# HTA POST

Volume 3
Issue 2
February 2019

*Healthcare Technology Advice for the Modern Independent Practice*

## WHAT'S NEW

**Lydia's House Gala**

The team at HTA would like to invite you to join us at Lydia's House Charity Gala, A Night for Hope and Healing, this month! Come for a fabulous evening of fun, auctions, raffles, dinner and dancing to support the wonderful work of Lydia's House, a local charity that supports the victims of domestic violence and their children. The Gala will be held in Chesterfield at The Double by Hilton on Saturday, February 23rd.

Visit *lydiashouse.org* to purchase tickets!

## 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, February 13** | 8-11am<br>MGMA Annual Medicare Update |
| **Saturday, February 23** | 6-10pm<br>Lydia's House Gala |
| **Wednesday, February 27** | 11:30am-1pm<br>SEMO MGMA Monthly Lunch Meeting |


**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.

## JOIN MGMA FOR THESE GREAT BENEFITS AND MORE!

The invitations have gone out! This year, consider joining the Medical Group Management Association to take advantage of an amazing group of peers and mentors. Greater St. Louis MGMA offers a diverse program of educational content and networking opportunities:

1. Attend monthly lunch meetings to hear speakers present on topics that inform and expand the conversation about medical practice management. Members get discounted registration.
2. Participate in several webinars a year – free for members – that let you enjoy quality education right from your computer.
3. The Annual Conference each fall represents a full day of education for experienced and new practice managers as well as A/R professionals – with the added benefit of in-person networking with your peers and business partners.
4. Gain valuable insights from the monthly newsletter packed with advocacy updates, events, and chapter information, and share your expertise and knowledge by participating in the mentor program.
5. Gain board certification and fellowship status to become nationally recognized as an expert in your field.

**Join or renew your membership online at *mgmastl.org* or call 314-499-9344!**

## BEST PRACTICE OF THE MONTH: UPDATES AND PATCHES

One of the first building blocks of any security plan is to implement regular, managed updates on all computers in a network. These updates can be both scheduled Operating System (OS) updates or security patches that are released as needed. OS updates often include quality of life improvements, greater functionality, or fixes for known bugs. Security patches, on the other hand, are often reactively published in response to a vulnerability being discovered. These may be discovered by in-house security teams – the good guys – or by malicious hackers.

What happens if you don't manage the regular installation of these updates? Your computers may not work as well as they could, as they'll be missing out on new improvements to the software. But the true danger lies in bad actors who can take advantage of discovered vulnerabilities – often released by the OS developer themselves shortly AFTER they have been patched. Once a fix has gone out to close a loophole, it's a race for the bad guys to find a way to exploit it and try to infect systems BEFORE the vital security patch has been installed.

A stark example of this is found in the WannaCry attack of 2017. This ransomware attack took advantage of a vulnerability that had already been patched by Microsoft two months earlier. However, the virus was able to infect machines that had either never installed the update or were so old they were past their end of life and were no longer receiving these vital security updates. One system that was affected was the United Kingdom's National Health Service. This attack forced hospitals to turn away patients and re-rout ambulances. It was found that many of the affected hospitals were still running Windows XP, an OS well past its end of life at the time.

With cyber attacks on the rise, every medical practice must manage the updates and patches on all computers in their network. Healthcare Technology Advisors can make it easy with our Cyber Security offering. **Call (314)312-4701 today to learn more.**

FEBRUARY 2019

# BREAKING! LATEST BREACH NEWS!

## WHAT'S NEW IN BREACH NEWS

**The Risk of 3rd Parties**

The Managed Health Services (MHS) of Indiana Health Plan recently announced that a third-party data breach had potentially exposed up to 31,000 records containing patient's personal data. The party in question is LCP Transportation, which provides non-emergency medical transportation solutions. As LCP handles the claims submission and processing for their patient's insurance, a hefty amount of personally identifiable information (PII) flows through their system.

The breach originated from a phishing email attack on LCP Transportation. Phishing attacks are becoming more and more prevalent as hackers realize that the easiest way into an organization is not through code or website exploits, but rather through the weakest part of any security plan: the people.

The MHS of Indiana had a Business Associate Agreement (BAA) with LCP Transportation, so they are not liable for the breach that occurred and exposed their patient's data. As a Business Associate of a Covered Entity, LCP Transportation is directly responsible for complying with HIPAA rules. This clearly demonstrates the importance of acquiring BAAs from any vendor working with a medical practice of any size. Had a BAA not been in place, MHS would have been responsible for paying any fines that resulted from this breach.

This breach of 31K patient records demonstrates both the danger of working with third parties and the importance of acquiring a BAA from any such party. So long as the third party understands their responsibility as a Business Associate and complies with their contractual agreements, which include fully following all HIPAA rules and regulations, the covered entity assumes no extra risk. However, if they do not have a BAA in place, all responsibility falls to the covered entity in the event of a breach, and all fines levied must be paid by the covered entity, not the third party.

# HIPAA FINE SPOTLIGHT - $125,000

In November of 2018, a small Allergy practice in Hartford, Connecticut agreed to pay $125,000 to the Office for Civil Rights (OCR) to settle a HIPAA violation. The practice, Allergy Associates of Hartford, P.C. is comprised of three doctors across four locations.

The fine was levied due to an improper disclosure of patient information. It started with a patient who contacted a local television station over a dispute between the patient and an Allergy Associate's doctor. In the course of their reporting, the reporter reached out to the doctor for comment. The doctor then disclosed the patient's protected health information.

The OCR investigation revealed several problematic issues with this situation. First, and obviously, the doctor showed reckless disregard for his patient's privacy. However, it was discovered that prior to speaking to the reporter, this doctor was instructed by Allergy Associate's Privacy Officer to either not respond at all or respond with "no comment." The practice knew what was correct and instructed this doctor appropriately, yet the doctor still chose to deliberately put his practice at risk by knowingly violating HIPAA privacy rules. In spite of this blatant affront, Allergy Associates did not take any disciplinary action against the doctor. Although they knew what was correct, they were unwilling to implement real consequences.

It is in situations like this that the OCR will be sure to levy fines against a practice. Both the doctor and the practice seemed to believe that they were above the law in this regard, either thinking that they would not be reported and caught, or that the OCR would decline to take action against them. Had both the action of the doctor and the inaction of the practice not been so blatant, they may have been given leeway to correct their actions, however it was obvious both parties made clear choices about their priorities.

Allergy Associates agreed to pay $125,000 as settlement for this case. In addition, they have been instructed to undertake a corrective action plan that will involve monitoring their compliance with HIPAA for two whole years. The fact that they had a known issue, and failed to do anything to prevent or correct it, means they must now prove their compliance instead of simple avoiding a breach.

Many small practices believe that they will never suffer a data breach of great enough magnitude to warrant an OCR investigation, but it is important to remember that personnel issues represent as great a risk to HIPAA compliance as IT. Make sure that your practice not only has policies and procedures in place, but that they are FOLLOWED in the event of a breach of any sort or origin.