HTA POST

Volume 3
Issue 3
March 2019

Healthcare Technology Advice for the Modern Independent Practice

WHAT'S NEW

HTA would like to invite you to join us at the Practice Management Summit in O'Fallon, IL. This three-day conference has been organized by the HFMA of Southern Illinois with support from MGMA Illinois and the Illinois Critical Access Hospital Network and features educational content devoted to excellence in practice management. Topics covered include revenue cycle optimization, leadership development, employee engagement, and IT development. Derrick Weisbrod of HTA will be presenting on Thursday morning, and HTA will be present during all three days. We hope to see you there!

Visit our Events page for links to registration and more info.

IN THIS ISSUE

Page 2 – HTA Advisory Board WINNER: Sarah Jensen of Regional Dermatology

Best Practice of the Month: Backups and Disaster Recovery

Page 3 – HIPAA Fine Spotlight

Windows 7 End of Life Update

Page 4 – Phishing attacks on the Rise

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

Wed-Fri March 13-15 — Practice Management Summit 8am-5pm O'Fallon, IL

Wednesday, March 20 — Greater St. Louis MGMA Luncheon 12-1pm

How to Keep Great Employees presented by Bryan Buesking

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.

HTA ADVISORY BOARD

Congratulations to Sarah Jensen of Regional Dermatology!

Dr. Sarah Jensen was the Grand Prize winner for our Q4 Quarterly Referral Drawing. You may have seen our livestream of drawing the winning name and giving Dr. Jensen her prize. Located in the Festus and Crystal City area, Regional Dermatology welcomes patients of all ages and treats a wide range of dermatological skin conditions. They are your best resource for compassionate care!

We hope Dr. Jensen makes good use of the gift, and we would like to thank EVERYONE who went out of their way to refer us to their peers. Our mission of raising the bar for Healthcare IT is ongoing and being able to reach out to the friends and colleagues of our amazing clients makes the path all the more enjoyable.

Do you know all the levels of rewards in our referral program? For every qualified referral, we'll send you a $10 gift card- just to say THANK YOU for thinking of us! If we have an appointment with that referral, we'll send you another $25 gift card.

Then, if that referral becomes a new managed client ofnours, we'll credit your business up to $1000 off your bill!

And, perhaps best of all, every referral gets you one entry into our grand prize drawing. The Grand Prize can be won by ANYONE who is a client of ours (not just the boss!)

We call our referees the HTA Advisory Board – get your name on the board today!

BEST PRACTICE OF THE MONTH: BACKUPS AND DISASTER RECOVERY

As we leave (most of) the ice and snow behind us and enter the season of thunderstorms and flash floods, every practice must ask themselves if they are disaster proof. Whether the disaster is severe weather such as lightning storms and flooding, a fire, or man-made problems like loss or theft of equipment, the recovery aspect is much the same. For medical practices covered by HIPAA, it is also mandatory.

HIPAA regulates that all covered entities must securely back up "retrievable exact copies of electronic protected health information" and must be able to fully "restore any loss of data." This backup must happen frequently, though there is some adjusting for size here. It would be unreasonable to expect all practices to fully back up all data on minute-by-minute basis, however data should be backed up at least every business day. Importantly, data must be recoverable. How do you ensure that? Test the backups! Data should be fully restored from backups periodically to make sure the entire process is working as it should. Simply checking that a backup has happened is not enough, as this does not prove that the backup is functioning properly or that the recovery process is working.

Having your data backed up is only half the battle. HIPAA rules also mandate having policies and procedures in writing (and probably backed up!) that detail your contingency plans. These policies will not only detail how and when data is backed up, but also what steps your practice will take to recover after an event. This Disaster Recovery Plan should be useful to reference any time data is lost due to power surges, destruction, theft, or malicious activity.

Healthcare Technology Advisors offers HIPAA compliant backup solutions to all our clients, and Disaster Recovery Plans as part of our compliance service for Covered Entities and Business Associates.

Call us or visit *htadvisorsllc.com/data-backup-and-disaster-recovery* to learn more.

HIPAA FINE SPOTLIGHT - $500,000

Advanced Care Hospitalists (ACH) of west central Florida agreed to pay $500,000 to the Office for Civil Rights (OCR) as settlement for potential violations of the HIPAA Privacy and Security Rules. ACH provides contracted internal medicine physicians to hospital and nursing homes, and has been in business since 2005.

