HTA POST

Volume 5
Issue 11
November 2021

Healthcare Technology Advice for the Modern Independent Practice

WHAT'S NEW

Bring on the crisp fall weather, the pumpkin patches, and the food comas! There's so much to be thankful for after a tumultuous year, and Healthcare Technology Advisors is ready to embrace the season!

UPCOMING EVENTS

Tuesday 16th 12pm: MGMA St. Louis Webinar *Navigating Practice Transitions* presented by Dale Kreienkamp

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?

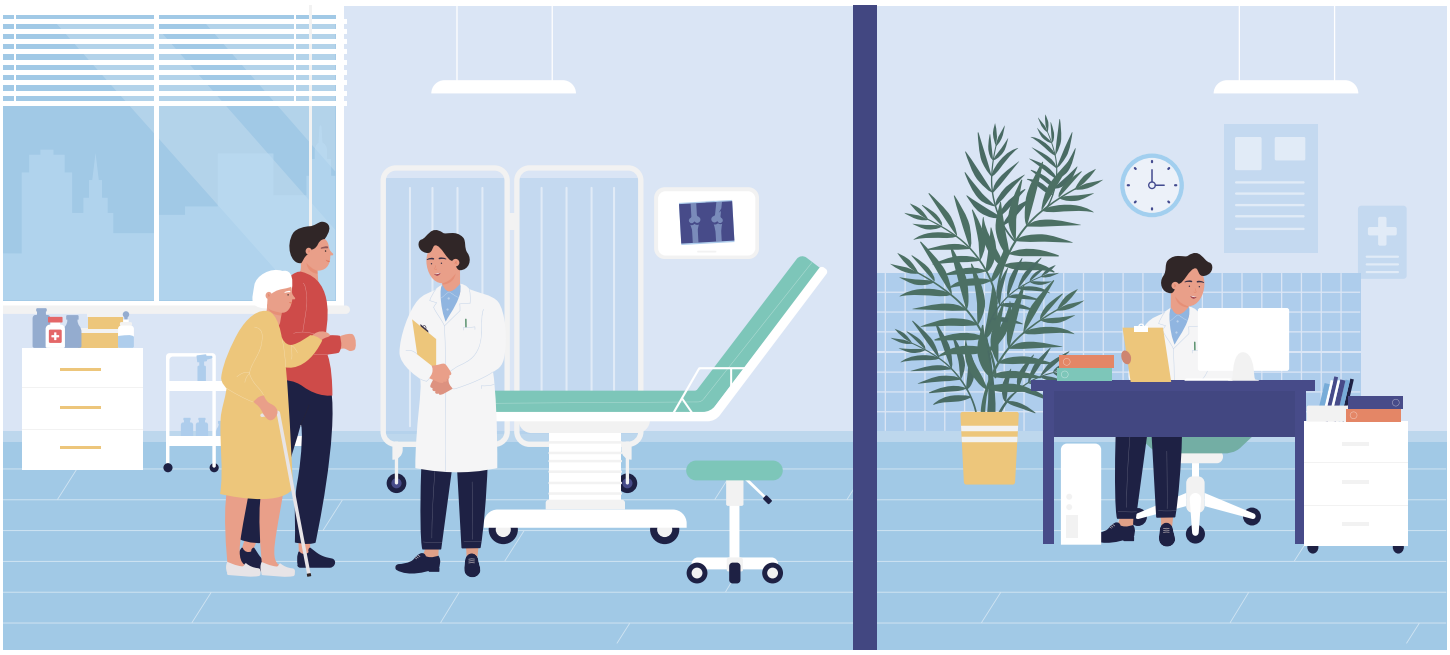
WIN a FREE iPad and EARN credits with HTA's Referral Rewards Program!

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.

BREACH REPORT: PREMIER PATIENT HEALTHCARE



Who? Texas-based Premier Patient Healthcare.

What? Unauthorized access of 37,636 records containing protected information.

How? A former executive accessed the information after their employment was terminated.

Of all the ways protected information can be stolen, malicious insider is perhaps the most distressing. Patients trust their doctors with personal and private information, just as employers trust their workers to have discretion and follow protocols.

When an employee is on their way out, either amicable or not, there are often policies in place to protect the interests of the former workplace. Non-compete and non-disclosure agreements are often used in the healthcare industry. The policy to protect patient information is, of course, HIPAA.

It is the duty of the covered entity to protect that information.

A retired doctor or fired executive shouldn't access patient information - but more than that, they should not be ABLE to access it. Offboarding an employee should involve resetting or removing all access to their accounts and scrubbing any protected information off their devices.

This can include deleting their accounts, changing passwords that they had access to (and may remember) and removing their authorization to access protected information on any internal or externally associated databases.

In June of 2020 a terminated Premier Patient Healthcare executive accessed nearly 38,000 records. The investigation believes that they did so through a third-party technology vendor. It is likely that the executive's accounts with this vendor were never updated or deleted, thus leaving the high-level access in place.

