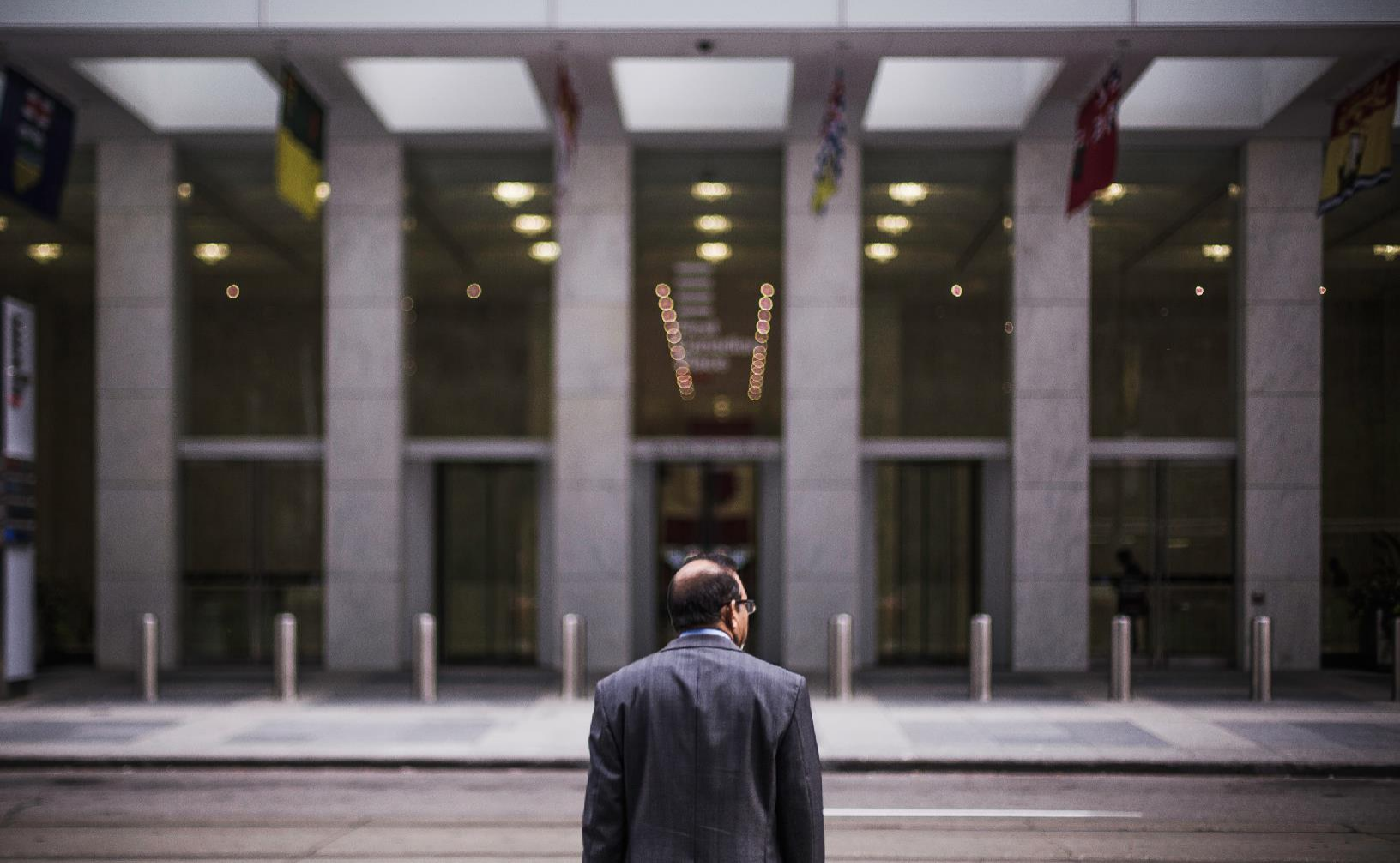


Making the Business Case Today for Enhanced PHI Security

The Financial Impact of Breached Protected Health Information: 2017 Update

Table of Contents

Introduction

By Rick Kam

One of the morning news programs has the slogan "What a difference a day makes." As we prepare this paper for the 2017 PPN conference, I'm thinking what a difference a few years and a group of passionate, dedicated people can make.

In early 2010, Ponemon Institute had already released a couple of studies showing that the rising tide of breaches wasn't being matched by growing investments in PHI protection. One day, a group of colleagues was speculating as to why healthcare organizations weren't investing more, and we hypothesized that it was difficult to make the business case for PHI protection without a way to assess its business value. Today's accounting system is based on centuries-old methods that are designed to account for fixed assets. Until recently, no one had begun figuring out how to value data.

To address the problem, we proposed a project to ANSI's 170 member organizations: an expert collaboration to develop a methodology for calculating ROI on PHI protection. The response was amazing. Seventy-seven companies signed on. More than 250 contributors volunteered their expertise in compliance, operations, technology, cyber insurance, law, and more. The team met soon after in Washington D.C. and formed sub-committees to address different aspects of the problem.

In 2012, after a year and a half of work, the American National Standards Institute (ANSI), the Santa Fe Group (SFG), and the Internet Security Alliance (ISA) published *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security.*[1] The new methodology made quite a splash. Howard Schmidt, czar for the Obama administration, helped us launch the paper at the D.C. press club. Chief Privacy Officer of Health and Human Services kicked off the meeting, and we presented to Congress that afternoon.

At the end of that meeting, a handful of us went to a little Mexican restaurant a block from the capital to celebrate. As we toasted with margaritas, one of our chief contributors asked, "Now that we've published this, how about doing a workshop to create champions for this approach?" Instead of just a workshop, we decided to create an ongoing learning and support community, and the PHI Protection Network was born.

A lot has changed in the ensuing 5 years. Today, the PPN has grown from the original 250 collaborators to about 400 members. It has brought together a unique combination of close associates across a spectrum of specialties and organizations, people with the talent and perspective to do projects like developing an annual education conference, and now this update to the 2012 report.

We are most proud of those that have used the insights from the original paper and the financial model to create their own business cases. Included in this update is an example of the use of the PHIve model at the University of California by contributor Grace Crickette. Grace's efforts have been acknowledged by the PHI Protection Network as the 2017 PHI Hero for her commitment to protecting health information.

The contributors to this paper include some of the original team plus new members who have brought their knowledge and commitment to the cause. As you will read in these pages, the challenges of protecting PHI have only grown with the digitalization of healthcare and our society and the increasing resourcefulness of the criminal element.

But we have also made progress, with new security technologies, innovative privacy and compliance programs, and improved success in getting our organizations on board with PHI protection. We hope this paper will help you build on the progress we've made. The ability to justify PHI protection to our organizations is needed now more than ever.

—*Rick*

chapter one:

The Progression of the Healthcare Ecosystem

It is said that, as a society, we accomplish more each year than the previous year, due mostly to our collective education and technologies. This is abundantly true for the healthcare ecosystem. In 2012, when the whitepaper *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security*[2] (the "2012 report") was written, the sweeping effects of what is now called the "digitalization" of healthcare were just being realized, and the impact on our society, our lives and our health continues to grow.

