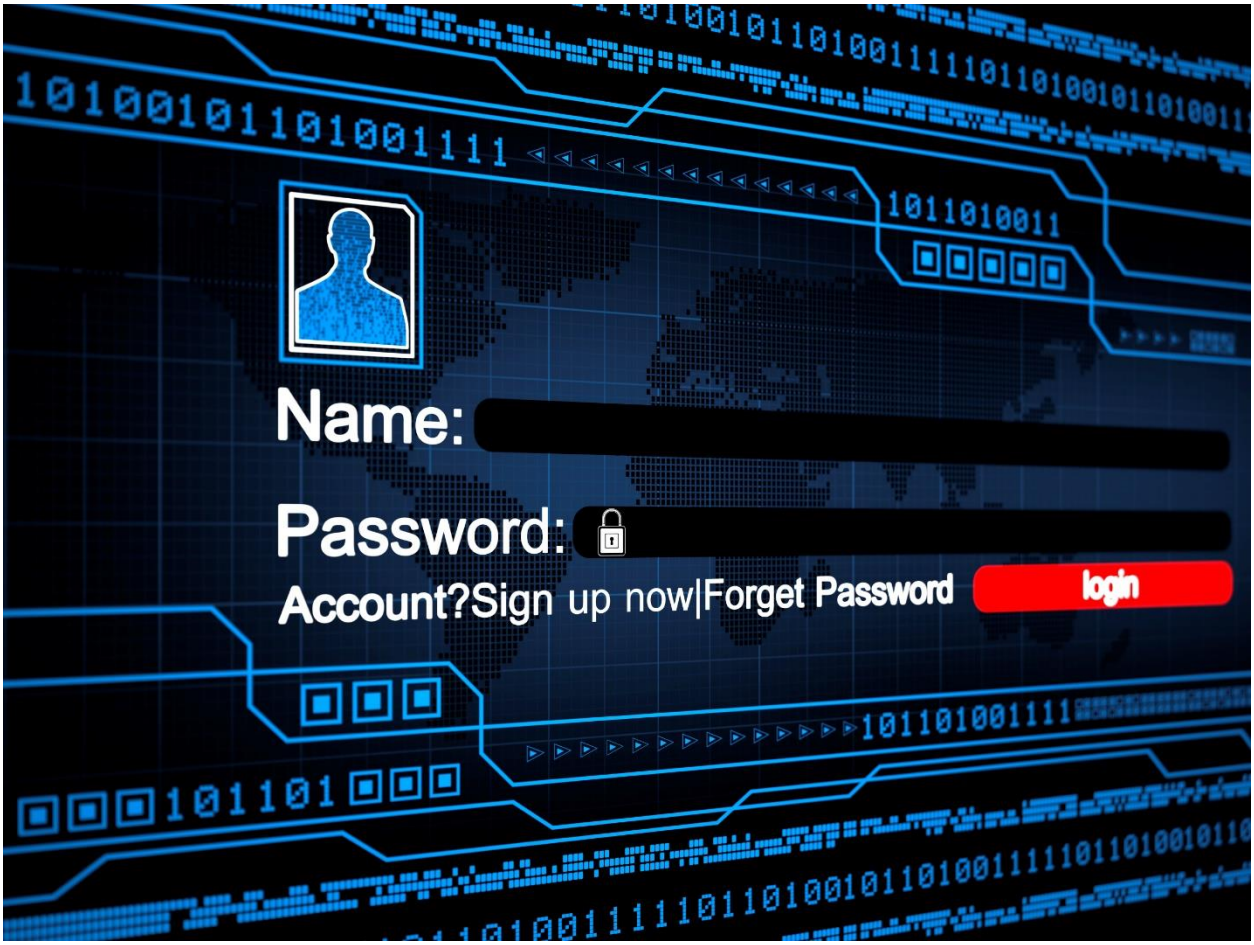


Redspin
An Auxilio Company

BREACH REPORT 2015:

Protected Health Information (PHI)

February 2016

Executive Summary

The HITECH Act mandates that large breaches of protected health information (PHI) totaling 500 records or more must be reported on a timely basis to the Office of Civil Rights (OCR) under the Department of Health and Human Services (HHS). This breach notification requirement was implemented in two interim rules and then finalized in the HIPAA Omnibus Rule. As of December 31, 2015, a total of 1,437 large breaches of PHI affecting 154,368,781 patients had been reported since HITECH went into effect in 2009.

