anthelio®
A higher aim. A newer standard.

White Paper

Data Security

Safeguarding The Privacy and Security Of Healthcare Data In Today's Challenging Environment

Protecting the privacy and security of healthcare data in today's increasingly complex healthcare environment can be extremely challenging. Large health systems and their associates, small physician offices and health insurance providers all struggle with this monumental task. A recent survey estimated that as much as 93% of data held by healthcare organizations requires protection, including medical records, claims histories and patient protected health information (PHI). Unfortunately, this same survey found that only 57% of this information was "somewhat protected," and 43% was inadequately safeguarded.[1]

Healthcare data security lags behind other industries

Over the past several decades, healthcare organizations have allocated a much smaller portion of their IT budget to data security than other industries.[2] Attaining compliance with the Health Insurance Portability and Accountability Act (HIPAA) compliance was the main priority, rather than risk management. (HIPAA, which stands for The Health Insurance Portability and Accountability Act, defines federal protections for personal and individual's health information entrusted to providers). Consequently, the healthcare industry has fallen behind other industries in data security capabilities beyond those needed to meet HIPAA requirements.

93% of data held by healthcare organizations requires protection

With the healthcare industry in a constant state of change and the threat landscape rapidly escalating, healthcare providers must progress beyond compliance requirements, employing advanced security technologies and sophisticated risk management practices to provide the level of privacy and security necessitated by today's environment. This issue becomes even more critical as healthcare organizations strive to meet government mandates to share patient data to enable coordinated care across the care continuum.

What is privacy and security?

According to the agreed upon terminology within the healthcare industry, privacy and security refers to the confidentiality of a healthcare systems' data with special concern for patients' records.[3] The U.S. Department of Health and Human Services developed guidelines for the protection of patients' medical records in the HIPAA regulations, which Congress passed and President Clinton signed into law in 1996. The Health Information Technology for Economic and Clinical Health Act (HITECH), which became law in 2009, further extended HIPAA to business associates and vendors of healthcare providers and required disclosure of HIPAA violations. Severe monetary penalties can be enforced for HIPAA violations, and fines have reached over $4 million for some organizations.[4]

How common are data breaches?

Healthcare security breaches are in the news more and more today, and these damaging events are becoming a growing trend that all providers and insurers must aggressively combat. In 2015, Anthem, the second largest health insurer in the US, acknowledged its database of sensitive customer information was stolen and sold posted online. Data included names, birth dates, medical IDs, Social Security numbers, mailing addresses, and employment information of 80 million customers,

© 2016 Anthelio Healthcare Solutions Inc. Proprietary and confidential information of Anthelio Healthcare Solutions Inc. All Rights Reserved.

including Anthem's own CEO.[5] A similar breach occurred at Washington state-based Premera Blue Cross, a not-for-profit plan whose corporate clients include such notable names as Microsoft and Starbucks. The company was targeted with a "sophisticated cyberattack" in January 2015 when hackers gained access to the financial and medical information of 11 million members, the second largest breach to hit healthcare after Anthem.[6]

A December 2015 article in Healthcare IT News recapped many of the year's security failures in an article titled, "2015 healthcare security breaches: a long list."[7] Here are just a few of the events they highlighted:

- Hackers swipe data of 4.5M at UCLA Health System in massive cyberattack
- Keystroke logger detected on hospital's computers
- Oncology group slapped with $750K HIPAA fine
- Coding update makes for HIPAA breach blunder
- HIPAA breach for hospital after worker swiped patient data
- Hackers hit business associate, swipe PHI and Social Security numbers
- Hospital with repeat security failures hit with $218K HIPAA fine
- State agency HIPAA security gaffe puts patient data on the Internet
- Cyber attackers swipe data of 1.1M at CareFirst
- Health system sees 7th HIPAA data breach
- Healthcare insider snoop indicted for fraud scheme
- No encryption means HIPAA breach for 45K

