HTA POST

Volume 3
Issue 7
July 2019

Healthcare Technology Advice for the Modern Independent Practice

WHAT'S NEW

Mark your calendars for October! The Greater St. Louis MGMA is planning its fall conference for Wednesday, October 16th. It will take place in Orlando's Maryland Heights hotel from 7:30am-1:45pm. The Annual Conference is a networking and education event that draws practice managers from across the St. Louis Metro area and provides two general sessions with two tracks of breakout sessions on topics of leadership, healthcare, finances, insurance, advocacy, human resources, and more. Billers and coders will also get valuable face-to-face time with sponsor and payor representatives who can provide education and assistance.

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!

UPCOMING EVENTS

Wednesday, July 10th
Greater St. Louis MGMA Legislative Webinar

Windows 7/Server 2008 presented by John Motazedi

Wednesday, July 24th
11am-1pm SEMO MGMA Monthly Lunch Meeting

Dexter's BBQ
Cape Girardeau, MO

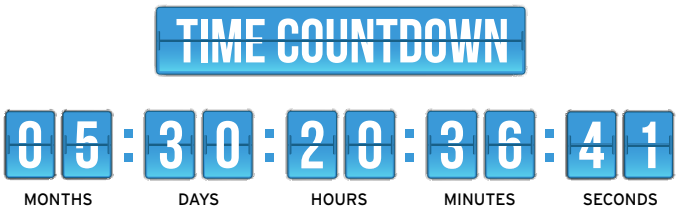
See more at:
htadvisorsllc.com/events

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.

SPOTLIGHT: WINDOWS 7 EOL



July marks the 6-month deadline! On January 14th, 2020, Windows 7 and Windows Server 2008 will leave extended support. This will result in several things.

1. Any machine running these operating systems will no longer receive vital security patches and updates. Any new virus or exploit that is discovered may not be patched, leaving the system vulnerable to hackers, malware, and ransomware.
2. Many third-party line-of-business applications may stop supporting the operating systems, meaning new updates to the software will not be available for Windows 7 computers.
3. Without proper security updates, any machine running outdated operating systems will no longer be HIPAA-compliant due to their increased vulnerability to breach.

Don't delay! Updating software and hardware should be planned out during your business strategy meetings with your IT team, so it doesn't become a huge, unexpected expense. If you don't already have a plan for replacing any old machines in your practice, contact HTA today to learn how to roll out upgrades in a predictable, budgeted fashion.

BEST PRACTICE OF THE MONTH: STAFF TRAINING ON CYBERSECURITY

Do you know what the number 1 risk to all medical practices' cyber security is? The one no anti-virus, firewall, or security update can protect you from?

The answer is YOU. And your employees!

Of course, there's no way to run a medical practice without people (yet), so what can we do to minimize this risk?

The best solution is to give your employees the proper training to help them protect themselves and your business from technology breaches. Regular training sessions that go over current risks and trends as well as best practices will help keep your staff aware of why procedures are in place and what they're safeguarding against. Phishing attacks are becoming truly sophisticated, and the only way to protect against them is to have a workforce that is trained to think critically about what is presented to them and make active decisions about how to react. Spam filters WILL NOT catch all phishing attacks. When these malicious emails end up in your staff's email account, make sure they are prepared to deal with them.

Healthcare Technology Advisors believes that ongoing education is the key to success in cyber security. Not only because the field of cyber security evolves quickly, but also because simple repetition is a good way to ingrain habits. It may feel redundant, but going over the nuances of how to handle a suspicious email once will quickly fade and be forgotten, while going over it every week will get the rules firmly entrenched in your mind. Any steady cadence of training is going to serve you well. Perhaps you sign up for a weekly cyber security email, or have a monthly staff meeting with a dedicated time slot for security training. Having quarterly education sessions can give your staff an in-depth refresher on best practices, procedures, and regulations.

If you need help finding training resources, call or contact HTA today, and we can advise on what would best work for you and your practice.

HIPAA FINE SPOTLIGHT - $100,000

Medical Informatics Engineering, Inc (MIE) is an Indiana business that provides electronic medical records and software services to healthcare providers. MIE has agreed to take corrective action and pay a $100,000 dollar fine to settle potential violations of the HIPAA Privacy and Security Rules.