This is Redspin's 6th annual *Breach Report: Protected Health Information (PHI).* At the conclusion of each year, we analyze the complete statistical data set of large breaches that have been reported to HHS. In the report, we assess the overall effectiveness of the current policies and controls designed to safeguard PHI. In the current year, we identify significant trends and draw attention to the specific areas most in need of improvement. We then offer Redspin's recommendations for preventive measures and corrective actions to address any critical gaps or weaknesses. Our goal is to help the healthcare industry continually improve its ability to protect patient information. As always, we hope this year's report makes an important contribution.

By the Numbers

1,437 large breaches of protected health information since 2009

154,368,781 patient health records breached since 2009

258 large breaches of protected heath information in 2015

113,208,516 patient health records breached in 2015

98.1% of records breached in 2015 were the result of hacking attacks/IT incidents

78,000,000 records breached in the single largest incident in 2015 and the largest healthcare breach in history

897% increase in records breached in 2015 vs. 2014

88.2% of all records breached in 2015 came as a result of the top 3 incidents

20.2% of all breach incidents since 2009 involved a business associate

26.3% of large breach incidents in 2015 involved paper or films

From the Beginning

The migration from paper files to electronic health records (EHR) began in earnest after the passage of the 2009 HITECH Act. Spurred by the Meaningful Use EHR Incentive Program, electronic health records are now in use at a vast majority of hospitals and other providers. However, the pace of EHR adoption has consistently outstripped the ability of health organizations to adequately safeguard protected health information from significant breaches.

PHI is a uniquely challenging data set to protect. On the one hand, it is extremely rich in deep demographics and other highly sensitive information that should not fall into the wrong hands. Unlike credit card numbers, once PHI is "out in the wild" it is not cancellable or recoverable. At the same time, PHI needs to be available virtually on demand and is readily shared among providers, patients, payers, and business associates.

Saying that the healthcare industry has yet to meet this challenge is more than an understatement. Over 150 million patient health records (154,368,781 to be exact) have been breached since 2009. Accounting for some duplication, this means that at least 1 of every 3 Americans have had their personal health information breached as the result of security flaws or human error.

The Year of the Hack

2015 was a watershed (or perhaps a "washout") year in healthcare IT security. In previous reports we warned that *"the threat from malicious outsiders – hackers – has the potential to wreak havoc on the healthcare industry."* In 2015, havoc was wrought. An astounding 113,208,526 patient records were breached, more than twice as many as in the 5 prior years combined. Even more ominously, 9 of the top 10 incidents and 98.1% of records breached in 2015 were the result of hacking attacks/IT incidents.

From 2009-2013, the primary cause of PHI breach was the loss or theft of unencrypted portable computing devices. In most cases of theft, there was little concern about information compromise as it was more likely the thief valued the device more than what was stored on it. Not so in 2015. Hackers knew exactly what they were after as they

pilfered health information and/or other personal data for nefarious purposes such as medical ID theft and fraud.

2015 was barely two months old when health insurer Anthem warned consumers that cyber-attackers had "executed a sophisticated attack to gain unauthorized access to Anthem's IT system and obtained personal information." Some 78 million records were involved, making it the largest breach in healthcare history. In fact, in 2015 we witnessed the three largest PHI breaches in healthcare history.