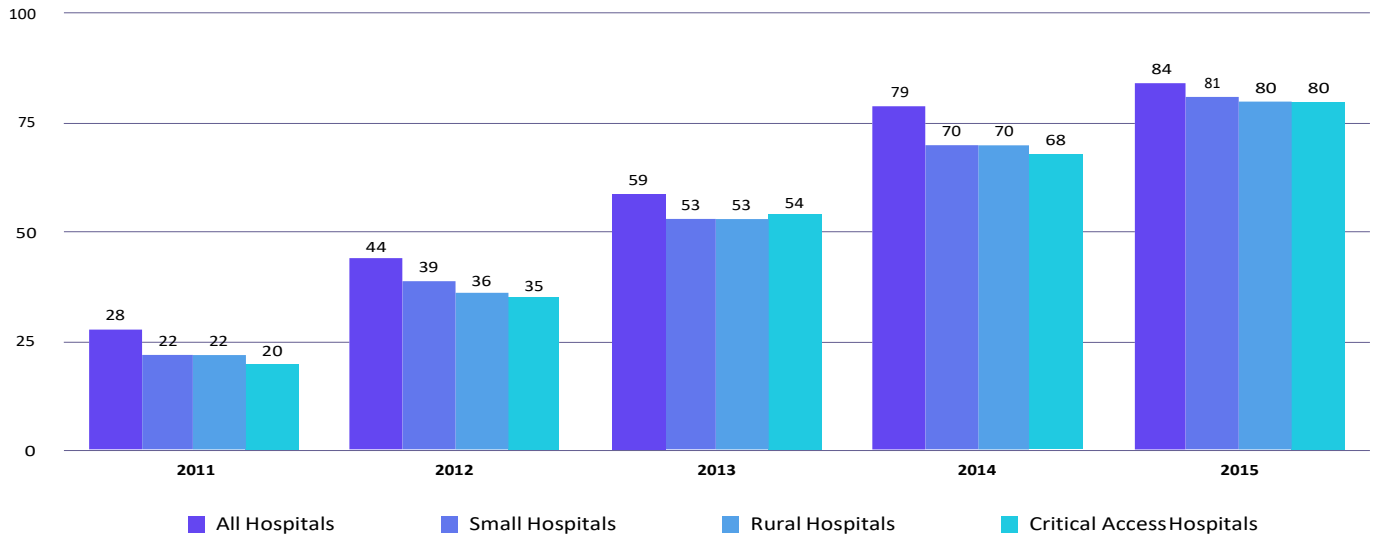


Figure 1 Healthcare Ecosystem - http://healthcare-competitiveness.com/news/

According to data from the Office of the Nation Coordinator for Health IT ("ONC"), the adoption rates for basic Electronic Health Records systems (EHR) increased significantly from 2011 to 2015:

- Critical access hospitals increased from 20 percent in 2011 to 80 percent in 2015
- Rural hospitals increased from 22 percent in 2011 to 80 percent in 2015
- Small hospitals increased from 22 percent in 2011 to 81 percent in 2015

Basic EHR adoption requires the system to have a set of EHR functions that certain functionality such as physician notes, advance directives, lab reports, or radiology tests, among others.[3] The four key domains of interoperability as defined by the *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*, include: electronically sending, receiving, finding, and integrating or using key clinical information.[4] Only 26% of non-federal acute care hospitals were utilizing all four domains in 2015.[5]

A similar survey by ONC on the adoption of EHR systems by physicians reported that 75% of physicians had adopted a certified EHR[6] but only 60% of them were viewing image results electronically.[7] Certified EHR technology meets the certain specific technological capability, functionality, and security requirements adopted by the Department of Health and Human Services (HHS).

Congress declared the achievement of widespread exchange of health information a national objective in the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA).[8] Despite the increased adoption of EHR systems, the results in terms of improvement in interoperability remain mixed.[9]

Still, the advancement of the technology has opened the doors for new uses and new stakeholders in the healthcare ecosystem. Since 2012, the digitization of healthcare information has extended to medical devices, from insulin pumps and pacemakers to advanced surgical systems and personal fitness devices, social media interactions, mobile applications, Customer Relations Management ("CRM") applications, collaboration tools, and more, creating more opportunities to aggregate healthcare and analyze healthcare options. Predictive analytics now can take advantage of artificial and machine intelligence to understand historic patterns and predict the future, including health outcomes, with the goal of refining medical treatments and reducing readmission rates.

The Ramifications

In 2012, healthcare organizations were just beginning to embrace digitalization. Today, electronic PHI (ePHI) flows across clinic and hospital networks, across public and private Wi-Fi, and across the Internet. ePHI is accessible everywhere in today's healthcare system —a far different scenario than the tightly controlled availability of paper records.

There was an understanding, even at the initiation of this endeavor, that with more stakeholders and more data, the opportunity for misuse would grow. It has. The number of breaches and complaints to the Office for Civil Rights (OCR), the agency responsible for enforcing the Health Insurance Portability and Accountability Act (HIPAA), have multiplied annually. New threat agents such as state-sponsored hackers, new attack tools such as ransomware for purchase on the Dark Web , and new vulnerabilities, including insufficiently protected devices and unpatched applications, have increased the ease and the rewards of stealing health information. The threats to the security of PHI are not specific to one stakeholder group but are ubiquitous throughout the entire ecosystem due to the volume and availability of PHI data and transmission of ePHI records.[10]

Over the last 5 years, the digitalization of medical information has taken healthcare capabilities to new heights and in new directions, and the pace of future change is limited only by the imagination. It is now time for those with the responsibility to protect health information to be given the resources and funding to do so.

According to a January 2015 Federal Trade Commission (FTC) report titled "Internet of Things: Privacy & Security in a Connected World," the year 2009 marked the first time that the number of "things" connected to the Internet surpassed the number of people in the world.[11] In early 2016, technology consulting firm Gartner projected that 6.4 billion connected things would be in use worldwide by the end of the year, up 30% from the previous year, and that the number of connected things would grow by more than three times, to nearly 21 billion by the year 2020.[12] While these devices can significantly improve the

lives and health of consumers worldwide, PHI risks multiply as digitization continues to evolve.

Another disruptive technology began to take hold in 2016: artificial and machine intelligence. We're all familiar with natural language processing from the personal assistants on our cell phones: it become commonplace to use machines that understand human voice commands at least as well as humans do. And roughly 40% of industries are now using predictive analytics that rely on a machine's capacity to understand historical patterns and predict the future. Healthcare has begun using machine intelligence to predict health outcomes, to refine medical treatments, and to drive robotic surgeons carrying out procedures not possible with human hands. In the near future, the advent of quantum computing will increase the ability of machines by orders of magnitude, likely yielding new capabilities such as gene and DNA splicing.

With ePHI center stange, the coming acceleration of change in healthcare is limited only by one's imagination.

chapter two:

The Evolution of Laws, Rules, and Regulations

In 2016, HIPAA celebrated its 20th anniversary as a federal regulation. Since that time, the regulatory and legal landscape has evolved to place broader and deeper responsibility on healthcare organizations to protect the privacy of PHI.

The Omnibus Final Rule

In early 2012, the Modification to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules was submitted to the White House Office of Management and Budget for review. The Omnibus Final Rule ("Rule") included changes to various HITECH Act provisions and major updates to HIPAA. In addition to clarifying that the definition of a breach includes even limited data sets of health information, the Rule established a new criterion for breach notification: "risk of compromise" rather than "risk of harm;" and new noncompliance penalties of up to $1.5 million per violation per year[13] for entities covered by the regulations, known as "covered entities (CEs)".

It also expanded individuals' access to and control of their PHI and put limits on use or disclosure of patient information for marketing and fundraising purposes. And significantly, the Rule made business associates (service providers of CEs that handle PHI on their behalf) and their subcontractors statutorily obligated to comply with the HIPAA Rules. The Rule went into effect in 2013, and as of August 2016, the ten largest HIPAA settlement amounts ranged from $1.7 million to $5.55 million.[14] In November 2016, under the new Federal Civil Penalties Inflation Adjustment Act, HHS increased by 10% penalties for HIPAA violations[15], suggesting that future fines for non-compliance are likely to be larger still.