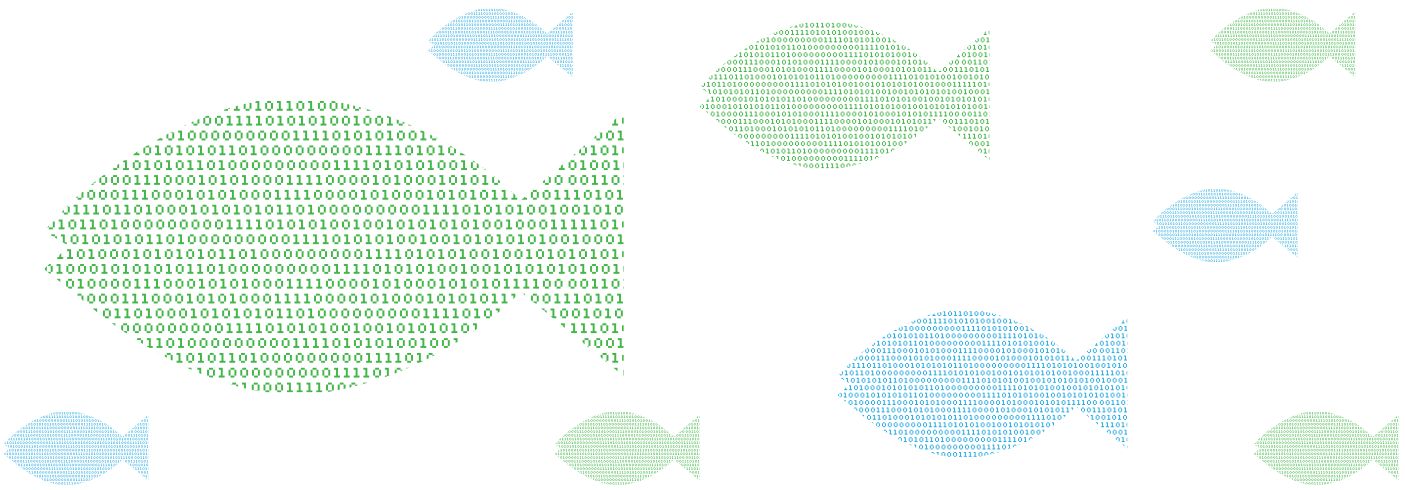
Between November 2011 and June 2012 ACH worked with an individual who claimed to be a representative of Florida-based company Doctor's First Choice Billings, Inc. This individual provided medical billing services to ACH using the name and website of Doctor's First Choice Billings, yet allegedly did so without the knowledge or permission of First Choice's owners.

Problems arose when a local hospital notified ACH that patient information was viewable on First Choice's website, including name, date of birth, and social security number. ACH subsequently identified 400 patients who were affected, and filed a breach notification report on April 11, 2014. After more investigation, however, they filed a supplemental breach report revealing that a total of 9,255 patients could have been affected.

The following OCR investigation revealed two very troubling things. First, ACH never entered into a Business Associates Agreement (BAA) with the individual who handled their medical billing as is required by HIPAA law. In fact, they failed to adopt any policy requiring business associate agreements until April 2014, after the breach report was filed. **Because no BAA was obtained, ACH is responsible and liable for every breach fine levied because of this event.** Second, the OCR found that between 2005 and 2014, ACH had never conducted a risk analysis or implemented security measures or any other written HIPAA policies or procedures. Essentially, ACH chose to completely ignore the HIPAA Rules, and never moved to implement the required policies until after a breach had occurred and patient data was exposed.

The fact that ACH blatantly ignored the rules they were meant to be following surely contributed to the final financial settlement amount they agreed to pay.

A fine like this highlights what is almost the worst position to put your practice in: willful non-compliance. And the worst part is that it's the patients who were hurt by having their data exposed. Not to mention that the individual handling the billing was not even a reputable employee of the company he claimed to represent, and the data could have been stolen for other more nefarious ends. To prevent a breach and fine like this, a practice need only have written HIPAA policies and procedures and implement them to the best of their ability, including obtaining BAAs from ALL third party vendors who have access to protected health information. Healthcare Technology Advisors gladly assists clients in not only performing security risk assessments but navigating the whole journey of compliance. **Visit *htadvisorsllc.com/our-compliance-solution* for more information.**



PHISHING: THE EVOLUTION OF CYBER THREAT

2019 is shaping up to be the year of the Phish. Where as 2017 and 2018 saw a rapid expansion of ransomware and crypto extortion, this year is predicted to see an increase in the type of laser-targeted phishing attacks that are hardest to prevent.

In the past, phishing scams generally took the form of brazen requests, like the infamous Nigerian Prince scheme. These emails were sent indiscriminately, casting a wide net in the hopes to catch anyone vulnerable or gullible enough to bite. They may have asked for a loan with a guaranteed return, or claim that the target has won a magnificent windfall but needs to send a small amount of money in order to secure the transfer into their account. Most people are trained to avoid such obvious bait.

The emails began adapting, however. Soon they began spoofing legitimate companies and asking for you to do things like update your password to your bank account or other sensitive data. Perhaps it's an email from company confirming an order you just placed – in fear or confusion, you may click on it to find out who placed an order in your name or with your account. These emails may contain malicious code, or link you to a spoofed website where any data you input will be stolen.

Now, the phishing scheme is evolving again. Instead of sending out a stock email to a massive list, hackers are targeting their attacks to specific companies and even specific employees. They study the language of the CEO via LinkedIn or other social media. They gain insider information, like when a CEO is going on vacation, and to where. Then, they craft an email directed to a particular employee. This email is meant to look exactly as though it came from the CEO, mimicking their communication style and utilizing either a hacked email account or an email that is almost exactly the same as the CEO in question, with only one character difference. This email may ask for a wire transfer of funds, or to verify an account number, or perhaps they forgot their password and are on the road or on a plane and they have to get this transfer done for a large client by the end of the night.

Specific, targeted, with an urgent call to action. This is the new formula for phishing attacks. Due to their intimate and customized nature, it is hard to rely on employees to make judgement calls on what communication is legitimate or not. The best defense against these types of spear phishing attacks is to document and implement standard operating procedures for everything, and then FOLLOW them. A wire transfer should never be up to one person. A forgotten password has steps to recover. And no one, not even the CEO, is allowed to bend the rules for their convenience.

Documenting these types of procedures is a big task, but the safety they offer is vital in this age of cyber threat. Call Healthcare Technology Advisors today for more information on how to prevent phishing-related breaches in your practice.