Their breach was filed on July 23, 2015, and detailed that MIE had discovered a hacker had used a compromised user ID and password to access the electronic protected health information (ePHI) of their patients, numbering approximately 3.5 million. A user ID and password could be compromised in any number of ways, including through spyware, poor password hygiene, or a third-party breach. However, the OCR's investigation into the MIE breach revealed that they had not conducted a comprehensive risk analysis, commonly called a Security Risk Analysis or SRA. Such an SRA is required by HIPAA Rules, and the absence of this record represents a violation that likely led to the fine levied.

SRAs are a vital part of an organization's cyber security and HIPAA compliance plan, as these in-depth reviews can reveal any gaps that exist or may arise in the future. Not only that, the risk analysis serves as the basis by which all measures can be judged as reasonable or appropriate. What is vital for a 200 bed hospital may be ludicrous for a 2 doctor practice, and the risk analysis helps define what is logical for each individual medical practice as they build their compliance roadmap.

It is important to note that, while investigating potential HIPAA violations, the OCR heavily weighs whether an organization has taken all the required steps and acted in good faith to attempt to minimize the risks of a breach. In the current landscape of technology, it is impossible to prevent all breaches. Simply having a breach does not mean that an organization will be fined. However, as this example shows, when it comes to light that the basic steps have not been followed to either reduce risk or improve response to a breach, the OCR is more likely to levy a fine.

Healthcare Technology Advisors advocates a yearly SRA carried out by a third party. This risk analysis can be used to build the yearly cyber security and compliance plan that will govern how staff is trained, how technology is handled, and how procedures are changed. That plan should be reviewed every quarter when meeting with your IT team and internal staff, to ensure that it is both still reasonable and possible to implement, and to check on its progress.

Having these steps in place and documented will not only greatly improve your practice's security, it will help protect you against HIPAA liability should a breach occur.

A SUMMARY OF 1,000 CLICKS

On March 18th, 2019 Fred Schulte and Erika Fry published the article "Death by 1,000 Clicks" on Kaiser Health News (KHN), a collaboration between KHN and Fortune Magazine. The article reviewed the findings of a three-month long investigation into the United State's implementation of electronic health systems. Their key take-aways are summarized below.
Read the whole article at:
khn.org/news/death-by-a-thousand-clicks

Part 2 – Physician Burnout

Our community has seen it in seminars and conferences; the topic of "physician burnout" is an oft-revisited one. A 2018 Merritt Hawkins survey found that 78 percent of doctors suffered symptoms of burnout. As more and more time is being spent on tasks that don't directly benefit patients, what may have once been dismissed is becoming acknowledged as a public health crisis.

Burnout is, of course, caused by many things. When related to EHRs, the most common trends are frustrations with how technology has changed the doctor-patient relationship, and with errors that occur due to faulty or unintuitive programs. The Joint Commission raised awareness of the issue of false alarms. Between 85 and 99 percent of all EHR and medical device alerts are false alarms. A study by researches at Oregon Health & Science University estimates that as many as 7,000 alerts pester the average provider working in an intensive care unit. These false alarms or passive alerts all take a heavy toll on the provider's ability to distinguish when an important alert surfaces. The Joint Commission tallied 170 reports of patient harm that were related to alarm management and alert fatigue. Of 170 reports, 101 incidents resulted in patient deaths.

Many doctors today have developed "low-tech" workarounds to the EHR systems they are tasked with using. An emergency medicine physician in Washington, D.C. often leaves important notes on a whiteboard to communicate with other doctors, or even writes the note on a paper towel and leaves it on their colleague's keyboard.

Further frustrations arise from mysterious bugs within the EHRs themselves. Occasionally, common shorthand, such as enclosing notes in brackets, would cause entire sections of text to be deleted. This 'feature' was unbeknownst to both the doctors and the EHR maker, and took weeks of study and trial-and-error to discover.

Underlying all of these is the other frustration – that of the changing dynamic within the consulting room itself. Where a doctor only has 7 to 11 minutes on average to actually spend with a patient, every second spent clicking between menus, searching for the correct history, figuring out where to input notes, and checking countless checkboxes that pop up regardless of pertinence grinds away at the core of why most doctors enter the field; to connect with and help their patients.

The professional frustration, the physical and mental stress, and the fear of errors all contribute to physician burnout as they relate to the technology they use. None of these issues, alone, could be made into a case to abandon the electronic systems, but they all must be taken into account as these systems continue to evolve and move our health care field with them. When so much time and money has been invested into a system it is logical to clamor for needed changes to improve it.

Our summary coverage of this topic shall continue next month as we cover the costs and ideals of the system.