HTA POST

Volume 5
Issue 7
July 2021

Healthcare Technology Advice for the Modern Independent Practice

WHAT'S NEW

Missouri's Medication Database

On Monday, June 7th, Gov. Mike Parson signed a bill that will establish Missouri's prescription drug monitoring database. With Missouri's adoption, every state in the Union now has such a database in place. The programs aim to track and flag possible misuse of prescription painkillers and some anxiety medication, the abuse of which has led to the opioid epidemic in America. The medication data will enable healthcare professionals to make informed decisions on prescriptions.

UPCOMING EVENTS

See more at: *htadvisorsllc.com/events*

IN THIS ISSUE

Healthcare Technology Advisors

REFERRAL

Want to get up to $2,000 OFF your annual IT investment?

WIN a FREE iPad and EARN credits with HTA's Referral Rewards Program!

Learn more at:
htadvisorsllc.com/about-us/referral-program

This monthly publication is provided courtesy of Derrick Weisbrod, CEO, and the Healthcare Technology Advisors Team.

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.

STAYING INDEPENDENT AS A MEDICAL PRACTICE

There are many towns across the country without a single independent medical clinic. As our healthcare system becomes over more complex, many providers chose to work with large networks of clinics or with their local hospital to take the burden of administration off their shoulders. However, we've talked to many providers who vehemently believe in staying independent, even if they are the last such practice in town.

One key aspect of remaining independent is the ability to choose your location. While large hospitals in Missouri are centered in St. Louis and several population hubs, there are many thriving towns that support multiple independent medical practices. The independent doctors and practice managers we spoke to said that choosing a location close to their home or in a specific community they wanted to support was important to their choices of working independently.

The biggest factor in remaining independent for the majority of our clients is their focus on patient care. Many stated that the bureaucracy and red tape of working in a hospital system, where they had no control over who was hired, fired, or worked with whom, was a drain on their mental energy and affected the care they were able to deliver. As an independent physician, they are able to put that energy into their patients, and craft a clinic that delivers exactly the type of care they want to be associated with.

On this fourth of July holiday, consider what opportunities being an independent practice has afforded you, and how you can use those to further your goals.

TECH TIP: HOW TO REDUCE THE COST OF RANSOM ATTACKS

The recent national and international news of the Colonial Pipeline cyber attack has prompted many businesses to look critically at their cyber security infrastructure. While Colonial Piepline spent millions on their IT network many businesses simply don't have those resources. Even with their robust safeguards, they still chose to pay millions in ransom in an effort to restore their data quickly.

The average ransom paid has tripled over the last year alone, to an average of $300,000 per incident. However, the total cost of an average attack is $1.85 million. This includes the ransom cost, cost of repair, and lost revenue.

Does that cost seem astronomical to you? Surely a small business would never incur such a high cost. Yet many small businesses are suffering from targeted cyber attacks that demand ransoms or wreck their infrastructure.

A key way to help recover from such attacks is to have Cyber Liability Insurance. This coverage helps you respond effectively to a cyber attack by covering your costs as you repair systems, recover data, pay for expert help, and settle any litigation that arises from a data breach.

Your IT team can help you find the right Cyber Liability coverage for your business -

HIPAA FINE SPOTLIGHT
$25,000

Peach State Health Management Clinical Laboratory

The Health Insurance Portability and Accountability Act (HIPAA) is a complicated set of best practices, expectations, and procedures. It is always evolving and being added to with new standards as our technology improves.

At times, it can feel overwhelming.

If you're a small medical practice without a dedicated security officer, what do you do to tackle the workload? There are programs, software, or third party vendors who can help you work through the steps. Healthcare Technology Advisors handles HIPAA risk assessments and policies for many of our clients, along with our technology and legal partners.

Even though this represents a cost, it can no longer be ignored. In December 2017, the Office for Civil Rights (OCR) initiated a compliance review of Peachstate Health Management, LLC. Based in Georgia, this medical practice was doing business as AEON Clinical Laboratories and providing diagnostic and laboratory tests, including genetic testing services.

Note that there was no data breach that caused the OCR to act. However, in their investigation they found systemic non-compliance with the HIPAA Privacy and Security Rules. Peachstate had failed to conduct the mandatory risk assessments, had no risk management and audit controls, and did not document their HIPAA policies and procedures.

The cost of Peachstate's non-action was a $25,000 settlement.

