hfma™ new jersey chapter
healthcare financial management association

garden state focus
national excellence award winner

November-December 2014 • vol 61 • num 2

focus •advertisers•

focus •points•

Who's Who in the Chapter 2
The President's View
by Tracy Davison-DiCanto 3
Certification Corner 14
New Members 19-20
Who's Who in NJ Chapter Committees 21
Focus on Finance 24
Job Bank Summary 25
Mark Your Calendar 32

focus •features•

36th Annual Institute Wrap Up
by Jenniver Vanegas and Michael P. McKeever, CPA 6

NJHFMA Celebrates Our 2013-3014 Award Recipients 10

Data Breaches Highlight Value of Medical Data
by Alex Wozniak 12

Once an Overpayment, Forever an "Obligation"
The ACA's 60-Day Rule Makes Murky Business of "Identifying" Overpayments
by Leonardo M. Tamburello, Esq. 16

The Nicholson Foundation Continues to Partner with and Support the New Jersey Health Care Quality Institute and Medicaid ACO Demonstration Project
by Dave Knowlton 22

Stabilizing Health IT Expenditures While Maximizing Productivity
by Jennifer Vanegas 26

Welcome to the Education Committee
by Michael P. McKeever, CPA, CHC, CHRC 27

Utilization of Healthcare Services Special Report
Redefining Care for our Communities
by Jeff Hoffman 29

You and Your 340B Program: Are You Compliant or Confused?
by Venson Wallin and Bill Bithone;y, MD 33

In Memory of John P. Sheridan 36

focus •cover•

Courtesy Hermitage Press, Inc.

Data Breaches Highlight Value of Medical Data

Alex Wozniak

by Alex Wozniak

A data breach is the actual release or disclosure of information to an unauthorized individual/entity which may cause the affected person or company inconvenience or harm. The recent data breaches making headlines, at Target and Home Depot, resulted in the unintentional disclosure of their Customer's financial data. Unfortunately, data breaches are not limited to credit card data and other financial information. Even more valuable than the few dollars credit card numbers sell for on the black market, are health care records.[1] Health care records frequently include Social Security numbers, desirable information for stealing someone's identity.[2] New threats to the security of records in the United States healthcare system emphasize the value and demand of patient data.

A 2014 study by the Ponemon Institute indicates that criminal attacks against healthcare systems have risen 100 percent since the study was first conducted in 2010. Highlighted by recent attacks against Community Health Systems and the Healthcare.gov website, the potential cost of data breaches on the healthcare industry could be as much as $5.6 billion annually.[3]

Community Health Systems is a publically traded company that runs 206 hospitals in 29 states. According to a regulatory filing by the company in August, personal information for approximately 4.5 million patients was stolen by hackers.[4] Between April and June, Mandiant, a cybersecurity firm hired by Community Health Systems, believes Chinese hackers bypassed the company's security systems to steal personal data of patients. The stolen information did not include credit card numbers or medical information, but names, addresses, telephone and social security numbers.[5] As required by law, Community Health Systems will notify those patients whose information was stolen and the company will also be offering identity theft protection services to those individuals.

Another, and even more concerning breach occurred on the Healthcare.gov website. According to a statement released by a unit of the Department of Health and Human Services, a portion of the website was breached when hackers uploaded malicious software on a test server.[6] The server did not contain personal information and no data was transferred outside the agency, as the server was not meant to be connected to the Internet. While no data was taken in the breach, it is a valuable reminder that this website contains valuable information and will be a high value target for hackers.

A variety of factors have lead to the increased exposure of healthcare clients. A majority of healthcare organizations see the implementation of the Affordable Care Act as a contributing factor for this increased exposure.[7] While medical providers continue to store patient's medical information on paper records, government incentives are encouraging a transition of medical records to digital format. Called Electronic Health Records, the hope is that digital records will improve healthcare quality and efficiency, by allowing users to access records from different locations.[8] However, this transition also increases privacy risks. A heavy dependency on outsourced service providers mean health information is shared amongst a large number of third parties. And many healthcare organizations are not confident that their business associates would be able to detect and notify the organization if there were a data breach.[9]

The other factors contributing to the security risk are employee negligence and BYOD usage. As with any industry and business, the human element represents a weakness in even the most secure cyber defenses. A Ponemon study revealed that 75% of organizations say employee negligence is their biggest worry.[10] Despite the risk, organizations allow their employees to use their own mobile devices, such as smart phones and tablets, to access their organization's networks. These unsecured mobile devices allow yet another point of entry into healthcare systems and represent an often unintentional security risk.

