HTA POST

Volume 3
Issue 8
August 2019

Healthcare Technology Advice for the Modern Independent Practice

WHAT'S NEW

R3 DYNAMICS, LLC
RESPECT. RESPONSIBILITY. RESOLUTION

HTA is proud to welcome R3 Dynamics, LLC to our family of clients! R3 Dynamics specializes in Revenue Cycle Management and Process Improvement for hospital and physician providers. Using a consultative approach, they work with their clients to maximize reimbursement through services such as on-site revenue cycle consulting, first party/early-out recoveries and third-party debt recovery for hospitals, physicians, and specialty services. They are growing their business in St. Peters and look forward to serving the Greater St. Louis area.

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, August 14th	11:30am–1pm Greater St. Louis MGMA Monthly Luncheon
	Compliance Plans with Diane Robben of Sandberg Phoenix & von Gontard, PC.
Wednesday, August 21st	3–5pm Greater KC MGMA Monthly Meeting
	MIPS and CMS Update
Thursday, August 22nd	7:30am–12pm Greater Heartland HFMA
	IT/CybersecurityHot Topics in Healthcare

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: PICKIN' ON PICKNIC!

Have you ever danced until dawn around a campfire to the sounds of strings picking and jamming while a full moon rises over the Meramec? Derrick Weisbrod could tell you a thing or two about it. In July, HTA was thrilled to sponsor the Pickin' on Picknic Music Festival in St. Clair, Missouri, along with our friends from Regional Dermatology. The four-day event was filled with love and laughter, joy and tears, as we celebrated a wedding, tore through some crazy-good bluegrass, and remembered the passing of a dear friend. This was the Picknic's second year, and we can only say it's getting better with age! Leftover Salmon, the headliner on both Friday and Saturday night, loved the experience and stayed up around the 'jamfire' until they missed their shuttle!

The entire HTA crew took part in this festival, from being a major sponsor, to doing creative work and consulting. Working together on this festival exemplified a lot of what we stand for as a company; community engagement, pulling together, and having a village mindset. It takes a lot of different heads and hands to pull off a music festival, and getting to work with everyone is a unique and rewarding challenge. We hope to see many more of you in the Shady Grove at Pickin' on Picknic 2020!

BEST PRACTICE OF THE MONTH: PROACTIVE MONITORING

If you've read any piece on proper healthcare technology, you've likely heard of proactive monitoring. This is the method of managing technology in a way that keeps it in the best working order possible, rather than waiting until something breaks or doesn't work properly before trying to fix it. It's akin to eating right and exercising, but for your computers.

In today's cyber landscape, this method of management is vital due to the constant evolving threat of viruses, ransomware, malware, and spyware – all malicious computer programs that can be installed on your network through user error or hacker infiltration. Most malicious programs take advantage of known exploits in a software or operating system such as Windows 10. To combat that, software developers release security patches that update the programs to fix the vulnerability, usually before it is even made public. Therefore, most hackers are only targeting those who have failed to properly patch and update their machines.

The best practice in this area is to employ both proactive patch management and network monitoring. Patch management involves scheduling, testing, and remotely installing new patches across a network in a predictable, step by step fashion. This ensures that the patch won't break any critical Line of Business applications (like suddenly causing your EMR to not launch) as well as that every machine in a network will get the patch, with no back-office computer forgotten. Meanwhile, monitoring entails keeping track of how systems are running and watching for errors or problems with backups. That way, if an issue comes up, it can be immediately resolved, usually before it causes any problems for the end user.

Minimizing downtime and interruptions is one of the biggest benefits of proactive monitoring and patch management, and is a basis of Healthcare Technology Advisors's managed service offerings. Any IT service provider should be able to give your practice detailed information on how they are proactively protecting your systems today.

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 3 – Costs and Incentives

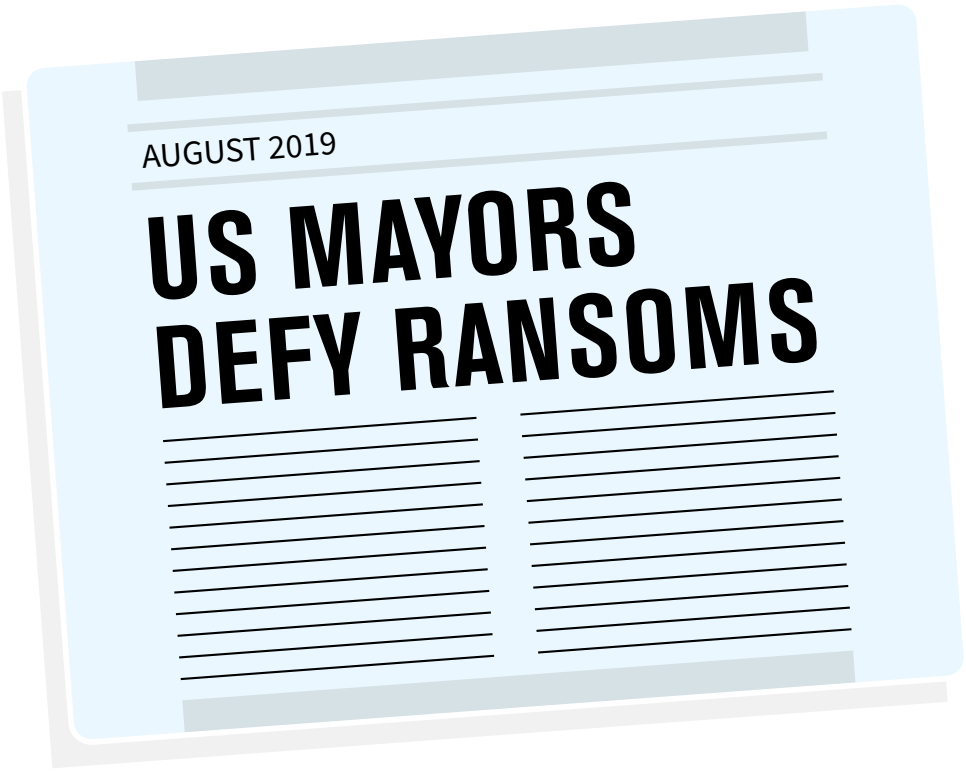
Transforming America's healthcare information landscape was never expected to be easy, or cheap. In the depths of the recession, however, it seemed exactly the sort of project that the government could apply stimulus budget to that could propel job growth and innovation in a vital sector of our economy. And so in February 2009 the HITECH bill was passed, which set aside a large portion of stimulus money for health information technology. The spending was outlined as an incentive program. Physicians who could prove they were meaningfully using a government-certified system would qualify for a federal subsidy of up to nearly $64,00, paid over a period of several years. This would offset the cost of transition as well as provide the financial incentive for swift and early adoption. Meanwhile, vendors had to develop new EHR systems that met government requirements for certification.

