HTA POST

Volume 3
Issue 9
September 2019

Healthcare Technology Advice for the Modern Independent Practice

WHAT'S NEW

On September 25th, the healthcare organizations in and around Kansas City are collaborating to present the Kansas City Healthcare Community Symposium. This all-day conference will be focused for healthcare managers and coders, concentrating on the collaboration of the sponsoring associations, the connections between both the organizations and individuals that make them shine, and the greater healthcare community from which all members can learn and grow. 12 speakers will present timely educational content from 7:30am-5pm at the KCI Expo Center. You can learn more at this website: nwmomgma.wildapricot.org/symposium

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, September 11th	11:30am-1pm Greater St. Louis MGMA Monthly Luncheon *Spazio Westport in St. Louis*
Thursday, September 19th	11am-4pm HFMA Greater Heartland Kansas City Regulatory Update & Payor Panel *Cerner World Headquarters in KC*
Wednesday, September 25th	7:30am-5pm KC Healthcare Community Symposium *KCI Expo Center in KC*
Thursday, September 26th	9am-5:30pm HFMA Greater Heartland St. Louis Regulatory Update & Payor Panel *Anders CPAs & Advisors St. Louis*
Monday, September 30th	7:30am-2pm HFMA Greater Heartland Golf Tournament *Staley Farms KC* HTA will be sponsoring a hole and playing!

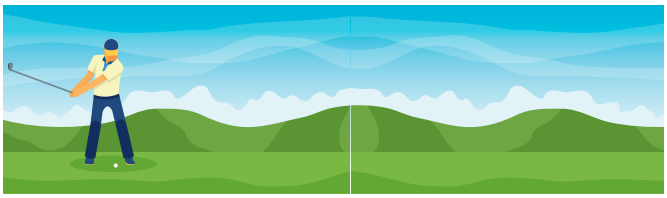
See more at:
htadvisorsllc.com/events

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 ON UPCOMING EVENTS



Healthcare Technology Advisors is looking forward to the September 30th Greater Heartland HFMA golf tournament, taking place at Staley Farms in Kansas City – even though it is on a Monday morning! The Greater Heartland HFMA serves the entire state of Missouri, hosting events in Kansas City, St. Louis, Springfield, Columbia, and the Ozarks. The morning golf tournament is a great opportunity to network with healthcare professionals in Kansas City, and we are excited to be sponsoring a hole along the way. Our team will also be playing in the shotgun scramble event.

The event will feature breakfast, lunch, and drinks, giveaways, hole prizes, and plenty of fresh air and quality company.

THE WOMEN'S SAFE HOUSE
EMPOWERMENT STARTS HERE

The Women's Safe House would like to invite you to "Yas, Brunch!" a fundraiser presented by the Young Professional Board. The brunch is from 10:30am-1pm on Sunday, September 15th at Boundary at the Cheshire Hotel in St. Louis.

Founded in 1977, the Women's Safe House is the oldest and largest domestic violence shelter in St. Louis. They are open 24 hours a day, 365 days a year, and serve between 400 and 500 women and children annually. This 501(c) Non-Profit can provide shelter for up to 12 weeks, and strives to provide safe shelter and transitional living services to battered women and their children while empowering them to make informed decisions about their future.

One ticket to this fabulous event is just $85 and comes with brunch and bottomless mimosas, making it easy to support this great establishment. Healthcare Technology Advisors is looking forward to attending and getting to know more about this organization. You can get a ticket at twsh.org/event and join us there!

BEST PRACTICE OF THE MONTH: ENCRYPTION

Encryption is a method of 'scrambling' data so that it cannot be read or used except by the intended recipient. Covered entities are required to encrypt Protected Health Information (PHI) "whenever deemed appropriate" which is intentionally open to interpretation. This is to allow the requirement to be both scalable and evolve with the pace of technology.

When trying to protect PHI encryption is vital in order to prevent the information being readable if it is stolen. An intercepted email, if encrypted, won't reveal PHI. A stolen laptop can't have its data read if the hard drive is encrypted. Even flash drives should be encrypted if they are carrying PHI. Strong encryption should be used any time PHI is entering or exiting a business via electronic means, either through an email attachment or file sharing technology.