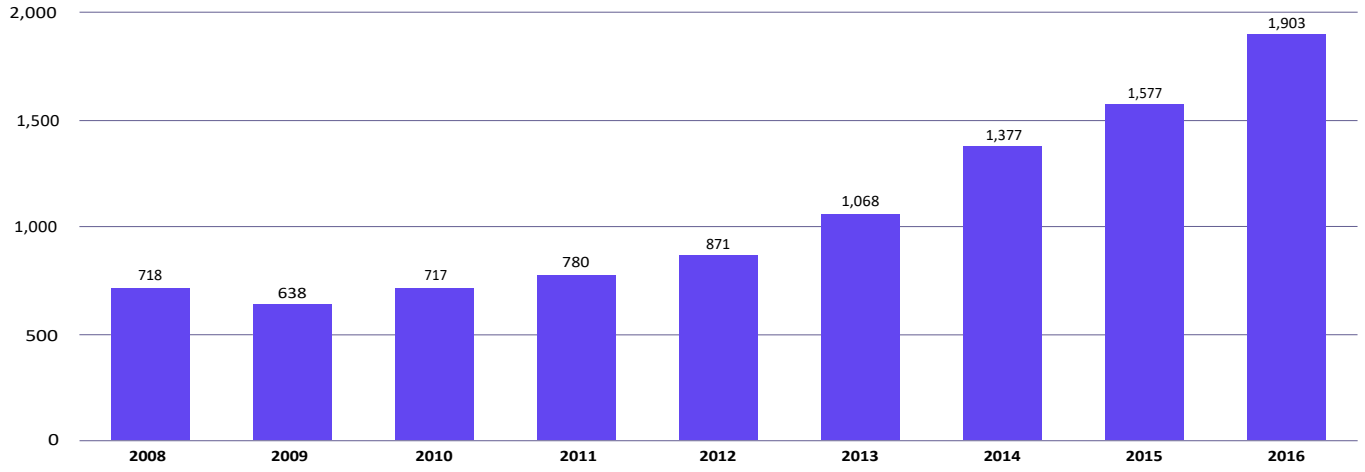
OCR Compliance Audits

The OCR began conducting compliance audits of applicable healthcare organizations in 2011.[16] The objective of the first round of audits was educational:

"to assess compliance efforts…examine mechanisms for compliance, identify best practices and discover risk and vulnerabilities" not seen before.[17] Only 11 percent of the organizations audited were found to be in compliance.[18] While the first phase of audits involved only 200 covered entities ("CEs"), the audit program has since expanded to cover more CEs and to include business associates (BAs) as well.[19] Industry reports over the last 5 years have shown that smaller healthcare organizations and BAs are most likely to struggle with compliance and therefore are at greater risk of data breaches. Now, in Phase 2 of the audits initiated in 2016,[20] OCR is auditing a larger and more diverse group of healthcare organizations. The more comprehensive audit procedures developed and tested in Phase 2 will then be used to develop a permanent, ongoing audit program.

Complaints

The volume of complaints reported to OCR has more than doubled since 2012 due, in large part, to the implementation in 2014 of an on-line reporting capability as well as increased education and awareness surrounding the rights that patients have under HIPAA. In 2016, complaints averaged 63 per day. OCR follows up with every complaint that they receive, formally investigating approximately half of them, resulting in corrective action plans for 70% of those investigated.



Monthly Average Complaints Received

Nine of the forty-nine settlement agreements to date were initiated from complaints.[21] The odds of being audited may be small for now, but the odds of being investigated by OCR are increasing.

New Guidance on Cyber Attacks, the Internet of Things ("IoT"), and More

As new privacy and security threats have evolved, regulatory agencies have responded with new rulings and guidance. As more and more medical devices connect to the Internet, the FDA has issued guidelines on cyber security for medical devices,[22] recommending that medical device manufacturers and healthcare facilities take steps to assure that medical equipment doesn't become a vector for cyber attacks. In September 2015, the HHS Office of Inspector General (HHS/OIG) issued two reports recommending the provision of additional guidance to organizations related to compliance. As a result, OCR began to issue more guidance to help healthcare teams protect PHI by spotting phishing attacks,[23] outlining safe use of Internet applications[24] and mobile devices,[25] and giving guidelines to HIPAA privacy for increasingly popular employee wellness programs. HHS has also taken steps to address new technical trends such as cloud computing,[26] which has seen huge adoption in the healthcare industry, and health-related mobile applications.[27] And in July 2016, in response to a 300 percent increase in ransomware attacks reported in the first 6 months of 2016 compared to 2015, the agency released a fact sheet on ransomware[28] and HIPAA stating that ransomware attacks must be assessed as potential data breaches, and if notification to impacted individuals and HHS/OCR is not provided, the entity bears the burden of proof that the incident did not pose more than a low probability of compromise to the ePHI involved.

State Data Breach Law

State regulatory agencies have not sat idly by in the last 5 years watching federal progress. The HITECH Act gave State Attorneys' General (AGs)[29] the authority to bring civil actions on behalf of their residents for violations of HIPAA; OCR provided comprehensive enforcement training to help the state AGs in investigating and seeking damages for HIPAA violations that affect residents of their

states.[30] States have also been busy passing new or updated data breach laws in their states, most recently in early 2017 in New Mexico[31] These new and updated laws have, among other requirements:

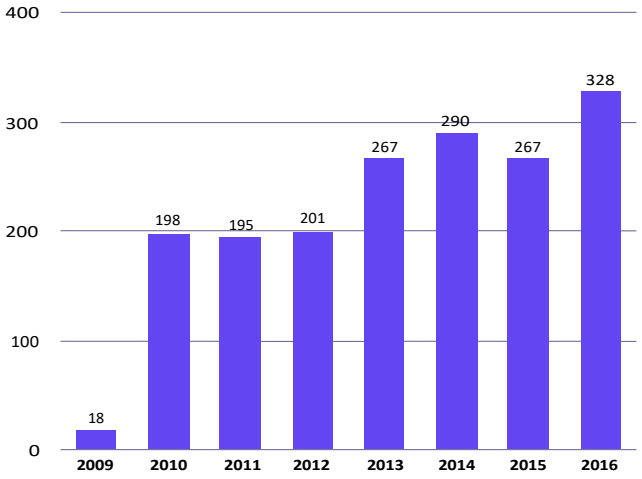
- Shortened timeframes required for reporting to affected individuals
- Required certain content in the notification letters
- Mandated that entities offer specific mitigation such as credit monitoring services
- Required reporting to Attorneys General, in some cases when only one individual's information is affected

The regulatory environment, like information security, is evolving. Part of the mission of privacy professionals is to keep their organizations' programs and priorities in compliance with this changing regulatory landscape.

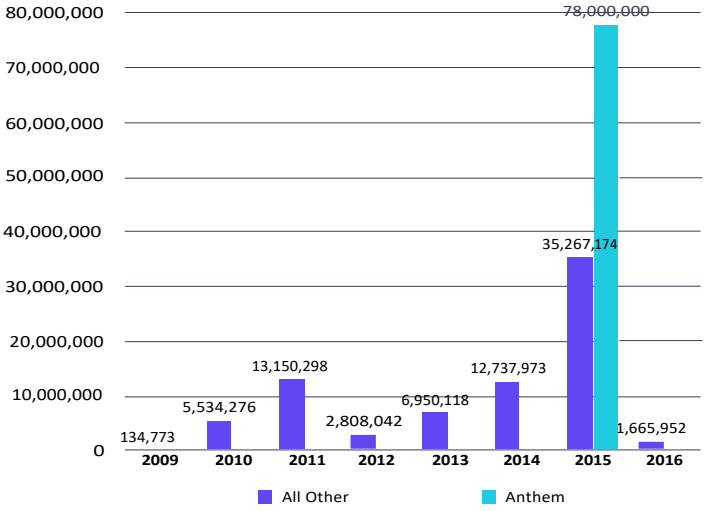
chapter three:

The PHI Data Breach Landscape

In 2012, data breaches involving PHI were exploding. In the previous 4 years (since the Breach Rule went into effect in 2009), almost 21 million health records had been breached according to large (>500 impacted individuals) breach reports to the OCR.