By simple adoption, the HITECH effort can be considered a success; today, 96% of hospitals use EHRs, which is up from 9% in 2008, before the stimulus package. However, the development and implementation of these systems has been plagued with problems, not the least of them accusations of corruption. The overhaul was expected to ultimately reduce healthcare costs for the consumer and the country, as information would be easier to share and superfluous tests and treatments might be reduced. Yet some say that EHRs, which were originally optimized for billing, not patient care, have made it easier to "upcode" and inflate a bill, although measures have been implemented to help catch such fraud as well.

Perhaps the most obvious growing pain for this system was the development of the EHR software itself. There was little control imposed over the developers, and almost any system seemed to be qualified as 'government certified.' Because of the huge cash incentive for developers to bring a product to market immediately, what could have taken a decade to mature was attempted in a few short years. The marketing frenzy that ensued led to lavish dinners courting doctors, high-dollar trips around America on advertising tours, and the eager adoption of systems that were not truly ready to be implemented on a large scale. "Athenahealth held "invitation only" dinners at luxury hotels to advise doctors, among other things, how to use the stimulus to get paid more and capture available incentives," states the Fortune and KHN article.

With such a focus on quick adoption to cash in on the government incentives, the oversight available was not enough to keep up. This may have contributed to the growing evidence that some doctors and health systems overstated their use of the new technology, leading to a potentially enormous fraud against Medicare and Medicade that will take years to unravel. The HHS inspector general estimated that, by June of 2017, Medicare officials had sent more than $729 million in subsidy payments to providers that didn't deserve them. Further audits have discovered overpayments in 14 of 17 state programs that were reviewed, totaling more than $66 million.

Our summary coverage will conclude next month with a review of interoperability.



Cities have been falling prey to ransomware attacks at a growing rate. From the Atlanta, Georgia attack in 2018 that lasted weeks, to the Baltimore, Maryland attack that took the city offline, hackers are systematically targeting city governments. There are several characteristics that make governments lucrative. These complicated and consistently underfunded systems are often years behind on the technology front. It is unlikely that the computers in the networks will be updated or that they will be actively monitored to detect threats. It is also likely that the cities do not have adequate backups of their data, preventing them from being able to easily restore their network functions after a ransomware attack. And, knowing how delinquent the technology is, paying a ransom to restore systems will be vastly cheaper than rebuilding and updating a network from scratch.

All of these traits make city governments a lucrative target for hackers. And hackers have been taking note. However, not all cities agree to pay the ransom. Baltimore, for instance, followed the advice of the FBI and chose to not pay a ransom of over $75,000 to restore their systems. The main reasons were that there was no guarantee of restoration once the ransom was paid, and that the money paid in ransom would not actually be helping the city improve – it would merely be a precursor to all the money they would have to pay to update and improve their cybersecurity anyway.

Indeed, mayor Bernard Young of Baltimore estimated that the attack would cost the city $10 million, in addition to an estimated $8 million lost while the city was offline. This figure could rise as Baltimore continues to pay for cybersecurity experts to improve their systems and defenses.

A ransom of $75K may seem reasonable next to a cost of $18 million, but recently the US Conference of Mayors adopted a resolution to no longer pay ransom demands to alleviate ransomware infections. The Conference of Mayors includes over 1,400 mayors from across the US, all representing cities with a population of over 30,000.

The conference noted that 22 ransomware attacks on city or state governments had already happened in 2019 alone. Many of them are successful in extracting a payment from cities. Two Florida cities paid a combined $1 million to hackers for decryption keys to unlock their data. However, even after a successful decryption, cities have to go through a rigorous rebuilding process to prevent further attacks, and this almost always costs more than the initial ransom. For that reason, many experts advise against giving any of that money to the hackers.

The Conference of Mayors stated that "Paying ransomware attackers encourages continued attacks on other government systems, as perpetrators financially benefit. The Unites States Conference of Mayors has a vested interest in de-incentivizing these attacks to prevent further harm."