As this partial list demonstrates, threats can come from all directions: outsiders, snooping employees and those with criminal intent—even well intentioned employees trying to do their jobs. How common are these events? Statistics show they are widespread throughout the industry. A recent benchmark study on privacy and security of healthcare data by the Ponemon Institute found that more than 90% of healthcare organizations in the study had a data breach during the preceding 24 months, and 40% reported more than five incidents during that time period.[8]

Healthcare faces 340% more security incidents and attacks than the average industry

What does the future hold? Unfortunately, from all indications, the situation will only worsen. The RaytheonWebsense Security Labs report on 2016 security predictions concluded that "with healthcare facing 340% more security incidents and attacks than the average industry, and no end in sight for the need and number of connected medical devices, reconciling patient needs with network security will become increasingly important."[9]

Healthcare security breaches are costly

Healthcare data breaches not only destroy trust and tarnish the provider's or insurer's image, they are also the most expensive to rectify compared to other industries, according to a new global analysis on the cost of data breaches.[10] In the U.S. healthcare industry, the average cost per exposed personally identifiable record was $398 in 2015, compared to an average of $217 for breaches across all U.S. industries, the study reported. The average cost a healthcare organization incurs managing and rectifying a data breach is estimated to be more than $2.1 million per event.[11] These costs cover such expenses as notifying people whose information has been compromised, investigating and collecting evidence,

© 2016 Anthelio Healthcare Solutions Inc. Proprietary and confidential information of Anthelio Healthcare Solutions Inc. All Rights Reserved.

public relations, regulatory fines, legal fees, crisis management services, and legal settlements.[12] For the industry as a whole, information security breaches cost up to $5.6 billion annually.[13] The estimated total cost for HIPAA breaches from 2009 through 2015 has reached over $31 billion. More than 153 million people were affected by the 1,286 breaches that occurred during that time period.[14]

Information security breaches cost up to $5.6 billion annually

Causes of data breaches

Criminal attacks on healthcare organizations are now the leading cause of data breaches and have increased 125%

There are many causes for the data breaches and security incidents that have become widespread throughout the industry, but chief among them is criminal attacks. Criminal attacks on healthcare organizations are now the leading cause of data breaches and have increased 125% since 2010.[15] Many security experts are voicing their opinions that healthcare is in the crosshairs of cybercriminals,[16] and their concerns are well founded. According to the Ponemon study, 45% of healthcare organizations report the root cause of their data breach was a criminal attack, with 12% indicating it was due to a malicious insider.[17]

The dramatic increase in criminal activity is driven by the cyber criminal's realization that a medical record has a longer shelf life and higher value than other types of stolen information. For instance, credit card data expires quickly because financial institutions replace the cards once they become aware the information has been stolen. Black market prices for medical records can run as much as 10 times those of personal information from breaches in other industries because the depth of information gathered from them can be used for identity theft and medical identity theft.[18]

A Private Industry Notification for the healthcare industry issued by the FBI's Cyber Division sheds further light on this topic: "Cyber criminals are selling the information [EHR data] on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen Social Security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft."[19]

Criminals also have many other creative ways to utilize compromised EHR data. There have been cases where healthcare organizations and their business associates have had their data held hostage for ransom. Criminals unleash advanced "ransomware" that infects computers and encrypts files, and then demand payment to release them.[20]

Another escalating threat to the privacy and security of patient data is workarounds. A workaround is a way of accomplishing a task when the usual or planned method isn't working well.[21] Today it is common for healthcare workers to bring their own smartphones, laptops and tablets to work so they can use them to perform workarounds when they encounter difficulties with the normal process. Workarounds allow healthcare staff to access, share and store patient information outside of the hospital's IT network, bypassing the organization's security protections and greatly increasing the risk that patient data may be compromised.[22]

With the proliferation of powerful mobile devices and apps, workarounds represent a growing threat to the organization's IT assets and the privacy and security of patient information. Using mobile devices and apps in the healthcare environment creates a wider attack landscape, exposes a broader expanse of data and creates a larger range of vulnerabilities for cybercriminals to exploit.[23] A recent survey of frontline healthcare workers found that an alarming 21.5% reported that workarounds happen every day that may not be in compliance with hospital privacy and security policies. Respondents indicated they resorted to workarounds because their IT policies inhibited them from efficiently doing their jobs,[24] highlighting the need to balance security with operational efficiency and the need for fast access to data to provide timely patient care.