Table 1: The 3 Largest PHI Breaches in Healthcare History

Covered Entity	Year	# of Records Breached	Cause of Breach
Anthem	2015	78,000,000	Hacking/IT Incident
Premera Blue Cross	2015	11,000,000	Hacking/IT Incident
Excellus Health Plan	2015	10,000,000	Hacking/IT Incident

Note that all three attacks were launched on health insurers. Prior to 2015, insurers reported less than 10% of all large PHI breach incidents and an even smaller percentage of records breached. Comparatively, in 2015, PHI breaches disclosed by insurers accounted for 23.6% of incidents and an overwhelming 90.9% of records.

Table 2: 2015 PHI Breaches by Type of Entity

Type of Entity	# of Records Breached	% of Total
Business Associates	3,950,312	3.5%
Health Plans	102,911,697	90.9%
Healthcare Provider	6,346,507	5.6%
Total	113,208,516	100%

Why the dramatic change? Large health insurers process and maintain enormous amounts of PHI, much more than a typical hospital. Given the potential ROI of successfully hacking into a major health plan's data, it was only a matter of time before payers were targeted.

Phish Where the Fish Are

Indications are that hackers gained access to Anthem's data by stealing the network credentials of at least 5 high level IT employees. What Anthem claimed as a "sophisticated attack" may well have begun with phishing, a tactic that involves using false pretenses such as a fraudulent email, phone call, or website to trick employees into disclosing their login ID and password, or downloading malicious code ("malware") that provides the hackers with long term network access.

It appears that hackers had Anthem, Premera and Excellus in their crosshairs for some time and likely that the attacks went undetected for months if not years. In the Anthem case, a bogus website may have been used in the heist. Security researchers traced the web address "we11point.com" to a Chinese hacking group (Anthem was previously known as Wellpoint) and found that the address had been in use since early 2014.

The Premera attack bore similarities to Anthem – the discovery of the web address "prennera.com" suggested that the same modus operandi had been used, possibly by the same threat actors.[1] Premera said they believed the initial attack had occurred in May 2014. When Excellus Blue Cross Blue Shield disclosed that its network had been penetrated, it revealed that malicious actors had access to their data for the prior 1 and ½ years.

Because phishing attacks exploit human vulnerabilities rather than technical, healthcare organizations must step up their security awareness education efforts for all employees. They need to be better trained to recognize phishing schemes through social engineering testing and security awareness training. Policies may also need to be tightened. As John Halamka, CIO at Beth Israel Deaconess HealthCare says "as hard as this is, it's increasingly important that we restrict the behavior of individuals more than we ever have before." [2]

[1] http://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/
[2] *"CIO Halamka on Security Action Items for 2016,"* www.healthcareinfosecurity.com December 15, 2015

How Providers Fared

In 2015, 185 providers reported PHI breaches impacting over 6 million records. While insurers bore the brunt of hacking attacks, healthcare providers were victimized as well. Of the PHI breaches among providers, hackers factored in 3 of the 5 largest incidents and 83% of the records reported breached.

Table 3: 5 Largest Data Breaches at Healthcare Providers in 2015

Providers	Records Reported	Type of Breach	Location of Breached Information
UCLA Health	4,500,000	Hacking/IT Incident	Network Server
Beacon Health System	306,789	Hacking/IT Incident	Email
Empi Inc and DJO	160,000	Theft	Laptop
Advantage Consolidated LLC	151,626	Hacking/IT Incident	Other
Jacobi Medical Center	90,060	Unauthorized Access/Disclosure	Email

On March 18th, 2015, Advantage Dental disclosed that an intruder had successfully used malware installed on an infected system to obtain illegal access to one of its patient databases. The database contained personal health information on over 150,000 patients.

On May 22, 2015, Beacon Health Systems (BHS) of Indiana issued a press release detailing a phishing attack that led to a breach of their email system. The email system included personal information as well as some health data on over 300,000 patients. It is believed that the attack took place over a period of 14 months.

On July 17, 2015, UCLA Health announced it had been the victim of a criminal cyber-attack and estimated that "as many as 4,500,000 individuals potentially may have been involved in the attack." [3] UCLA began working with the FBI and private forensics experts as soon as suspicious activity was detected in October 2014.

