HTA POST

Volume 4
Issue 4
April 2020

Healthcare Technology Advice for the Modern Independent Practice

WHAT'S NEW

The impacts of the COVID19 Pandemic are now being felt in our community in Missouri and Southern Illinois. Mandated quarantines, self-isolation, and school closings can have huge effects on the economy, and on the workforce.

Many offices are implementing as much remote work as possible to help combat both disease spread and lost productivity. This can be done by giving your employees options for working from home, such as remote-access to their work computers, setting up video conference calls instead of in-person meetings, and letting them take projects home with them to work on. It's always important to review policies with your employees to ensure both your practice's data and your patient's information stays protected.

UPCOMING EVENTS

Due to the unknown state of the COVID19 response, most upcoming events in April have been canceled or postponed. Stay tuned to your local organization and our Facebook page for news about webinars and rescheduled events!

See more at:
htadvisorsllc.com/events

IN THIS ISSUE

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!

Healthcare Technology Advisors

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: SPECIALISTS IN GASTROENTEROLOGY

Specialists in Gastroenterology (SIG), located at 11525 Olde Cabin Road in St. Louis, MO, is a well-established G.I. group with over 100 years of combined experience. The single-specialty medical group has a staff of highly trained and experienced physicians specializing in gastroenterology. The medical staff includes Dr. Leonard Weinstock, Dr. Erik Thyssen, Dr. Steven Fern, Dr. Aman Singh, and Dr. Nikhil Banerjee. These doctors are assisted by three physician assistants: David Van Hoornbeek, Jennifer Gorham, and Kimberly Birenbaum.

SIG offers a wide range of clinical services, from hemorrhoid treatment and colonoscopies, to endoscopies and pelvic floor therapy. The group diagnoses and treats challenging clinical G.I. problems and has expertise in diagnostic and therapeutic endoscopy procedures of the gastrointestinal tract. SIG emphasizes the use of innovative new technology coupled with compassionate patient care. Patients can trust the 100 years of combined clinical expertise and their passion for practicing medicine. SIG is actively engaged in clinical research and teaching at Washington University and Barnes-Jewish Hospital.

TECH TIP: ARE YOUR BACK UPS UP TO 2020 STANDARDS?

Is your practice READY to restore operations from your current back up?

Spring floods, tornadoes, lightning – the Midwest knows the drill. With our rolling thunderstorms and wonderous rivers spring and fall always bring new challenges. We know it's coming. Is your practice prepared?

If you can't answer "Yes" to these three questions, you may suffer financial losses in the event of a natural disaster.

1. Is your data backed up to a remote location, and have you tested the recovery capabilities?
2. Do you have your disaster recovery plan documented in a way that is easy for all staff members to follow, with minimal disruption to daily activity?
3. Can your revenue cycle activities, such as billing insurance and patients, carry on if your office is closed?

Having these solutions in place is a vital component of being HIPAA compliant, and important for maintaining basic business functions in the face of everyday disruptions, such as power outages, workplace accidents, or travel restrictions.

Need help? Call HTA today or go online at htadvisorsllc.com/10essentials/ to discover the top 10 essential steps to safeguard your practice or business against natural disasters.

Schedule a free Backup and Disaster Recovery Consult to help get your plan in place!

HOW MUCH ARE YOU WILLING TO SPEND ON HIPAA FINES?

Do you know if your referral partners are putting YOUR patient's data at risk?

Every medical practice knows the risks of not having a BAA in place with vendors. Not only is it bad for your patients, should a vendor prove disreputable OR simply fall victim to a cyber attack, it is bad for your practice's bottom line if a fine is levied against you as a result of a breach. This was seen in the Advance Care Hospitalists settlement of $500,000 when it was discovered that not only did they have no BAA in place with their billing service provider, but that the billing service was providing its service fraudulently to the hospital.

A BAA represents due diligence on the part of the medical practice – you've made every effort to ensure that your patient's data is safeguarded when it leaves your walls. Yet risks from third parties continues to be a problem.

Have you ever considered the risk of referring your patients to other doctors who may not be HIPAA compliant, even willfully so? Even if their medical judgement and care is sound, they may not have put any effort into maintaining a compliant network infrastructure, policies, or procedures. If you refer your patients to an office you know to be a liability, their trust in you will be damaged if their protected health information ends up stolen, lost, or misused.

IS YOUR WORKFORCE TRAINED ON PHISHING SCAMS?

Hackers are targeting COVID19, are your employees ready?

As employees work from home and we experience greater disruptions, be extra vigilant for phishing scams. Hackers KNOW that the workforce is confused and constantly adapting to new procedures. They WILL take advantage and attempt to mislead and trick your employees into revealing sensitive information or credentials.

This could come in the form of "mimic" emails, enticing workers to click through to a website that will steal their credentials.

Or, it could come in the form of a spoofed email that **LOOKS** like it is from the CEO, management, or a 3rd party vendor.

Perhaps an important meeting was canceled and the boss needs help accessing the video conference platform? Or an in-person delivery was changed and you now need to wire a payment directly? These are plausible occurrences, and employees need to know exactly what procedures to follow to make sure they do the right thing and don't fall for a criminal's tricks.

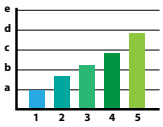
Be VIGILANT and review your SOPs!

5 THINGS TO PUT IN PLACE FOR REMOTE WORK

With the rapidly evolving situation around the COVID19 virus, many workplaces are initiating work-from-home policies that have never tried to accommodate this workflow before. Whether your office is doing this to safeguard employees through social distancing, or as an option for parents who must stay home with children, it can be hard to make such a huge adjustment quickly. Some amount of training is required, and you may need to implement new technology, software, or hardware to enable your employees to work remotely.

These are 5 vital components of remote work you should put in place or review ASAP.

1. Time Tracking – If you have employees who are paid hourly, or who need to report for certain time frames throughout the day, make sure you have a time tracking policy and procedure in place that your employees can use as they work from home. Whether it's as simple as making sure they can access the clock-in software remotely, as opposed to using a designated machine in the office, or going over expectations during remote work, it's important that everyone understands exactly what they need to do and how they need to do it.



2. Progress Reporting – Similar to tracking their time, some of your employees will need to track their progress on certain projects. While this may have been done in-person in the office, now it is important to make sure you have Key Performance Indicators (KPIs) in place for each position. Whatever their jobs entail, there should be measurable results that the employees can report to their supervisors to ensure that all operations are running as smoothly as possible.

3. Multi-Factor Authentication – As your employees access their work accounts, emails, and documents from different computers and new internet connections, it's vital to put in place a form of multi-factor authentication to guard against cyber attacks that may use stolen credentials to break in to your network.

4. Video Conference Options – It may never be as easy as walking into someone's office, but video conference platforms such as Zoom, GoToMeeting, or Skype can help keep teams together and communicating effectively while they are miles apart.

5. SOP Review – Your Standard Operating Procedures (SOPs) for remote work may be dusty, or they may not exist at all. It's important to glance over them, make sure they are updated for your current workplace reality, and then to spend time going over them with any workers who will be doing their job from home for the first time. This will include expectations for time tracking, KPI reporting, cyber security measures, and communication standards.

While the realities of this health crisis have been disruptive to many businesses, having the flexibility to offer remote work to your employees will help you respond to future disruptions with greater ease. For now, check in with your workers to make sure their questions have been answered, and that they are comfortable with what they are expected to do and how they are expected to do it. This crisis may get worse or taper out, but what we learn from it can be carried into the future.