© 2016 Anthelio Healthcare Solutions Inc. Proprietary and confidential information of Anthelio Healthcare Solutions Inc. All Rights Reserved.

In addition to criminal attacks and workarounds, other common causes of data breaches include:

Stolen or lost laptops
Employee negligence resulting in lost or stolen devices is a major cause of security incidents in healthcare organizations. Ninety-six percent of respondents in the Ponemon survey had a security incident involving lost or stolen devices during the 24-months prior to the survey.[25] Unfortunately, more than 41% of healthcare organizations report they have not deployed endpoint encryption, which could reduce the risks associated with device loss.[26]
A mobile workforce
A Forrester Research study found that roughly a third of healthcare employees work outside of the office or clinic at least once a week, and many use unsecured devices that put data at risk.[27]
Employee mistakes or unintentional actions
Employees responding to contaminated emails or failing to protect passwords can also enable data breaches.
Third-party errors
Business associates may not follow guidelines for secure data handling, or policies may not exist.

Many organizations are unprepared for the escalating threat landscape

In spite of the growing risk for data breaches that healthcare providers and insurers face on a daily basis, many do not have the administrative, technical and organizational skills required to detect, mitigate and prevent cyberattacks. The Ponemon study found an alarming number of respondents lacking the necessary security policies, procedures, expertise, and technologies required by today's challenging healthcare environment:[28]

- ✓ Only 33% have the resources to prevent or promptly detect unauthorized patient data access, loss or theft;
- ✓ Only 58% have guidelines and procedures to prevent or quickly discover unauthorized attempts to gain access to patient data;
- ✓ Only 53% believe their staff has the technical skills to identify and solve data breaches, and
- ✓ Only 49% have technologies in place to effectively impede or discover unauthorized attempts to gain access to patient data.

Another survey found similar results. Just 53% of executives at healthcare organizations and 66% of health insurers reported they are prepared to defend against attacks.[29]

Information from a recent HIPAA Security Conference revealed that some healthcare organizations still have not implemented even the most basic preventative security measures, such as intrusion detection systems, infrastructure security assessments, remote data wiping of mobile devices, or encryption. Information was also presented at the conference indicating that approximately 60% of healthcare data breaches since 2009 could have been prevented through encryption.[30]

Some healthcare organizations still have not implemented even the most basic preventative security measures

Although the Ponemon survey found that some progress has been made over the past five years, there is strong evidence throughout the industry demonstrating that many healthcare organizations and insurers simply are not adequately prepared to protect the assets they are entrusted to manage.

© 2016 Anthelio Healthcare Solutions Inc. Proprietary and confidential information of Anthelio Healthcare Solutions Inc. All Rights Reserved.

White Paper

anthelio®
A higher aim. A newer standard.

Safeguarding patient data and network assets with a comprehensive security program

Healthcare information technology grows incredibly more complex every day, due to massive changes in the industry driven by mergers and acquisitions, new technologies and government mandates. The complicated network of connected devices, systems and entities throughout the healthcare enterprise creates vulnerabilities that make a robust security program a necessity. Healthcare organizations and insurers must aggressively work to achieve a strong security posture by implementing controls to protect sensitive information, network assets, and computer systems. It is imperative that organizations have a clear understanding of their systems' vulnerabilities and that they are protected against both internal and external attacks.

While some healthcare organizations and insurers are well on their way to building effective security programs with their own staff and IT resources, many simply do not have the personnel, expertise and technologies necessary to successfully do the job themselves. For those organizations, outside specialists offer cost-effective and efficient solutions.