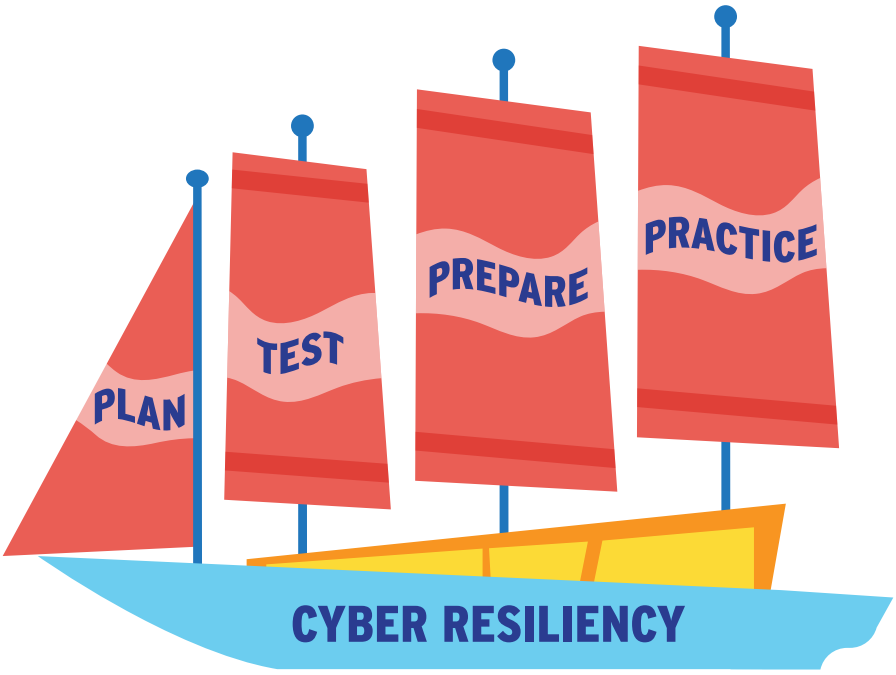
The breach was not discovered until nearly a year later in April 2021. The investigation has not found any evidence of intended or actual misuse of the data. However, even if the breach was accidental or innocent, it is a stark reminder of how vulnerable patient data is when covered entities are not enacting and enforcing the policies that HIPAA requires them to have.

Healthcare Technology Advisors believes in guiding our clients through policies, procedures, risk assessments, and audits to ensure that nothing falls through the cracks. If you're not 100% confident that your practice is protecting patient data correctly, schedule an appointment now with our HIPAA experts by calling (314)312-4701.

HOW RESILIENT IS YOUR PRACTICE?

Cybersecurity can be bewildering. Your business faces threats from all sides daily, so you want to be sure that you've got the right protection in place. An estimated 25% of business owners say that they don't even know where to start when it comes to protecting their companies from cyberattacks. However, by concentrating your efforts on making one security improvement, you can put a great foundation in place to protect your business from trouble.

That security improvement is building your company's cyber resilience (sometimes called cyber resiliency). That concept means that you've built defenses that not only protect your business from cybercrime, but that also make it easy for your business to keep chugging along in the face of adverse conditions like a cyberattack. **A cyber resilient business is ready for anything.**



How can you do that? Start by creating an incident response plan. Set up a formal procedure that details the who, what, when, why, and how of handling a cybersecurity incident. For example, what if an employee realizes that they've fallen for a phishing attack? Who do they inform, and how is the incident handled? Or if your company falls victim to a ransomware attack, do you know who needs to get to work right away and what they'll do to right the ship?

Having a formal, tested incident response plan is critical to keeping your business from losing productivity and revenue if it grinds to a halt as everyone scrambles to deal with a problem. IBM reports that only 39% of companies with a formal, tested incident response plan experienced a disruptive security incident last year, compared to 62% of companies that did not have formal, tested incident response plans.

Take some time to sit down and make sure that everyone knows what to do in the event of a cybersecurity incident. In order to ensure that your employees know what to look for, make sure everyone is undergoing regular security awareness training. That's a boon to your defense too – companies who run regular security awareness training using a solution like BullPhish ID have 70% fewer cybersecurity incidents in the first place.

Start your journey to improved cyber resilience now and you'll be ready for what the future holds.

Schedule a demo of BullPhish ID with Healthcare Technology Advisors today.

CRYPTOCURRENCY: MAINSTREAM PHENOMENON OR DARK WEB DARLING?

Cryptocurrency has many faces. For some it is an exciting math and social science experiment, charting the rise and fall in value and then making predictions. An exclusive mini stock market of sorts.

For others it's a complete mystery, as unintelligible as binary, and they would like to keep it that way.

For cybercriminals, cryptocurrency represents a clandestine and untraceable way to get paid. Most ransom demands are only payable in bitcoin, and transactions in the dark web also use cryptocurrency for security and safety.

Cryptocurrency has gone mainstream in many ways. It is spoken about and written about in the news with the same seriousness as any other currency. That shows that although it is a dark web darling, crypto has also gone legit – and that makes it an even bigger target for cybercrime.

5 Essential Things to Know About Cryptocurrency

- There are over 5,000 different currencies.
- Bitcoin is the most common, but not the only, digital currency used in ransomware attacks.
- Ransomware groups snatched at least $81 million in crypto from victims by May 2021.
- The U.S. Federal Bureau of Investigation managed to recoup 63.7 of the 75 Bitcoins paid by Colonial Pipeline after their ransomware attack.
- Almost 80% of Americans polled in a recent survey were aware of Bitcoin and 32% were aware of Ethereum, two of the biggest brands in the cryptocurrency world.

The cryptocurrency world has just begun its journey into the mainstream business world, but it's already witnessing an uptick in the kinds of cyberattack threats that were previously reserved for investment firms and financial institutions. In recent months, cyberattacks at two major crypto exchanges have demonstrated the danger that cryptocurrency is in, as well as the danger that such a volatile investment presents for investors.

The top way that bad actors use to snag unwary crypto fans into their traps is phishing. **Specifically, social media phishing.** While that is a growing area of phishing for cybercrime in general, it's the king of the con in the cryptocurrency industry. Experts estimate that almost 55% of cyberattacks that swindled people out of their cryptocurrency (or the passwords to their digital wallets) came from threat actors impersonating representatives of hot tech and retail brands, posing as employees of cryptocurrency exchanges, or pretending to be celebrities and executives from an array of industries on social media. **But it's just as much of a danger to businesses, too – social media threats targeting enterprises have increased 47% since January 2021.**