Number of Reported Breaches >500 Records



Number of Records

This trend has accelerated. In the last 4 years alone, over 171 million records have been reported breached to the OCR. In 2012, our report noted that, at $60 billion a year, Medicare fraud had become one of the most profitable crimes in America. According to the U.S. Department of Justice, some estimates now put healthcare fraud at over $100 billion per year.[32] The growth in frequency and severity of PHI data breaches continues for a simple reason: healthcare crime pays. In 2012, hacking and Information Technology (IT) incidents, represented only 8% of the total breaches reported to OCR; in 2017 that number has grown to 34%, and the total number of records breached is 14 times higher.[33]

In 2012, the largest breach due to hacking/IT incident reported to HHS was by a hacker from Eastern Europe who broke into the Utah Department of Technology Services' server using a weak password and accessed the medical records of 780,000 individuals, including Social Security numbers for Medicaid claims.[34] In 2015, Anthem, Inc., reported the largest breach reported to HHS/OCR to date, 78.8 million individuals, as a result of a hacking attack. That same year, Premera Blue Cross and Excellus BlueCross BlueShield also reported hacking incidents to OCR impacting 11 million and 10 million individuals, respectively. In 2016, three hacking breaches exceeded a million records each: Banner Health,[35] Newkirk Products,[36] and 21st Century Oncology.[37]

	2012		2016		Multiple
Hacking / IT Incident	900,684	8%	13,426,813	34%	13.9
Improper Disposal	21,830	4%	125,730	2%	4.8
Loss	96,952	10%	557,952	5%	4.8
Theft	1,017,765	64%	904,451	19%	(0.1)
Unauthorized Access / Disclosure	770,811	14%	1,641,006	40%	1.1
	2,808,042		**16,655,952**		**4.9**

Number of Records Breached by Reported Cause

Criminals are developing new tactics to make hacking more profitable. Instead of mounting time-consuming direct attacks on networks, they are attacking from inside our firewalls and inside our buildings, what Angela McKay, Director of the Government Security Policy and Strategy at Microsoft,[38] has called the "soft underbelly" of healthcare's network defenses.

The Enemy Within

In a recent interview, McKay stated that we are past the point of defending the perimeter: our perimeters have already been breached, and the attackers are inside. Our job now is to stop the looting and pillaging. This is certainly true in

healthcare data breaches. A 2016 report from the Ponemon Institute found that 49% of healthcare breaches are due to insiders,[39] some unintentional (36%) and some intentional and malicious (13%).[40]

Who's Most at Risk

While the news stories focus on big PHI breaches at large healthcare organizations, the secret gold mine for criminals is small private practices or clinics and small business associates. OCR has stepped up their investigation of breaches affecting fewer than 500 individuals,[41] the details of which aren't as easily researched. Reports of such smaller breaches are due annually to OCR 60 days after the end of each calendar year for breaches discovered during the preceding year.[42] OCR has also announced in 2017 its first resolution agreement for untimely breach reporting with Presence Health, which included a payment of $475,000 and a corrective action plan.[43]

Small offices can't afford industrial strength security. Their staff is often handling multiple functions and too busy to stay on top of security practices. Vulnerable to attacks, a patient record from the small medical office is worth just as much on the black market as a patient record from a large urban hospital that has more sophisticated security controls and takes longer to successfully exploit vulnerabilities.

The breach reported in 2016 by Athens Orthopedic Clinic illustrates the challenges for smaller organizations. Attackers gained access to clinic networks using login credentials stolen from a third-party contractor and stole the records of almost 400,000 patients—every record the clinic had ever created. The hacker who claimed responsibility under the alias "The Dark Overlord" claimed to have had access, without detection for months, to the clinic's systems using the credentials of an outside contractor who performed certain services for the Clinic.[44] As larger organizations become better at countering breach threats, smaller organizations become bigger targets, so they must become even smarter in countering threats.[45]

PHI Care is Patient Care for Providers

Another significant increase in the breach landscape is public awareness. Today, with mega-breaches and ransomware attacks in the news, in addition to breach notifications to millions of Americans, the public is more aware than ever of the dangers of compromised health information, often resulting in damage to a healthcare organization's reputation and bottom line. In 2016, the FBI Cyber Division reported that 70% of people won't go back to a hospital that has been breached.[46] With medical payment reform (MACRA) going into effect in 2017, more than ever doctors need to be confident that strong PHI security is part of the care they provide their patients, or their public ratings could suffer.

In today's healthcare industry, protecting PHI is an integral part of health care because PHI is forever. Unlike a stolen credit card, patient's medical records can't be cancelled or reissued with a different number. With near-universal adoption of EHR systems, Internet-connected health systems, the Internet of medical "things", and mobile access, PHI is at constant risk. Organizations need to understand the risk and invest in PHI security efforts that are up to the challenge.

chapter four:

Threats and Vulnerabilities

The 2012 report outlined 11 elements that threatened PHI security, including various insider threats, outside attacks, and emerging factors such as mobile, cloud computing and the "virtual physician's office," now referred to as telemedicine. All of these vulnerabilities and threats still exist, but they have expanded with the growing digitization of healthcare and the increasing sophistication of cybercrime.

Threats

As healthcare has progressed in its digital transformation, PHI theft has progressed with it. In 2012, some of the most significant breaches were caused by lost or stolen media or by human error such as improper disposal of medical records. In 2015, cyber attacks became the primary cause of data breaches across all industries.

Cyber Crime is Big Business

Cyber crime is now organized like big business. An aspiring attacker can find business training, tools, and ready markets on the Dark Web.[47] Highly sophisticated hacking tools are now available for purchase on dark net markets as point-and-click Software-as-a-Service (SaaS) model. On the Dark Web, would-be hackers can purchase access to malicious services such as:

- A point-and-click distributed denial of service (DDoS) attack for as little as $10 for an hour
- Remote access to compromised servers and networks inside medical facilities for $2,000
- Full botnet command and control capabilities in the $1,000 range
- Code for several botnet variants has been released into the wild and can be downloaded and used for free

Meanwhile, medical identities remain a valuable asset on black markets due to the availability and longevity, in addition to the relative ease of obtaining them.

The Emergence of Ransomware

While selling stolen medical identities can be lucrative, more enterprising thieves are increasingly cutting out the middleman by encrypting all the data at medical and health systems and holding it for ransom. Numerous ransomware attacks in 2016 brought hospital operations to a halt, delaying treatment or diagnosis and putting lives at risk, forcing ransom payments and causing untold reputational damage. Alarmingly, the number of ransomware variants increased 752% in 2016.[48] As healthcare organizations have become smarter about backing up systems, ransomware attackers have grown more sophisticated at corrupting backups or exfiltrating data before demanding ransom, so that they can back up the threat of data destruction with a threat to expose already stolen information.

Vulnerabilities

Over a half million covered entities participated in the Centers for Medicare and Medicaid Services (CMS) Electronic Health Records (EHR) incentive programs, and the resulting change is revolutionizing how we deliver and evaluate healthcare. Unfortunately, too many security practices have not kept pace with digitization. protections of the traditional network perimeter through public networks to the cloud and mobile devices.

Update on Mobile Devices

In late 2016, the number of people accessing the Internet through mobile devices (smartphones and tablets) surpassed the number connecting through personal computers globally.[49] This confluence of mobile device adoption with medical record digitization has finally brought the realization of the promise of telemedicine within reach. Approximately 61% of U.S. health care institutions and more than 50% of hospitals currently use some form of telehealth.[50] PwC projected in December 2015 that "In 2016, millions of American consumers will have their first video consults, be prescribed their first health apps, and use their smartphones as diagnostic tools for the first time."[51] The implementation of appropriate mobile security infrastructure is not keeping pace.

Health care staff have been enthusiastic adopters of mobile computing. Doctors use their mobile devices to access and send medical image files and information. 96% of physicians own smartphones and between 56% and 76% own tablets.[52] Nurses also use smartphones for patient care far more than previously estimated. Some 95% own a smartphone and 88% of them use smartphone apps for work. Ensuring that effective mobile security controls are actively protecting these health workers' devices as they send and receive PHI remains a significant challenge. Mobile devices are an attractive hacking target and the majority are in fact vulnerable to compromise, allowing them to be both a source of data breaches and to be used as attack vectors for more widespread infection.

As the use of mobile devices in the health care industry has grown, so too has the rate of mobile malware development. Security vendor McAfee reported that its collection of mobile malware variants grew by 151% over the previous year to just under 2 million strains in the first two quarters of 2016.[53] Organizations should consider this carefully when deciding to transfer security risk to mobile devices that are used as a core component of two-factor authentication infrastructure.