Whether the organization tackles this critical task on their own or calls upon outside experts, certain activities should be undertaken to ensure a strong foundation for the security program. A comprehensive security risk assessment should be completed that closely examines the organization's current overall information security profile. This includes key activities such as:

- ✓ Identifying any impediments to the information security program;
- ✓ Detecting gaps in existing security policies and procedures;
- ✓ Documenting vulnerabilities in core systems and networks;
- ✓ Reviewing security architecture;
- ✓ Evaluating compliance management;
- ✓ Conducting vulnerability scans and penetration tests, and
- ✓ Examining business applications security.

This in-depth assessment usually involves multiple information gathering techniques, such as questionnaires, on-site interviews, documentation reviews and automated scanning tools. The information gathered from the assessment process then drives the creation of a comprehensive risk management plan that provides a detailed roadmap to effectively address and correct the identified risks.

Conclusion

Data breaches in healthcare continue to put patient data and organizational assets at risk, potentially costing millions of dollars in fines and crisis management, in addition to damaging the organization's image and consumer trust. More importantly, data breaches negatively impact the organization's ability to provide accurate and timely information that is critical to delivering quality patient care across the care continuum.

In today's growing threat landscape, no healthcare organization or insurer, regardless of size, is immune from a data breach. Data privacy and security can no longer be a low priority, as they have become mission critical in today's era of cybercrime. Organizations must be proactive by implementing a comprehensive security and privacy program that empowers the organization to provide quality care while protecting the sensitive information and assets they are entrusted to safeguard.

© 2016 Anthelio Healthcare Solutions Inc. Proprietary and confidential information of Anthelio Healthcare Solutions Inc. All Rights Reserved.

References:

1. EMC2. “The Digital Universe: Driving Data Growth in Healthcare.” 2014. http://www.emc.com/analyst-report/digital-universe-healthcare-vertical-report-ar.pdf
2. Forrester Research, “Industry Spotlight: US Healthcare Security Budgets, Priorities, And Challenges.” February 19, 2014. https://www.forrester.com/Industry+Spotlight+US+Healthcare+Security+Budgets+Priorities+And+Challenges/fulltext/-/E-res109443
3. Healthcare IT News. “Privacy & Security defined.” December 2015. http://www.healthcareitnews.com/directory/privacy-security
4. Ibid.
5. MSN.Com. “2015’s big hacks, attacks and security blunders.” http://www.msn.com/en-us/news/technology/2015s-big-hacks-attacks-and-security-blunders/ar-BBnG38A?li=BBnbcA1&ocid=iehp
6. Healthcare IT News. “Premera Blue Cross hack exposes 11M.” March 18, 2015. http://www.healthcareitnews.com/news/premera-blue-cross-hack-exposes-data-11m
7. Healthcare IT News. “2015 healthcare security breaches: a long list.” December 10, 2015. http://www.healthcareitnews.com/slideshow/2015-healthcare-security-breaches-long-list?page=0
8. Ponemon Institute LLC. “Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data.” May 2015. http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf
9. RaytheonWebsense Security Labs. “2016 Security Predictions.” December 2, 2015. http://www.websense.com/assets/reports/report-2016-cybersecurity-predictions-en.pdf
10. Modern Healthcare. “Healthcare data breaches are costliest: study.” May 28, 2015 http://www.modernhealthcare.com/article/20150528/NEWS/150529899
11. Ponemon Institute LLC. “Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data.” May 2015. http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf
12. HIT Technology. “Healthcare Security Breaches Cost $31B and Growing.” September 15, 2015. http://hitconsultant.net/2015/09/15/healthcare-security-breaches-cost-31b/
13. CNBC. “Health Care Information Security Breaches Cost The Industry Up To $5.6 Billion Annually.” March 12, 2014. http://www.cnbc.com/2014/03/12/health-care-systems-56-billion-security-problem.html
14. HIT Technology. “Healthcare Security Breaches Cost $31B and Growing.” September 15, 2015. http://hitconsultant.net/2015/09/15/healthcare-security-breaches-cost-31b/
15. Ponemon Institute LLC. “Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data.” May 2015. http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf
16. Healthcare IT News. “Premera Blue Cross hack exposes 11M.” March 18, 2015. http://www.healthcareitnews.com/news/premera-blue-cross-hack-exposes-data-11m
17. Ponemon Institute LLC. “Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data.” May 2015. http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf
18. Modern Healthcare. “Healthcare data breaches are costliest: study.” May 28, 2015 http://www.modernhealthcare.com/article/20150528/NEWS/150529899
19. FBI Cyber Division Private Industry Notification. “Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain.” PIN #: 140408-009. April 8, 2014. http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf
20. HIPAA, HITECH & HIT. “Hacked Health Records Prized for their Black Market Value.” March 16, 2015. http://hipaahealthlaw.foxrothschild.com/2015/03/articles/privacy/hacked-health-records-prized-for-their-black-market-value/
21. Whatis.com . “Workaround definition.” May 29, 2003. http://whatis.techtarget.com/definition/0,,sid9_gci868091,00.html
22. HIMSS Media. “Workarounds in Healthcare, a Risky Trend.” 2013. http://www.intel.com/content/www/us/en/healthcare-it/workarounds-in-healthcare-risky-trend.html
23. RaytheonWebsense Security Labs. “2016 Security Predictions.” December 2, 2015. http://www.websense.com/assets/reports/report-2016-cybersecurity-predictions-en.pdf
24. HIMSS Media. “Workarounds in Healthcare, a Risky Trend.” 2013. http://www.intel.com/content/www/us/en/healthcare-it/workarounds-in-healthcare-risky-trend.html
25. Ponemon Institute LLC. “Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data.” May 2015. http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf

© 2016 Anthelio Healthcare Solutions Inc. Proprietary and confidential information of Anthelio Healthcare Solutions Inc. All Rights Reserved.

26. Forrester.com blog. “It’s Time For Healthcare CISOs To Close The Faucet Of Data Loss.” September 4, 2014. http://blogs.forrester.com/christopher_sherman/14-09-04-its_time_for_healthcare_cisos_to_close_the_faucet_of_data_loss_1
27. Ibid.
28. Ponemon Institute LLC. “Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data.” May 2015. http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf
29. KPMG, LLP. 2015 Healthcare Cybersecurity survey. “Healthcare And Cyber Security: Increasing Threats Require Increased Capabilities.” August 27, 2015.http://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf
30. InTelligence. “Healthcare Security Incidents Need Not Lead to Data Breaches.” November 10, 2014. http://blogs.absolute.com/blog/healthcare-security-incidents-need-lead-data-breaches/#.VohuoPkrKM8

Anthelio Healthcare Solutions

Anthelio is the largest independent provider of healthcare technology solutions in the market. We offer solutions across the spectrum of care, providing customers the ability to solve their critical technology needs from a single source while delivering cost savings and efficiencies. Our end-to-end solutions include IT infrastructure services, IT applications management, EHR optimization, Patient Engagement, Analytics, and Revenue Cycle Management (RCM) including HIM Services, Patient Financial Services and Cancer Registry Services. Anthelio drives sustainable value to over 63,000 physicians and nurses in hundreds of healthcare organizations supporting their annual revenue of over $67 billion and impacting quality care to over 60 million patients.

Anthelio Healthcare Solutions Inc.
One Lincoln Centre, Suite 200,
5400 LBJ Freeway,
Dallas, TX - 75240

Phone: 214-257-7000
Toll-Free: 855-268-4354
info@antheliohealth.com

https://www.facebook.com/Anthelio
https://www.linkedin.com/company/anthelio-healthcare-solutions
www.twitter.com/Anthelio/