Not having appropriate encryption in place can lead to not only the loss of data but also fines levied by the OCR as a result of violating HIPAA rules. There have been several examples of fines levied after a laptop was stolen from an employee's vehicle. Because that laptop was not encrypted, and contained PHI, the incident represented a preventable breach. Had the laptops been encrypted, the PHI would have been considered safe and no breach need be reported.

Healthcare Technology Advisors understands that each practice will need to consider what the appropriate level and method of encryption is for their environment, which is why we work so closely with our clients to align technology with their business goals. Whatever the solution, it should include strong encryption for all laptops, workstations, and server disks, emails containing PHI, and methods of transferring PHI between covered entities and business associates.

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 4: Cone of Silence

One of the driving notions for the HIPAA rule is that patients have the right to access their personal medical data and take it with them wherever they go. This idea was naturally expanded by the HITECH act, with the vision that one EHR should talk to another being a key part of the original plan. The government hoped that all EHR systems would eventually be interoperable.

However, business forces were working against that from the beginning. A free exchange of information meant that patients could easily take their records and leave one doctor to be treated by another, in a different practice or hospital. This is of course not good for business, and hospitals were loath to let such proprietary value walk out the door. So while possible, moving medical records is often far from easy. On the software side, EHR companies had few incentives to interoperate while they were concentrating on gobbling up market share. Indeed, being the most widely-used system in any given healthcare region could be seen as a boon, and if it was difficult for the non-users to work with that system, all the more reason to encourage them to adopt the status quo. Meanwhile, it seemed unrealistic to insist that the various systems share data in the early years of adoption, because 90% of the nation's doctors and practices had no system or data to exchange.

Now, in the light of the difficulties of using EHRs and exchanging information between them, or even obtaining records from them, there are many problems that need to be addressed. Yet getting information about the various failings of these expensive systems is proving just as difficult. EHR vendors often have contractual gag clauses that discourage or prohibit buyers from speaking publicly about problems with the systems, even when those issues present real safety risks to patients. The KHN and Fortune article points out that two doctors who spoke candidly about problems with their EHR later asked that they not be identified by name as their health care organization had forbidden them to talk.

Additionally, many EHR vendors have contract stipulations known as "hold harmless clauses" that shield them from liability in the event that a hospital is sued for medical errors. This may be why so many of the lawsuits filed against hospitals that relate to the use of this technology are settled out of court, with the records only saying that the EHR vendor has denied all liability.

It is clear that both the cone of silence around individual EHR systems and the forced silencing of their critics and users must end if progress is to be made with the national network of medical records.

DHS RECOMMENDATIONS AGAINST RANSOMWARE

In response to an increase in ransomware attacks against government systems, the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, National Governors Association, Multi-State Information Sharing and Analysis Center, and other government groups released three recommendations on July 19th 2019 that outline a defense against ransomware. They stress in their press release that prevention is the most effective defense.

1. Back Up Your Systems – Now and Daily!

All critical information, including system configurations, should be immediately backed up onto a separate device (not a networked workstation) and stored offline. That way it can be accessed even if the internet connectivity of an office has been compromised. These backups should be refreshed daily to ensure that as little data as possible is lost in an attack, and the restoration process should be tested on a regular basis to make sure that it is working as intended.

2. Reinforce Basic Cybersecurity Awareness and Education

Almost all ransomware attacks rely on human error, as evidenced by the spike in phishing attacks that regularly find their mark. Refresh employee training on how to recognize these attacks, as well as how to report a suspected or confirmed breach to the appropriate IT staff in a timely manner.

3. Revisit and Refine Cyber Incident Response Plans

Agencies must have a clear plan to follow if an attack occurs, that details how to minimize the damage, restore what was lost, and includes how to request assistance from external cyber first responders in the case that internal capabilities are overwhelmed. For HIPAA covered entities, this must also include how to determine if PHI has been compromised and how to report the breach to the authorities.