Increasing Number of Connected Devices

In 2012, IoT was barely on the radar, but today internet-connected medical infrastructure and medical devices have to be top of mind for security teams. The FDA has pushed medical device manufacturers to build in better security to protect medical devices such as pacemakers and insulin pumps.[54] In addition to connected medical devices, the move to "smart" buildings and connected appliances, the healthcare IoT has come to include a hospital's refrigeration unit, HVAC unit, and energy controls, as well as the TVs, security cameras, Wi-Fi routers, and other connected devices that are an everyday part of our infrastructure.

All these devices present a three-fold threat: they can be hijacked and held for ransom, they can be hacked to steal data directly or attack healthcare networks, and the devices themselves can be weaponized—harnessed for DDoS or botnet attacks. Typically, the investment in devices for efficiency has not been accom-

panied by investments in security to protect those devices or the networks to which they are connected.

Cloud Service Providers

According to The Economist, healthcare is second among major industries regarding adoption of cloud services.[55] Cloud computing poses different vulnerabilities than in-house networks, and with large numbers of potentially affected individuals and websites, there are very significant aggregated risks. The security of cloud services is typically based on a shared responsibility model and many healthcare organizations don't always have a clear understanding of where their responsibility begins and ends. This lack of clarity can lead to critical security controls slipping through the cracks.

For example, there are many systems designed to protect data in the cloud, but these are typically add-on services that require skilled resources and time to implement. Regardless, shifting computing infrastructure to the cloud doesn't get around the problem of information security: either way, it takes time, money, and skilled human resources. For small to mid-sized organizations with limited information security budgets, migrating to the cloud may result in an improvement over in-house security in a standard server environment. But covered entities and business associates need to assess risks carefully and gain an explicit understanding about security expectations and responsibilities with any cloud vendor.

Shadow IT

"Shadow IT"[56] has now risen to the forefront of vulnerabilities. Individuals create new vulnerabilities and risk exposures for their organizations by employing IT solutions and applications that store data outside of, and in many cases completely invisible to central IT and are therefore unprotected. According to CipherCloud, 80 percent of employees admit to using unsanctioned Software-as-a-Service (cloud-based applications).[57] Eighty-three percent of support staff concede that they know the cloud applications they are using are unsanctioned.[58]

Getting these non-sanctioned applications under the security umbrella can be a long, costly process. Gartner predicted that shadow IT management would

account for one third of IT expenses in 2016 and that shadow IT would be implicated in a third of security breaches.[59] Shadow IT also greatly complicates incident tracking and response due to the difficulty of determining the information compromised and the individuals who had access to the shadow IT information.

Hiding from Cyber Risk Is No Longer an Option

Five years ago, PHI data breaches were an unfortunate risk of running a healthcare practice, something that could possibly be prevented with better physical and network security and by training staff in good privacy and security practices. Today, with well-armed, determined attackers targeting our information, using multiple vectors across a vast and rapidly expanding attack surface, PHI data breaches are inevitable.

Teams still need to be trained in good privacy and security practices, but investment is needed in tools and programs that will detect attacks early and build resilience to help limit the damage inflicted by cyber criminals. In 2012, losing an unencrypted laptop containing PHI was an act of carelessness. Today, it can be considered willful neglect of an organization's duty to protect that PHI under the law. Defining what is considered "reasonable and appropriate" security protection for each organization is a requirement of the Security Rule, and not doing so can result in significant financial damage and operational distraction for an organization in OCR's cross-hairs.

chapter five:

Safeguards and Controls

Protection Through a Risk Analysis

In 2012, advice on safeguards and controls for PHI was very much centered on policies, procedures, and technology as preventive measures. The 2012 report also highlighted many up and coming threats such as mobile devices, business associates, cloud service providers, virtual physician's offices, wireless devices and state-sponsored cyber-crime. The largest breach at that time was 4.6 million records stolen out of a contractor's car. Massive PHI breaches weren't so often in the news, and many were more concerned about compliance and the looming possibility of OCR audits. Since then, hundreds of millions of healthcare records have been breached.

Because no one has an unlimited security budget, a more fundamental process needs to be established that assesses current vulnerabilities and ranks the risks according to the strength of the safeguards or controls in place to reduce the likelihood and impact of a breach. Aligning budgets to address the highest ranked risks will go a long way towards protecting PHI from impermissible access or disclosure.

Go Deeper with Risk Analysis

OCR has been stressing risk analysis for many years. Their warnings started in earnest with former OCR Director, Leon Rodriquez, and continued to be emphasized by his replacement, Jocelyn Samuels. But it has only been in recent years that OCR has emphasized the need to include BAs in a CE's risk assessment. Four out of the 47 settlement agreements have highlighted noncompliance by BAs. The challenge of BA risk analysis is how deep the assessment should go. Providing details of a risk analysis to a customer CE, exposing security weaknesses and results is yet another vulnerability for the BA. Resources of the CE are then required to review those risk analyses and decide on a course of action and follow-up.

The Privacy Rule states that the CE must obtain "satisfactory assurance" that the BA will appropriately safeguard the information.[60] The Omnibus Final Rule added that a BA must do the same for their subcontractors.[61] OCR has posted a number of frequently asked questions (FAQs) on their website related to BAs, indicating that "covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract." [62]

OCR also provided this guidance regarding Cloud Service Providers ("CSP") but the guidance applies to any BA: "The HIPAA Rules do not expressly require that a CSP provide documentation of its security practices to or otherwise allow a customer to audit its security practices. However, customers may require from a CSP (through the BAA, service level agreement, or other documentation) additional assurances of protections for the PHI, such as documentation of safeguards or audits, based on their own risk analysis and risk management or other compliance activities." [63]

And finally, regarding certifications, OCR posted this information:

". . . there is no standard or implementation specification that requires a covered entity to "certify" compliance [of their BA]. The evaluation standard §164.308(a)(8) requires covered entities to perform a periodic technical and non-technical evaluation that establishes the extent to which an entity's security policies and procedures meet the security requirements. The evaluation can be performed internally by the covered entity or by an external organization that provides evaluations or "certification" services. It is important to note that HHS does not endorse or otherwise recognize private organizations' "certifications" regarding the Security Rule, and such certifications do not absolve covered entities of their legal obligations under the Security Rule. Moreover, performance of a "certification" by an external organization does not preclude HHS from subsequently finding a security violation.[64]

Since BAs have been responsible for nearly 20% of breaches and over 40% of the records breached, CEs and upstream BAs must determine the best way to achieve satisfactory assurances of their high risk-ranked downstream BAs.

Protect Credentials with Training, Management, and Monitoring

The criminal element has become well-organized and well-funded in the last five years—in some cases even state-sponsored. Criminals are always finding more clever and convincing ways to trick workforce members into exposing their PHI. To help combat phishing and social engineering, more training is needed for the healthcare workforce. A 2015 study by the Ponemon Institute found a 50X return on investment (ROI) on anti-phishing training.[65] Social engineering tactics will continue to evolve, requiring that training programs be continuously utilized, updated, and enhanced.

Because no amount of training will be successful in stopping all social engineering attacks, it is important to continually inventory and continuously protect login credentials that have privileged access. Privileged accounts should require longer passwords—some organizations require up to 20 characters—and be more frequently changed than login passwords for the general workforce. People with privileged accounts should be using two-factor authentication for remote access. It's also important to monitor changes to access privileges, for example, to the Domain Admins group in Microsoft Active Directory.

Monitor What You Can't Control

Securing the perimeter of an organization has changed in today's computing world because the perimeter has become very loosely defined. Mobile technology, cloud computing, and IoT, including biomedical devices, all connect to a hospital's network. As boundaries continue to change, these endpoints need to be inventoried, analyzed for risk, and secured.

As the boundaries of our networks become less clear, it is critical that the environment is monitored to identify when bad things are happening so that we can contain the damage. Several 2016 studies found that on average, unauthorized access occurred for over 200 days before breaches were discovered.[66] Persistent monitoring helps confirm that safeguards and controls are working as expected and ideally discovers problems sooner.

More and more endpoints are being added to networks, some without appropriate safeguards. In 2015, the Food and Drug Administration (FDA) issued an alert regarding medical device security risks highlighting an infusion system that could be accessed remotely through a hospital's network, allowing an unauthorized user to control the device.[67] Also in 2015, a third-party application used in hospitals' medical record systems exposed the health information of 3.9 million patients of more than 230 hospitals, doctors offices, and clinics, when a hacker realized that authentication was being handled by the application itself.[68] Due diligence of security measures used by device manufacturers and software developers should be required before use.