[3] https://www.uclahealth.org/news/ucla-health-victim-of-a-criminal-cyber-attack

Beware BA's

Healthcare business associates have always been required to maintain the privacy and security of any PHI they possess in relation to the work they do for covered entities. However, the stakes got higher for BA's after the 2013 HIPAA Omnibus Rule went into effect. Today BA's must fully comply with HIPAA and can now be held directly liable for breaches of protected health information.

Prudent covered entities still maintain stewardship over the PHI they entrust to their BA's. They risk reputational harm as a result of a BA breach or even joint liability if they are found to have been negligent in their oversight. Given that over 20% of all PHI breach incidents to date have involved a BA, it would be wise for all covered entities to conduct a vendor risk analysis and keep it up-to-date.

The Omnibus Rule extended the reach of HIPAA considerably. For example, many technology companies provide software-as-a-service (SaaS) applications to healthcare providers. If these applications transmit, process, or store PHI from the provider, then the software company must comply with HIPAA regulations, including the requirement to conduct regular HIPAA Security Risk Assessments (HSRA). For these companies, the HSRA should include a thorough security assessment of the SaaS application itself.

We predict BA's will be increasingly targeted by hackers. Many BA's store as much PHI or more than a large hospital. For example, Medical Informatics Engineering, an Indiana medical software company, disclosed last summer that the private information of 3.9 million people nationwide was exposed when its networks were hacked earlier in the year. The attack occurred on its main network and its *NoMoreClipboard* network. The company said the exposed information included names, addresses, birthdates, Social Security numbers and health records. This breach was the 5th largest of 2015.

Congress Gets in the Act

In 2015, PHI breaches in healthcare not only grabbed headlines but also caught the attention of lawmakers. In February of last year, the Senate Health Committee launched an initiative to examine the security of health information. Redspin's 2014 Breach Report was one of the industry reports reviewed by Congressional staffers.

The committee invited participation from many health organizations—including health insurers, doctors, hospitals and other businesses. Across the board, participants expressed the need for clearer guidance from the Department of Health and Human Services on ways to safeguard against cyber threats. Most lacked clarity as to who at HHS had leadership responsibility for cybersecurity matters.[4]

Based on this input, 9 pages of healthcare-related cybersecurity measures were included in the Cybersecurity Act of 2015. Signed into law on December 18, 2015, the bill calls on HHS to report to multiple congressional committees on the healthcare industry's preparedness on cybersecurity threat responses. HHS is also required to select a leader to head cybersecurity initiatives and detail methods for addressing threats across its health divisions.

Healthcare is a critical U.S. industry. The Federal government is justifiably concerned about the industry's track record in safeguarding patient information. Making cybersecurity in healthcare a higher priority at HHS in 2016 is a step in the right direction. More importantly, IT security needs to be made a higher priority in the industry itself. That means commitment from the top, from CEO's and Boards of Directors alike. It should not take a massive breach to get their attention. 1 out of every 3 Americans can tell you that.

Show Me the Money

Budget dollars for IT security at healthcare providers have traditionally been hard to come by, despite the evidence that breaches can be very costly. Proposed increases in security budgets face scrutiny on an "ROI" basis, a metric that CEO's understand. When the risk

