HTA POST

Volume 4
Issue 11
November 2020

Healthcare Technology Advice for the Modern Independent Practice

WHAT'S NEW

Whether you're facing travel restrictions, health concerns, or families in quarantine, this Thanksgiving is likely to be toned down. If you and your family are forgoing the large, expensive feast this month, consider banding together to donate to local charities or food banks instead. Share a drink over Facetime, connect over the phone, and be united in helping your community celebrate in these trying times.

UPCOMING EVENTS

Wednesday, November 4th

12-1pm
MGMA Webinar
presented by Tammy Krebel
"Healthcare's Next Normal"

See more at:
htadvisorsllc.com/events

IN THIS ISSUE

Page 2 - Client Spotlight: Saint Louis Rheumatology
Lydia's House Holiday Project 2020

Page 3 - Bullphishing: Proactive Cyber Security Training

Page 4 - HIPAA Fine Spotlight: $1.5 Million

Healthcare Technology Advisors

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!

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.

CLIENT SPOTLIGHT OF THE MONTH: SAINT LOUIS RHEUMATOLOGY

Saint Louis Rheumatology specializes in the diagnosis and treatment of rheumatic and autoimmune diseases. They also focus on researching a wide variety of autoimmune and rheumatologic diseases, including rheumatoid arthritis, lupus, psoriatic arthritis and many others.

At Saint Louis Rheumatology, every patient is paired with their own medical team consisting of a physician assistant and a rheumatologist. The team works together combining physical examinations, medical history, sophisticated immunologic and imaging tests to achieve an accurate diagnosis in the most efficient and effective manner.

Healthcare Technology Advisors has been proud to work with Saint Louis Rheumatology as they expended and grew their practice (formerly Clayton Medical.) You can find them online at stlrheum.com

LYDIA'S HOUSE HOLIDAY PROJECT 2020

This year HTA is partnering with Lydia's House St. Louis to promote their Holiday Project.

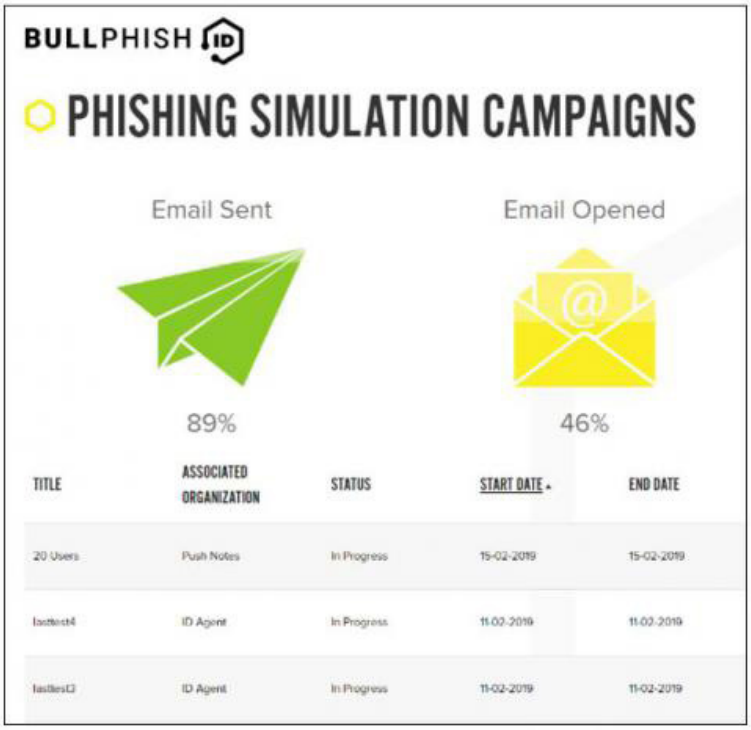
The Lydia's House Holiday Project is a time to support 50 families. With the help of individuals, families, and businesses, Lydia's House will provide gift and meal baskets for 50 adult women and 85 children.

By adopting a family, you can make a direct difference in their holiday season by providing gift baskets. Lydia's House will select a family for you to adopt and send you the wish list and ages of the children. You also have the option of providing a holiday meal basket consisting of non-perishable items and grocery store gift cards for meat products.

Lydia's House works year-round to provide a safe harbor for victims of domestic violence. Abused women and their children are able to find safe, secure long-term housing where they are able to rebuild their financial, emotional, and social lives until they are able to move out into their own housing. This is the only shelter of its type in the greater St. Louis area.