Despite these security risks, there are many industry best practices that healthcare organizations can adopt to increase breach preparedness. This begins by having a breach response plan in place before an event occurs. An organization would benefit from conducting breach response exercises and pre-arranging breach response services with a security firm.

Healthcare organizations should also monitor event logs and secure remote access settings to be more aware of any outside data breaches. The most important thing an organization can do to prevent disclosure of protected information is to encrypt their data. That way, even if there is unauthorized access to the data, it is encoded and unreadable.

In our experience, the large data breaches reported by retailers like Target or Home Depot have had a limited impact on the broad spectrum of the market. Certainly, carriers will want to evaluate their larger accounts, which might be more susceptible to a mega breach due to their size. However, companies of this size already have large self-insured retentions and dedicated Risk Management departments, so the best way for the carrier to limit their exposure would be to restrict the capacity limits offered. For instance, instead of providing the insured $15 Million limits, the carrier may want to only provide half of that amount and ask the insured to find excess coverage elsewhere.

Another noteworthy issue, highlighted in the media by the celebrity exposé scandal, is the increased use of the Cloud. From what we have seen, the use of cloud based services to store data and run applications have only had a limited impact on the market. While insurance coverage is an important issue because cloud providers generally accept very limited liability, some cyber insurance policies are written with language broad enough to cover cloud computing risks. However, as the insured is still responsible for the data, the insurer will want additional information about any cloud based services used. This has resulted in supplemental applications being developed and additional questions being asked by underwriters to help them understand the insured's exposure.

As these and other breaches continue to occur, so will underwriting continue to adapt based on the claims reported. While the underwriting appetite has not changed, there is no one size fits all approach to this coverage and every risk will be viewed differently by every carrier. In our experience, carriers are still competing to write coverage for the best risks. By this we mean those risks which can not only demonstrate an effective system of loss prevention, but also Risk Management policies which are followed and enforced by the insured. These accounts should also possess first rate security systems and up-to-date anti-virus protections.

Like every organization, the U.S. Healthcare system is struggling to adapt in the modern world. Technological advancements offer opportunities for companies to lower costs and improve quality & efficiency. However, these advancements also increase privacy risks. The implementation of legislation has forced the consolidation of digital records and provides targets for hackers. As evident by recent breaches, network attacks on healthcare systems are becoming more frequent and are affecting a record number of individuals. While their focus is on healthcare and not security, the healthcare industry needs to be aware of the rising threat of cybercrime.

About the author

Alex Wozniak is an Executive Risk Consultant with CBIZ Insurance Services, Inc. He focuses on the development and implementation of cyber liability, directors & officers, and employment practices liability insurance programs for clients in all industry sectors. He is a graduate of Loyola University Maryland. Alex can be reached at awozniak@cbiz.com.

Bibliography

"Fact Sheet 8d: Protecting Health Information: the HIPAA Security and Breach Notification Rules." *Protecting Health Information: the HIPAA Security and Breach Notification Rules.* N.p., n.d. Web. 25 Sept. 2014. <https://www.privacyrights.org/content/protecting-health-information-hipaa-security-and-breach-notification-rules>.

Meyers, Jessica. "Health care industry ill-prepared for vicious cyberthreats - The Boston Globe." *BostonGlobe.com.* N.p., 6 Sept. 2014. Web. 24 Sept. 2014. <http://www.bostonglobe.com/news/nation/2014/09/05/health-care-industry-ill-prepared-for-vicious-cyberthreats/ZdvDGaipJi7VSN0TogezkL/story.

Millman, Jason. "Health care data breaches have hit 30M patients and counting." *Washington Post.* The Washington Post, 19 Aug. 2014. Web. 24 Sept. 2014. <http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/>.