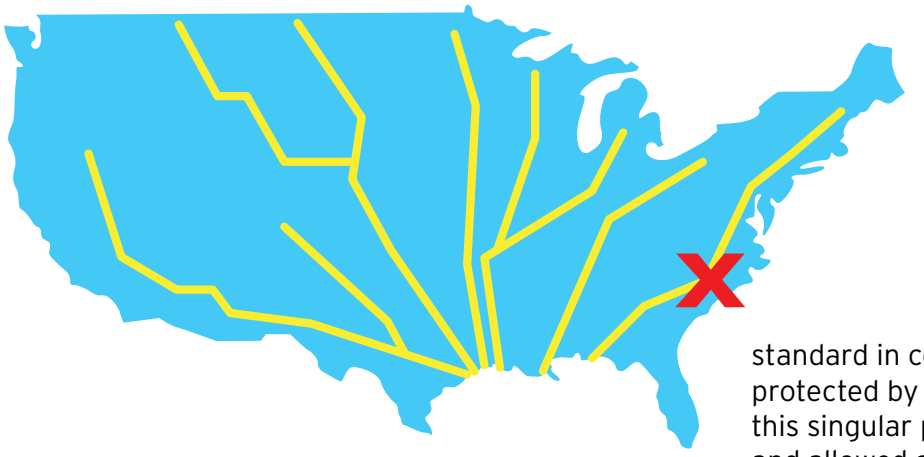
"Clinical laboratories, like other covered health care providers, must comply with the HIPAA Security Rule. The failure to implement basic Security Rule requirements makes HIPAA regulated entities attractive targets for malicious activity, and needlessly risks patients' electronic health information," said Robinsue Frohboese, Acting OCR Director. "This settlement reiterates OCR's commitment to ensuring compliance with rules that protect the privacy and security of protected health information."

Healthcare Technology Advisors has several option to help your practice implement Security Rules.

Don't know where to start?

Start by going to htadvisorsllc.com/mitigate-hipaa-risks to take our HIPAA Readiness Quiz and learn what areas your practice needs to focus on first. Then call us at (314)312-4701 and let us help you get your HIPAA house in order.

WHAT THE COLONIAL PIPELINE RANSOM ATTACK REVEALS ABOUT AMERICAN INFRASTRUCTURE



On Thursday, May 6th, hackers launched a cyberattack against Colonial Pipeline. They stole 100 gigabytes of data, then proceeded to lock computers and systems down while demanding a ransom payment. By the next morning, Colonial Pipeline had both paid nearly $5 million in an attempt to recover their data and taken several key systems offline to prevent further damage. This move shut down their fuel delivery systems throughout the east coast of America.

While the company scrambled to implement alternative fuel delivery systems, leaning on truck or train, their main pipelines remained inoperable. Smaller lines were brought back on manual control. As the situation developed over the weekend, by Monday May 10th the American public was aware of the attack and the consequences; fuel may be running low.

By Wednesday May 12th over 1,000 gas stations were out of fuel amid a panicked run on gas. Officials warned consumers to not store gasoline in plastic bags. Cars waited in long lines for gas, and experts pleaded for people to not hoard gasoline. After all, it was only a temporary shortage as the Colonial Pipeline began operating its main lines that very day.

What caused all this mayhem? A security safeguard that wasn't quite strong enough, and a lack of rapidly-deployable backups.

In a statement to congress, CEO Joseph Blount revealed that the compromised account was not protected by two-factor authentication (2FA) as is standard in corporate security. Rather it was protected by one password, albeit strong. It was this singular password that became compromised and allowed a Russian-based hacker group known as Darkside to infiltrate and encrypt Colonial Pipeline's network.

Although the company initially stated it would not pay a ransom, it did quickly supply 75 bitcoin, valued at around 4.5 million USD, to the hacker group in an attempt to restore their offline systems. However, the decryption program provided by Darkside worked so slowly that Colonial Pipeline ended up restoring their systems from their own backups. Colonial Pipeline, despite investing heavily in IT and cyber security, had never developed a cyber attack response plan.

Even though the Darkside attack did not target any physical infrastructure such as the controls for the fuel pipes themselves, their attack on the systems that handled billing for the company still shut down the entire operation. And with one company attacked, the eastern seaboard was without 80% of its fuel supply. Despite the economy being heavily dependent on this private company's service, there are no regulations on how Colonial Pipeline protects itself, its IT infrastructure, its physical infrastructure, or its data.

The most obvious conclusions to draw from this incident are to enable 2FA on all critical infrastructure and to deploy tested backups to enable restoration from any ransom attack. Yet, according to Sen. Maggie Hassan of New Hampshire, "it is a wake-up call that more must be done to secure our critical infrastructure."