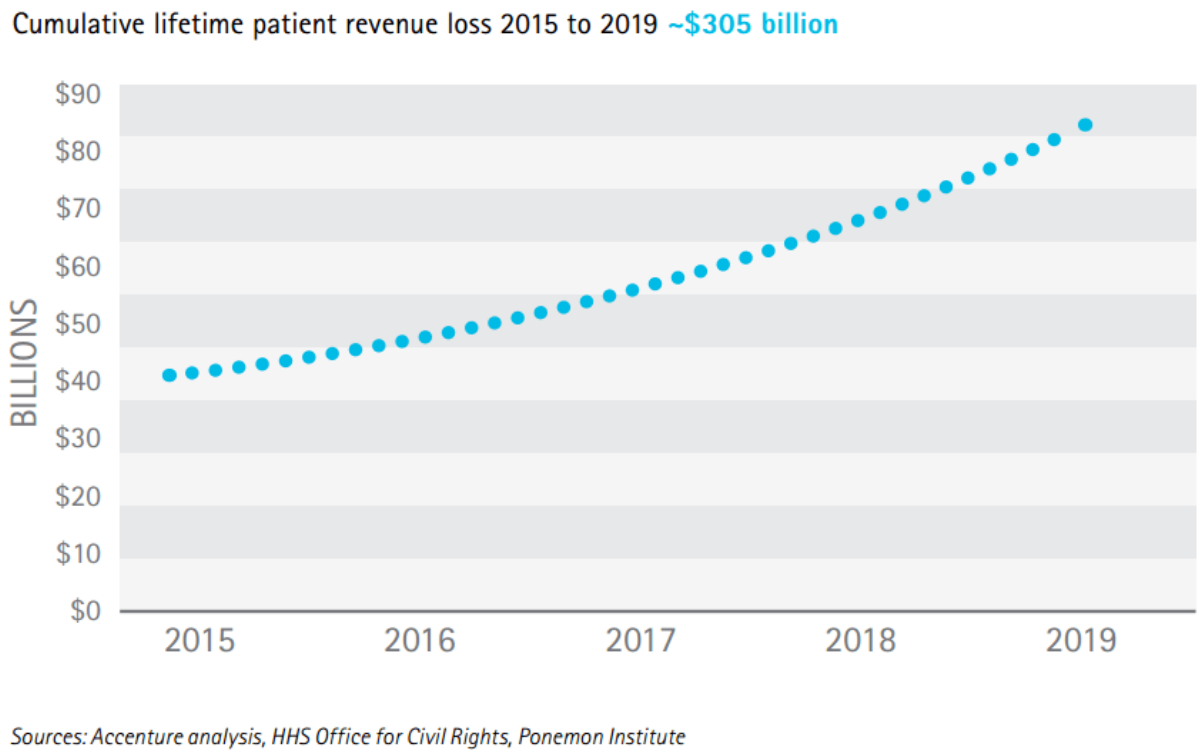
[4] http://hitconsultant.net/2015/10/29/senate-cybersecurity-bill-5-key-facts-healthcare-organizations/

is presented as only the hard costs of a potential breach, some executives have chosen to accept that risk rather than invest significant additional dollars in security.

But after 2015, there is a now a growing argument that such a cost-benefit analysis should consider potential reputational damages and revenue loss as well as the immediate hard costs of PHI breach. A hacking attack has a greater likelihood of creating harm to patients than a lost or stolen portable electronic device.

According to a recent report from Accenture, data breaches over the next 5 years will cost U.S. health systems $305 billion in cumulative lifetime revenue. Accenture argues that as many as 1 in every 13 Americans could experience a tangible financial loss from identity theft resulting from a healthcare breach. They believe this would anger and inconvenience consumers enough to switch health providers.

Table 4: Health Systems Potential Revenue Loss Due to ID Theft



Sources: Accenture analysis, HHS Office for Civil Rights, Ponemon Institute

Kaveh Safavi M.D., J.D., managing director of Accenture's global healthcare business states "If healthcare providers are complacent to safeguarding personal information, they'll risk losing substantial revenues and patients as a result of medical identity theft."

What to Expect in 2016

It is unlikely that attackers will stop targeting healthcare organizations anytime soon. The economics are simply too compelling. PHI remains a valuable commodity on the black market and cyber defenses to date have done little to discourage hackers from attempting to steal it. As John Halamka says "Not a day goes by where we don't receive some kind of email with a phishing or spear-phishing campaign. They're getting increasingly sophisticated." [5]

That said, at Redspin, we are seeing early indications of positive change. 87% of respondents to the 2015 HIMSS Cybersecurity Survey indicated that information security had become a critical business priority during the past dozen months.[6] More and more of our healthcare clients are requesting services such as network penetration tests, vendor risk management, and social engineering testing of their employees. These services compliment annual security risk assessments as they can be conducted at shorter intervals and deliver immediate, actionable results.