We hope all our clients and peers will join us in supporting Lydia's House and their residents during this holiday season. To register for the Holiday project and learn more, please visit their website at **lydiashouse.org/holiday-project**

BULLPHISHING: PROACTIVE CYBER SECURITY TRAINING



As we've detailed in the past, 2020 is fast becoming the year of spear-phishing. Spear-phishing is defined as "the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information." Whereas normal phishing scams may just try to dupe you into logging into your Facebook or Apple account, modern spear phishing focuses on targeting specific individuals, both to imitate and to "phish." The hacker may choose to spoof the email of a CEO, and send a directive to the administrative assistant of the CFO. They mimic not only the email address, but the language and writing style of the CEO. The aim is to make the correspondence seem as normal and legitimate as possible. And more often than not, it works.

For nearly every cyber security threat, the solution is twofold; technological mitigation, and employee education. But, educating people about the risks of email scams can get repetitive, and once the basics are understood it's hard to keep employees engaged. So, what if you could have your employees actually PRACTICE responding to a scam?

Healthcare Technology Advisors is offering an educational service where we do just that. First, employees are given training on how to detect phishing scams, how to react to suspicious emails, and what preventative measures are in place to protect their networks and computers. Then, an email is sent out (by us) that aims to imitate a trusted source and attempts to get the employees to give up valuable information such as their log-in credentials.

After the test is sent out, we gather all the information and report it back to your practice. This is a great educational tool, as it will reveal where your practice has security deficiencies, and also is a safe way to train and teach employees about phishing scams.

Everyone believes that they would never fall for a scam, be it from a conman or email. Until the day they do. Instead of having that day be disastrous for your practice, it could be educational and actionable if done during a bullphishing training exercise implemented by Healthcare Technology Advisors.

HIPAA FINE SPOTLIGHT: $1.5 MILLION

ORTHOPEDIC CLINIC PAYS $1.5 MILLION IN OCR SETTLEMENT OVER SYSTEMIC NONCOMPLIANCE

In September, the Office for Civil Rights reached a settlement with Athens Orthopedic Clinic for $1.5 million over a 2016 data breach caused by the notorious hacking group known as "thedarkoverlord" (TDO). The OCR audit into the security incident revealed systemic noncompliance with the HIPAA rule.

A journalist first notified Athens Orthopedic that some of their patient records may be posted online for sale on June 26, 2016. Two days later, TDO contacted the clinic and demanded payment in order for the complete patient records to be returned.

Athens Orthopedic's investigation revealed TDO leveraged credentials stolen from a third-party vendor on June 14, which gave them access to its electronic medical records system and a trove of sensitive patient health information, including Social Security numbers.

Although Athens Orthopedic terminated those compromised credentials, TDO had access to its EHR for more than a month until July 16, 2016.

The hacker then posted the stolen data online and on the dark web, after failing to extort the provider. Patients soon filed a lawsuit against Athens Orthopedic arguing the provider was negligent, breached implied contract, and "unjust enrichment." A judge recently revived the case after an initial dismissal.

On July 26, 2016, Athens Orthopedic reported the breach to OCR, which then launched an audit. The OCR investigation revealed a range of longstanding, systemic noncompliance with the HIPAA Privacy and Security Rule, which included failing to conduct a risk analysis, implement risk management and audit controls, and the requirement to implement sufficient security measures to reasonably reduce risks and vulnerabilities.

OCR also found the clinic did not maintain HIPAA policies and procedures, nor secure business associate agreements with multiple business associates until August 7, 2017. Athens Orthopedic also failed to provide HIPAA Privacy Rule training to workforce members until January 15, 2018.

The investigation also found the clinic did not follow the HIPAA requirement to implement sufficient hardware, software, and or procedural mechanisms for recording and examining activity in information systems that contain or use ePHI from September 30, 2015 to December 15, 2016.

"Hacking is the number one source of large health care data breaches," OCR Director Roger Severino, said in a statement. "Healthcare providers that fail to follow the HIPAA Security Rule make their patients' health data a tempting target for hackers."

The Athens Orthopedic settlement is just the fourth breach-related settlement this year, as OCR laxed enforcement amid the COVID-19 pandemic: LifeSpan Health System ($1.04 million), Agape Health ($25,000), and Steven Porter, MD in Ogden, Utah ($100,000).