Manage Vulnerabilities

Basic measures such as applying security updates are critical to protect PHI. The challenge for healthcare is the time required to test patches before applying them to systems used to treat patients. For devices regulated by the FDA, the patching cycle can be nine months or more.[69] When there are known vulnerabilities that can't be addressed immediately, compensating controls need to be created. For example, medical devices with known vulnerabilities could be set up on a separate network segment, limiting traffic to them. Privileges could be set to block attempts to access those devices, and rules on their network could be set to allow only certain devices to communicate with each other.

Build a Risk-based Defense

Safeguards and controls are critical for warding off criminals. Thorough, ongoing risk analyses are required to identify the greatest vulnerabilities and multiple layers of security that need to be put in place to protect an individual's PHI.

chapter six:

Survey Findings on Current Practices and Attitudes

From Compliance to Security

Surveys of organizations regarding privacy and security over the last 15 years reflect significant change, both in attitudes and organizational priorities. One of the biggest changes has been in the last 5 years, spurred on by the need to comply with various laws and regulations. In 2012, compliance was the major impetus for investing in privacy and IT security, including cyber security. In addition to HIPAA, there were other major regulations to comply with: PCI DSS[70], GLBA[71], SOX[72], and FTC[74] regulations, as well as others at the state, federal, and global levels.

Compliance was considered important to avoid fines and being in the headlines. Over the last 5 years, protecting PII and PHI has moved from a tactical to a strategic priority, as organizations realized the severity of the threat and how quickly a breach results in the loss of trust and confidence of customers and business partners. Sixty-nine percent of healthcare organizations and 63 percent of business associates participating in the *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data* (Sixth Annual Benchmark Study) believe they are more vulnerable than other industries to a data breach.[73] This change in priorities has affected how healthcare organizations structure, fund, and outfit their privacy and security programs.

Coping with the Cyber Threat

One reason that security has taken precedence is that PHI is at more risk that it was 5 years ago. The adversaries have become more sophisticated, stealthy, and dangerous. Numerous cyber breaches and ransomware attacks have shut down hospital systems and interfered with healthcare organizations' ability to provide care.[75, 76] "Cyber war" was once considered science fiction, but now nation states are attacking the pharmaceutical industry to "further their own strategic national healthcare initiatives."[77] In the *Sixth Annual Benchmark Study* survey re-

spondents reported that 50 percent of the breaches at their organizations were due to criminal attacks, including ransomware, malware, and denial-of-service (DoS) attacks.[78]

There is also insecurity that comes from too much complexity in our defenses. With the recognition of increased threats, security budgets have increased to buy defensive tools such as sophisticated monitoring and intrusion detection applications in addition to security information and event management (SIEM) systems. But implementing these systems is time-consuming and complex. In a study on the *Cost & Consequences of Security Complexity*, 71 percent of respondents reported that the complexity of their IT security architecture made it difficult for them to see the vulnerabilities in their systems, and they list complex technology, lack of expertise, and inability to integrate with other systems among the top challenges.[79]

From Compliance to Active Risk Management

There have been many positive developments in PHI protection: increased C-level involvement, focus on a culture of security, and breach response preparation.

Organizational Involvement

There is more organizational involvement in PHI protection from C-level management in healthcare. Executives and directors are coming to understand that managing privacy and security risks is part of their governance responsibility. Akin Gump lists cyber security and risk management third and fourth in its top 10 priorities for boards of directors.[80] Yet, according to the Global State of Information Security Survey 2016:

- Only 40% of board members understand their organization's security strategy
- 32% of board members are aware of it but don't commit to understanding it
- Only 25% have "formally considered security and privacy risks"[81]

According to the Healthcare and Information Management Systems Society (HIMSS) Analytics Healthcare IT Security and Risk Management Study,[82] "With

only occasional interactions with top-level leadership, there is a lack of urgency and understanding to see security as more than just a technical issue, but rather a business issue." Understanding and acceptance of the responsibility are moving in the right direction, but not quickly enough.

Culture

There is a recognition that security is the responsibility of all workforce members, reinforcing a culture of security and compliance. Training and security awareness programs can be key to supporting this culture, if the programs are relevant and effective. One of the most effective investments is in phishing awareness training. According to the 2016 *Verizon Data Breach Investigations Report*,[83] the threats of social media campaigns and phishing messages rank right below hacking and malware as attack tactics.

According to Symantec's April 2016 Internet Security Threat Report (ISTR), new malware variants jumped 36 percent from 317 million to 431 million from 2014 to 2015.[84] Over the same time period, crypto-ransomware assaults rose from 737 to 991 per day. In a 2016 study by SANS, successful spear phishing attacks have been responsible for 95% of all attacks on enterprise networks.[85] A Ponemon Study titled "The Cost of Phishing & Value of Employee Training" reported that an average 10,000 employee-company spends $3.7 million a year dealing with phishing attacks.[86] The study also reported that businesses that conduct effective training programs recognize improvement of between 26% and 99% in decreased phishing email click rates.

Preparation

More companies have an incident response plan in place today than in 2012. Five years ago, many organizations had to come up with an impromptu response when a PHI incident happened. Today, many more have a comprehensive response plan that details the investigation team, processes, mitigation activities, communication, legal contacts, remediation plans and required documentation. According to Experian's 2015 annual data breach preparedness study, senior leadership has become more involved in data breach preparedness than ever before.[87] Yet, while there is greater awareness and preparation for a breach, organizations are still not confident in their ability to secure data

and manage a breach. Response plans are often not updated regularly, and 35 percent of respondents had not reviewed or updated their response plan since it had been put in place.[88]

One of the greatest changes in protection is the availability and adoption of cyber insurance. Twenty-plus years ago, the market was immature due to the lack of sufficient statistics on frequency and impact, and the safeguards and controls deemed reasonable and appropriate to reduce the threats. In 2013, American Medical News reported that 32% of healthcare organizations had cyber insurance against breaches,[89] but sometimes, depending on the wording of the risk insurance contract, losses weren't covered. Massachusetts Bay Insurance Company did not consider falling for a phishing message a "hack" and refused to cover a $1.8 million theft as a result.[90] Now, cyber liability insurance has evolved to cover breaches, loss of data, and ransom scenarios, but premiums are increasing.[91]

On December 27, 2016, the United States Department of the Treasury issued a "Notice of Guidance" stipulating that stand-alone cyber liability insurance policies are included under the Terrorism Risk Insurance Act of 2002 ("TRIA"). Effective April 1, 2017, TRIA requires insurers to "make available" terrorism risk insurance for commercial property and casualty losses resulting from certified acts of terrorism and providing for shared public and private compensation for such insured losses.[92]

2017 predictions include the provision of cyber insurance by more insurance companies and will include extortion coverage due to the explosion of ransomware.[93]

chapter seven:

The 5-Step Method of Data Breach Costing

Despite the 5 years that have passed since the 2012 report was first developed, the 5-step method for projecting data breach costs for a specific organization, the PHI Value Estimator (PHIve), is not only still a valid approach, but is an increasing necessity. The risks to health information are greater than ever due to emerging threats, the exploitation of new vulnerabilities, the exploding amount of health information available electronically, and the expanding number of organizations that need to protect it.

Yet funds for information security are still limited. In its *Sixth Annual Patient Privacy and Data Security Report*, the Ponemon Institute reported that 59 percent of healthcare organizations and 60 percent of business associates don't believe their organization's security budget is sufficient to minimize data breaches. Given the increasing threats and continued underfunding, the PHIve method has never been more necessary to bring attention to the potential ROI from strengthening security around high risk assets. The start of the journey, however, is knowing where the exposures to PHI exist.