Chuck Kesler, CISO at Duke University Health System, has seen a shift to a "breach first" mentality. He says "there's a sense of urgency out there right now…. In many ways what you need to do is start with the assumption that you're going to have a breach soon…." [7]

Focusing on the likelihood of a breach is a proactive security posture. Potential threat vectors can be identified and mitigated with immediacy, rather than after an event occurs. HIPAA risk assessments are necessary but not sufficient. They meet compliance and meaningful use objectives but healthcare organizations can be compliant without being secure. The breach statistics certainly bear this out.

[5] *"CIO Halamka on Security Action Items for 2016,"* www.healthcareinfosecurity.com December 15, 2015
[6] http://www.himss.org/2015-cybersecurity-survey
[7] http://www.healthcareitnews.com/news/duke-health-ciso-chuck-kesler-healthcare-shifting-breach-first-mentality

Conclusion

2015 exposed to the world how vulnerable the U.S. healthcare industry is to cyberattacks. And safeguarding PHI is likely to get even more complex. "As providers, payers, employees, patients, and partners become increasingly intertwined through shared data, transparency, and analytics, the opportunities for loss, error, or theft grow exponentially."[8] The stakes will get higher too. To date, theft or loss of PHI has led to breaches of privacy and confidentiality; future hacking attacks could compromise the availability and/or integrity of health data, putting lives at risk.

The hacking of medical devices poses an even more direct risk to patients. "Hundreds of thousands of medical devices such as patient monitors, infusion pumps, ventilators, and imaging modalities – many of which are life-sustaining or life-supporting – currently reside on hospital networks across the United States. Other medical devices are accessible via wireless technologies, for example, insulin pumps and pacemakers." [9]

More than anything, the 2015 experience calls out for a fundamental change in how healthcare organizations view IT security risk. It is not just a compliance and privacy issue – it is a trust issue, one that can ultimately jeopardize an organization's ability to deliver patient care. It is a business issue if, as Accenture predicts, medical ID theft will lead to a loss of patients and lost revenues at providers. And it is a legal and ethical issue if failing to protect sensitive data, IT infrastructure and/or medical devices leads to preventable loss of life.

Securing the healthcare environment should now be a part of every health organization's strategic plan. Embracing IT security in its full definition – confidentiality, integrity, and availability – is in alignment with other strategic goals such as improved patient care delivery and better patient outcomes.

[8] http://www.informationweek.com/healthcare/security-and-privacy/10-ways-to-strengthen-healthcare-security

[9] "Networked Medical Device Cybersecurity and Patient Safety," Deloitte

About the Author

Daniel W. Berger is the President of Redspin, an Auxilio Company. Redspin is a cybersecurity professional services firm based in Santa Barbara, CA that provides penetration testing, IT security risk assessments, and consulting services nationwide. Under Mr. Berger's leadership, Redspin has become a leader in healthcare cybersecurity, providing HIPAA security risk analysis services to 135 hospitals, nearly 1,000 clinics and many business associates. The company helps healthcare organizations meet and maintain HIPAA compliance while fulfilling the security risk analysis requirement for "meaningful use" under the EHR incentive program. More importantly, Redspin helps safeguard PHI from data breach.

Mr. Berger is a frequent speaker at industry conferences on the topic of healthcare cybersecurity. Prior to joining Redspin, he spent 25 years in the global networking industry holding senior sales, marketing, and general management positions in companies ranging from the Fortune 500 to ground-floor start-ups. In 1996, Mr. Berger received a commendation from the Oklahoma City Department of Health for his participation in the conference "The Role of Technology in Disaster Preparedness." He is an honors graduate of Colby College in Waterville, ME and was awarded distinction in his major field of study.

Redspin, An Auxilio Company

4690 B Carpinteria Avenue

Carpinteria, CA 93013

T: 1-800-721-9177

info@redspin.com