Peterson, Andrea, and Jason Millman. "HealthCare.gov server hacked. But HHS says no consumer information taken.." *Washington Post.* The Washington Post, 4 Sept. 2014. Web. 25 Sept. 2014. <http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/04/healthcare-gov-server-hacked-but-hhs-says-no-consumer-information-taken/>.

Ponemon Institute. *Fourth Annual Benchmark Study on Patient Privacy and Data Security.* N.p., n.d. Web. 25 Sept. 2014. <http://www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security>.

Sullivan, Gail. "Chinese hackers may have stolen your medical records." *The Washington Post.* N.p., 19 Sept. 2014. Web. 24 Sept. 2014. <http://www.washingtonpost.com/news/morning-mix/wp/2014/08/19/chinese-hackers-may-have-stolen-your-medical-records/?utm_campaign=KHN:+First+Edition&utm_source=hs_email&utm_medium=email&utm_content=13838254&_hsenc=p2ANqtz-_sF0EtBvNdGGylzphXEjs8rxztJ_jTiMV3oXoz6CjpOJgg1FL81Jio2sA1eliH_et3aKQeiPcR1-fBaDf6XQe951o0RMTY14dV-qWWc0RdBJLBOU4&_hsmi=13838254>.

continued on page 14

continued from page 13

Footnotes

[1]Meyers, Jessica. "Health care industry ill-prepared for vicious cyberthreats - The Boston Globe." *BostonGlobe.com.* N.p., 6 Sept. 2014. Web. 24 Sept. 2014. <http://www.bostonglobe.com/news/nation/2014/09/05/health-care-industry-ill-prepared-for-vicious-cyberthreats/ZdvDGaipJi7VSN0TogezkL/story.

[2]Millman, Jason. "Health care data breaches have hit 30M patients and counting." *Washington Post.* The Washington Post, 19 Aug. 2014. Web. 24 Sept. 2014. <http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/>.

[3]Ponemon Institute. *Fourth Annual Benchmark Study on Patient Privacy and Data Security.* N.p., n.d. Web. 25 Sept. 2014. <http://www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security>.

[4]Millman, "Health care data breaches have hit 30M patients and counting."

[5]Sullivan, Gail. "Chinese hackers may have stolen your medical records." *The Washington Post.* N.p., 19 Sept. 2014. Web. 24 Sept. 2014. <http://www.washingtonpost.com/news/morning-mix/wp/2014/08/19/chinese-hackers-may-have-stolen-your-medical-records.

[6]Peterson, Andrea, and Jason Millman. "HealthCare.gov server hacked. But HHS says no consumer information taken.." *Washington Post.* The Washington Post, 4 Sept. 2014. Web. 25 Sept. 2014. <http://www.washingtonpost.com/blogs/the switch/wp/2014/09/04/healthcare-gov-server-hacked-but hhs-says-no-consumer-information-taken/>.

[7]Ponemon Institute, p.3.

[8]"Fact Sheet 8d: Protecting Health Information: the HIPAA Security and Breach Notification Rules." *Protecting Health Information: the HIPAA Security and Breach Notification Rules.* N.p., n.d. Web. 25 Sept. 2014. <https://www.privacyrights.org/content/protecting-health-information-hipaa-security-and-breach-notification-rules>.

[9]Ponemon Institute, p. 3-4

[10]Ponemon Institute, p. 13

•Certification Corner•

I hope everyone had a great Thanksgiving holiday. Since the last issue, I have some great news to report. The certification study group that we participated in with the New York chapters was a huge success. We had 17 people from New Jersey participate. The sessions ran every Monday night for two hours via GoToMeeting. Instructors from the NY chapters led the sessions and participants were able to ask questions during the presentations. If someone was not able to attend, the sessions were recorded so that they could be accessed later. Participants' evaluations indicated that most thought the sessions were extremely valuable.

Since the ending of the session, Alan King from Princeton Medical Center from our Chapter, took and passed the exam! Congratulation, Alan!

We are looking into other programs to add to the Certification calendar in the upcoming months. There may be a joint chapter study group for the Revenue Cycle certification. I will keep you posted.

We are looking forward to more members of the Chapter sitting for the exam. As your Certification Chair, I am available to assist members in any way I am able. Please don't hesitate to contact me if you have any questions.

Enjoy your holiday season!

Rita Romeu, Certification Chair
Romeur@comcast.net