Table 3: PHIVE (PHI Value Estimator) - The 5 Step Method for Calculating the Potential Cost of a Breach

1	Conduct a risk assessment: assess the risks, vulnerabilities, and applicable safeguards for each "PHI home."
2	Determine a "security readiness score" for each "PHI home" by determining the likelihood of a data breach based on the "security readiness score" scale.
3	For each "PHI home" that has an unacceptable "security readiness score," examine the relevance (i.e., likelihood) of the cost using suggested cost categories, and apply a "relevance factor" from the "relevance factor hierarchy."
4	Determine the impact: relevance * consequence = impact. • Relevance = the "relevance factor" assigned to the cost category for the organization. • Consequence = the result of the cost formula provided for the cost category. • Impact = "relevance factor" multiplied by the consequence = adjusted cost.
5	Add up all adjusted costs to determine the total adjusted cost of a data breach to the organization.

HIPAA and the NIST Framework

As pointed out in the 2012 report, healthcare delivery depends on data, especially ePHI, which must be guarded and governed at a level which it has not yet achieved. As part of its ongoing effort to protect ePHI, Congress has funded development of the National Institute of Standards (NIST) cybersecurity frame- work in cooperation with U.S. industry. Now legislation is in place to implement that framework in all government agencies and recommending voluntary adoption.

In February 2016, the Office for Civil Rights (OCR) released a "crosswalk" document[94] developed jointly by NIST and the Office of the National Coordinator for Health IT (ONC), to identify "mappings" between the NIST Framework for Improving Critical Infrastructure Cybersecurity (the "Cybersecurity Framework") and the HIPAA Security Rule. The NIST framework further clarifies the NIST Roadmap for Improving Infrastructure Cybersecurity[95] to compliance but it also sets new expectations for PHI security for healthcare privacy and security teams evaluate where their systems and programs stand in relation to the NIST framework.

The good news is that the cost of conducting a PHIve assessment has been considerably reduced due to the establishment of a standard OCR-recommended risk analysis approach based on NIST. This eliminates an organization having to spend hundreds of thousands of dollars on control checklists or SOC2[96] audits, which do not comply with the regulations and do not adequately protect information.

In March 2017, the White House circulated a draft executive order on cyber security that would require federal agencies to adopt the NIST cyber security framework, and a panel in the House of Representatives has proposed a bill calling for NIST to audit federal agency compliance with its cyber security frame, further supporting its adoption.

Since 2012, OCR has provided a number of documents and recommendations to help organizations conduct a bona fide risk analysis that is the first step in the "costing of a data breach" exercise. An analysis of settlements with OCR reveals that almost 9 out of 10 (89%) of the organizations that experienced a breach of ePHI had failed to conduct a bona fide risk assessment, causing former OCR director Jocelyn Samuels to remark: "We continue to see a lack of comprehensive and enterprise-wide risk analysis and risk management that leads to major breaches and other compliance problems."

Five years later, there is now sufficient breach data available that assessing the likelihood of a breach is no longer a purely qualitative exercise: there are solid statistics to help rank risks. For example, statistics from the large breach reports posted on the HHS website show high likelihood that PHI will be compromised due to lost or stolen unencrypted devices, untrained workforce members, or inadequate policies and procedures. In place of the "Security Readiness Scale", the PHIve process can be simplified by using a 1–5 rating for the likelihood and impact of a breach for each PHI home.

Rating	Likelihood	Impact
0	Not Applicable	Not Applicable
1	Rare	Insignificant
2	Unlikely	Minor
3	Moderate	Moderate
4	Likely	Major
5	Almost Certain	Severe

The overall risk score would be calculated by multiplying the Likelihood rating and the Impact rating. The Impact can be developed based on the amount and type of information that is contained in the asset at risk, using the cost model in the original report.[97]

Risk response can include: Accept, Avoid, Mitigate or Transfer, but the organization should agree on a risk tolerance level above which a risk will not be Accepted. Such a score, for example, might be 15, which would be represented by ratings of (a) 4*4 or (b) 3*5 or higher.

Documentation of the organization's risk response plan and progress should be used to report progress to a Governance Committee or Oversight Council and maintained to help prove due diligence in case of a breach.

chapter eight: a case study

Calculating the Cost of a PHI Breach using Phive

Following the publication of *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security,* Grace Crickette, one of the authors, put the framework and assessment tool to work. As Chief Risk Officer for the University of California at the time, Grace worked with a cross-functional team at the University to build a compelling case for investment in information security. Following the process outlined in the paper regarding Protected Health Information Value Estimator (PHIve), Grace and her team automated the 5-step process to:

1. Identify all information assets and assess the risks to those assets
2. Determine a security readiness score based on the likelihood of a threat exploiting a vulnerability of that asset
3. Determine the relevance of various costs that could be associated with a breach of that information
4. Calculate the total cost of a breach
5. Determine a return-on-investment (ROI) for investing in stronger controls for those most vulnerable assets

The assessment results created an opportunity for a dialogue between the risk management functions, the established business risk team, and the nascent IT cyber security risk function.

Highlights of the resulting targeted IT investments included:

- Development and rollout in 2013 of the PHIve tool that increased understanding of the financial impact of a PHI breach and provided a process for evaluating and recommending the appropriate investments necessary to mitigate the risk of a data breach. This methodology has continued to help reduce potential financial exposure while strengthening the organization's reputation as a protector of the PHI entrusted to its care.
- Several sessions were added to the organization's 2013 Risk Summit on this area of risk, including a general session on "Institutional Framework for Privacy and Infor-

mation Security" presented by Kent Wada, Director of Strategic IT Policy and Chief Privacy Officer at UCLA, and a workgroup session of the IT Security Council.[98]

- The Information Security Awareness Training Program was launched at seven campuses and the Office of the President, with incentive programs supported by the Office for the Protection of Research Subjects (OPRS).
- As the University has moved to a shared services model for administrative systems, such as the UCPath payroll personnel system/human resources information system, security and privacy activities are integrated from the very start of the process when developing and deploying these types of services.
- More risk analysis activities are being completed on data centers, campus and other vendors, and the team is developing standard language for cloud computing contracts.

Conclusion

There have been many changes in the protection of health information since the 2012 report was written, but never has it been more critical that organizations protect the information with which they are entrusted. Costs have increased in every category: Reputational, Financial, Legal and Regulatory, Operational, and Clinical.

In the end, however, recovery from reputational damage of a data breach, the top-ranked risk in the Aon Survey, should not be underestimated. The bottom line, as always, is the investment in the solution. The Cost of a Data Breach model outlined in the original report, *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security*, remains as relevant today as when it was published in 2012.

And there are greater challenges ahead. According to Beckers Hospital Review:[99]

- The majority of healthcare data—80 percent—will pass through the cloud by 2020, as providers increasingly use the cloud for data collection, aggregation, analytics and decision-making.
- Sixty-five percent of healthcare interactions are predicted to be mobile by 2018.
- Seven out of 10 healthcare organizations worldwide will invest in consumer-facing apps, technologies, wearables, and virtual care by 2018 to reduce costs associated with managing chronic conditions.
- As big data becomes more integrated and utilized, the need for special IT support for big data may diminish by 2018, as more than 50 percent of what are currently deemed to be big data issues become operational IT issues.
- As outsourcing increases, more than half of providers will demand increased risk sharing from service providers by 2018, highlighting the vendors' growing role in the delivery process.
- Big data will continue to generate new information, but 42 percent of the data will remain unprotected by 2020.

In the end, the reaction to harm to individuals resulting from healthcare data breaches will be what drives healthcare's new reality for protecting information. Healthcare organizations and their service providers must increase their investment in information risk management and understand that not doing so simply isn't an acceptable business practice.

Contributors

Mary A. Chaput is Chief Financial Officer at Clearwater Compliance, LLC. Her extensive business and finance background spans several industries, including pharmaceuticals, health care/clinical trials and venture capital consulting. She has held senior-level financial positions with companies such as General Electric, Pharmaco International and ClinTrials Research. She is regarded as one of the country's foremost privacy experts for her knowledge of and practices implemented to comply with PHI privacy and security regulations.

Grace Crickette is SVP, Chief Risk & Compliance Officer, AAA Northern California, Nevada and Utah. Prior to coming to AAA NCNU, she served as the University of California's chief risk officer. She received the Information Security Executive (ISE) of the Decade Award in 2012 for her work there, developing a program that will drive improvement and best practices into the future. She has consulted with numerous public and private entities on the implementation of ERM, including Harvard University and SingHealth, Singapore's largest healthcare group.

