weisbrod & Hugh Anderson,
Founding Advisors of Healthcare
Technology Advisors.

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.



CLIENT SPOTLIGHT: : ADVANCED ENDOSCOPY CENTER



In 2005, the Advanced Endoscopy Center (AEC) opened in Creve Coeur, Missouri. AEC is an outpatient, State Licensed, Medicare Certified, AAAHC Accredited Endoscopy Center that is dedicated to providing a positive experience.

As their page of nearly 40 glowing testimonials demonstrates, the physicians and staff of AEC put patient comfort first during a procedure that is often approached with apprehension.

AEC is staffed by a team of experienced physicians who strive to create a comfortable experience for their patients. Through continuing education, hardware upgrades, staff training and meticulous attention to detail, AEC continues to improve their care.

2020 will mark the third year that Healthcare Technology Advisors has provided IT services to both AEC and its sister office, Specialists in Gastroenterology. It has been nothing but a pleasure to work with the wonderful staff of this facility. Their commitment to best-in-class service for their patients matches ours, and we are proud to work with them and continue pursuing that goal.

TECH TIP: REDUCE DOWNTIME AND INCREASE EFFICIENCY!

Do you love summer thunderstorms? Does the sudden temperature drop fill you with excitement?

Do you also HATE the sudden blackouts, the torrential downpours, and the internet outages that often follow?

Maybe the hectic weather wouldn't be so bad if you could count on your internet to stay on! With our ever-more connected hardware and applications, it's hard for any function of your office to continue without the internet. Even if the power is on, having an internet outage can grind your practice to a halt on both the patient and staff side.

According to a 2019 Ponemon Institute study, it costs a healthcare facility an average of \$740,357 per downtime incident. Internet outage can contribute to IT downtime, and gravely affects your practice's ability to serve patients, send results to other offices or labs, or process appointments and billing.

One of the best ways to prevent internet outages in your practice is to switch to fiber optic internet. While copper co-ax internet only comes with a promise of "best effort" by your ISP to repair damage and restore connections, fiber comes with a 99.99% guarantee. Not only will you rarely experience prolonged downtime, your office will also benefit from faster upload and download speeds, which will increase efficiency and probably please your staff!

Visit htadvisorsllc.com/fiberquote to see if your office is eligible to upgrade to fiber today!



LEADING THROUGH EMPATHY AND FLEXIBILITY

Derrick Weisbrod



As we are entering or preparing to enter the phase 1 opening, I am certain there are a lot of mixed feelings among our employees and management teams alike. Schools are still enacting remote learning and making it difficult to manage staffing as our team members weigh schooling priorities with working priorities. Our clients are asking for services in a more diverse way than they were just two months ago.

But we are, in fact, getting back to a more active state of business affairs. Our business is getting back to having a generally full office—or as full as our office gets with us already having a partial remote-work culture in place. I know my feelings are mixed when weighing all the different inputs on the pandemic subject. What I am left feeling most is the importance of empathetic flexibility for our clients, patients, team members, families and pretty much everything about our co-existence with each other.

Empathetic flexibility to put ourselves in the shoes of our peers, to respect their views and help each other be safe and thrive while we continue to pivot within our business to make things work.

Empathetic flexibility to understand the fears and needs of our patients and clients so we can ensure we are providing services to help them without inducing unnecessary anxiety and stress.

Empathetic flexibility to understand that schooling for our children requires change in our lives to ensure

they understand homework assignments, coach them through not having the joy of celebrating that last day of school while looking forward to summer break with their friends, and the possibility they may not be able to return to school in fall with their friends.

Empathetic flexibility to be a good partner in our private lives, to realize, appreciate, and support our partner through the stress of change they are enduring in their professional and personal lives.

We are experiencing something truly unique for all of us. The change that is happening at an amazing clip is not always easy for us to process. As we have pivoted our businesses and realigned the plans we set at the beginning of the year with the new realities we are expected to contend with, we need to step back and reflect on how much stress and anxiety this has created for those in our personal and professional lives even while leading them through this. As leaders, we need to make sure we are open to being flexible with the dynamic pace of change while digging deeper than we normally may to ensure we are being empathetic with all the emotional stress that is surrounding us as we lead our way through this phase 1 re-opening process.

I hope you stay safe and your business pivots lead to successful outcomes for the coming month while the pandemic numbers continue to flatten.

JUNE 2020

BREACH REPORT: THE TRUE COST OF RANSOMWARE

As the headlines about ransomware attacks pile up, it is impossible to not think about what may happen if your practice is targeted. Some readers may have already experienced this, hopefully more of you have not. Industry leaders continue to say that it's not an IF, it's a WHEN. With the high profits, ease of distribution, and relative low risk for the hackers, there is no sign that ransomware will slow.

Although the FBI does not recommend paying the ransom in an attack, a recent survey commissioned by Sophos found that 26% of companies who experienced an attack chose to pay the ransom to recover data. Yet this survey finds that organization who pay ransom end up paying more overall to recover their data than those who are able to recover from backups.

The problem is, many companies find themselves with limited options to recover. If appropriate backups are in place, restoring operations can be simple. 56% of attacked organizations reported that they chose to recover from backups. If that is not an option, then companies must weigh the risk of paying the ransom, with no guarantee of file recovery, versus the massive cost and lost data of rebuilding their damaged and vulnerable infrastructure. 85% of the surveyed companies had cyber liability insurance, yet only 64% said their policies covered ransomware. Of that 64%, 94% said the ransom was paid by their insurance company. Even then, there is no guarantee of full file recovery. Some companies may find themselves paying the ransom and THEN paying to rebuild or paying litigation over losing data.

The Sophos survey states that "victims of ransomware attacks were asked to provide an estimate cost of the attack, including downtime, staff costs, equipment costs, lost business, and other associated costs. The average cost in cases where the ransom was not paid was \$732,520 whereas the cost was around twice that amount at organizations that paid the ransom - \$1,448,458."

If an organization chooses to pay the ransom, which is often sizeable, they are still faced with other costs associated with an attack. Even further down the line, there may be litigation over the data breach or loss. And while recovery by ransom may seem the fastest way to resume normal operations, decrypting endpoints is often a cumbersome and time-consuming process, and you risk data corruption during encryption and decryption.

As the FBI recommends, you should never pay a ransom unless there is no other choice. Paying the ransom only feeds the attackers and ensures that ransomware attacks remain a viable business for decades to come. Organizations should recover their files from backups, and take the appropriate steps to make sure that option is in place, including ensuring multiple backups are made with one copy stored on an air-gapped device. Equally important is testing the backups on a regular basis to make sure they are not corrupted. While these steps may seem like unnecessary expenses, the data shows that not having them is even more costly.