Keith Fricke is a Partner and Principal Consultant for tw-Security, a firm specializing in healthcare information security. Previously, he was the Chief Information Security Officer for five and a half years at Mercy Health, the largest not-for-profit hospital system in Ohio. Keith has 30+ years of IT experience, the last 18 of which focused on Information Security. He frequently speaks at national, state, and local security events. He has been CISSP certified since 2002. He is a Board member of the Cleveland InfraGard Chapter. He is also an adjunct professor at Ursuline College where he teaches in their graduate MBA program.

Ben Goodman, CRISC is the recipient of ISACA's CRISC, Worldwide Achievement Award. He is the founder of 4A Security and Compliance, a firm that helps clients strengthen their information security while managing cyber risk and meeting their compliance requirements. With over 25 years of experience in information technology, technology strategy, and risk management, he is dedicated to strengthening the cyber defenses and resiliency of US organiza-

tions, institutions, and critical infrastructure. He is a faculty member at Drexel LeBow, recipient of ISACA's CRISC Worldwide Achievement Award, and a Fellow of the Ponemon Institute.

Rick Kam is president and co-founder of ID Experts. Rick is an expert in privacy and information security, with extensive experience leading organizations to address the growing problem of protecting PHI/PII and remediating privacy incidents, identity theft, and medical identity theft. With over 30 years of experience in the technology industry, Rick leads and participates in several cross-industry data privacy groups, speaks at conferences and webinars, and regularly contributes articles to industry and business publications.

Anita Osterhaug is President of Communications Associates, Inc., a technology marketing and training company that helps clients show their thought leadership in creating better solutions for business and society. Her work has appeared in numerous books and industry publications. She has been writing, producing multi-media content, and publishing about technology and data security for thirty years, and she is as passionate about security and privacy today as the day she started.

Dr. Larry Ponemon is the Chairman and Founder of the Ponemon Institute, a research "think tank" dedicated to advancing privacy, data protection and information security practices. Dr. Ponemon is considered a pioneer in privacy auditing and the Responsible Information Management (RIM) framework. Security Magazine named him one of the "Most Influential People for Security."

Robert Pruter, Executive Vice President, Sales & Marketing at SPHER, has spent the last six years helping hospitals and providers with cybersecurity and identity management solutions and has over 20 years of experience in the healthcare information technology (HIT) space. Prior to SPHER, Robert held senior level executive positions at INFOR, AGFA Healthcare, and Merge Technologies.

Raymond Ribble is President of SPHER, Inc. With over 25 years of delivering leading edge technology solutions in Healthcare Security, Aerospace, and Financial Systems, Ray brings a unique dynamic to SPHER Inc and the privacy and security sector. Prior to launching SPHER, a leading breach detection solution, Ray oversaw healthcare consulting and IT delivery to 2000+ Meaningful Use attestations as a Certified Service Partner within the HITECH Program across Southern California.

Kimberly Shutters, BCS, founder and CEO of HIPAA alli, has over 25 plus years in the healthcare industry working in Primary Care, Internal Medicine, Cardiology, Urology, and Otolaryngology practices. Her experience includes 10 years in the biotech industry developing and implementing solutions, improving processes as a Software Verification and Validation Engineer. This required creating software policies, procedures, and processes, risk analysis and risk management reports and other essential documentation necessary for submission to the FDA, CDRH, and CBER divisions.

Edward L. Stull is Executive Vice President and CTO/ Co-Founder at MiddleGate, Inc. He has over 5 decades experience in the U.S. Air Force, government and industry, including 35 years as a national and international standards award-winning chair; board member and executive, project and site manager. He specializes in machine and artificial intelligence for the development of large-scale open distributed processing technology plus command and control systems for healthcare, financial services and insurance. He is also active in promoting the performing arts at the Kennedy Center.

Sponsors

4A Security & Compliance has a proven track record of helping organizations in health care and other highly regulated industries secure sensitive data and meet information security, risk management and compliance requirements.

Why call 4A Security & Compliance?

- Because we've helped health care organizations respond to reportable PHI breaches so that OCR closed the cases with no fines, penalties or follow-up audits.
- Because we've delivered rapid HIPAA compliance support, helping organizations stand up robust security and privacy programs from scratch in just a few months.
- Because our clients have told us that when our team conducts a HIPAA risk analyses, they are empowered by all the practical insight we provide.

For more information, info@4asecurity.com

Communications Associates, Inc., specializes in content marketing that gets to the heart of your story and your expertise. We start with content strategy to deliver the results you want, then develop print, online, and multi-media content that shines a spotlight on your thought leadership. With decades of experience in communications and computing technology and data privacy, we're uniquely qualified to help your customers, partners, and investors understand the value you offer.

For more information, osterhaug@att.net

Clearwater Compliance, LLC is a leading provider of hospital and health system compliance and cybersecurity management solutions. Its mission is to empower hospitals and health systems to successfully manage healthcare's evolving cybersecurity risks and ensure patient safety. Exclusively endorsed by the American Hospital Association, Clearwater solutions have been deployed within hundreds of hospitals and health systems, Fortune 100 organizations and federal government institutions. More information about Clearwater Compliance is at http://www.clearwatercompliance.com

Epiq provides unmatched expertise in responding to and remediating all types of cyber incidents. Our solutions range from precision mailings to dedicated contact centers and strategic communications to minimize or eliminate the impact of an identity theft incident. Should a data breach result in a negotiated settlement, we work closely with you to develop legal notice plans, facilitate claims review and processing, and ensure that class members receive appropriate remedies. www.epiqsystems.com

For more than three decades, GCG has been the premier provider for class action settlement administrations, restructuring and bankruptcy matters, mass tort settlement programs, regulatory settlements, and data breach response programs. GCG provides industry leading reorganization services including services relating to chapter 7 liquidations, chapter 9 restructurings, chapter 11 reorganizations, chapter 15 cross-border proceedings, Creditors' Committee assistance, and out-of-court restructurings and corporate events. GCG is a subsidiary of Crawford & Company. www.gardencitygroup.com

ID Experts is a recognized market leader for breach response services and innovative, patent-pending identity monitoring products and solutions serving millions of Americans today. Rated A+ by the Better Business Bureau for over 10 years, ID Experts' award-winning team takes pride in providing superior breach response service and a superior customer care experience. After the largest breach in U.S. history, the federal government chose ID Experts to manage the response and provide identity protection to over 21 million Americans. www2.idexpertscorp.com

The Lewis Brisbois team, led by a former federal cyber attorney, has extensive experience managing responses to information security incidents. Their rapid response service includes access to a 24/7 data breach hotline, geographically distributed teams in every time zone, and complete project management of the breach response process. They work closely with cyber insurance brokers and carriers to maximize client access to resources, including facilitation of all services to contain, investigate and remediate the incident.

MacKenzie+ is a full-service marketing, research, and communications agency located in Portland, Oregon. MacKenzie+ has been in business for more than 13 years working with government, corporate and nonprofit clients – providing services in market research and strategic planning, digital and brand strategy, public/media/crisis communications, reputation management, and program management. MacKenzie+ is comprised of experienced senior strategists, innovative creative, and outcome-focused personnel that deliver a range of marketing capabilities for superior, cost-effective results. www.mackenzieplus.com

MiddleGate

With its product Grace™ already deployed to well over 200 provider locations, MiddleGate has applied advanced AI techniques and built a distributed machine intelligence focused on Medical Billing's oldest and biggest problem: some 20% of medical claims are underpaid, denied or rejected leaving providers with crippling recovery and write-offs costs. Grace skips industry dashboards and jumps straight to answers with Grace enunciating or taking actions as needed – all this while speeding payment cycles and removing needs for costly human intervention. https://www.middlegateinc.com/technology

PROTENUS

Protenus uses advanced analytics to detect and thwart insider threats in electronic medical records. Protenus detects when employees or hospital affiliates look at patient records inappropriately, doing so without the voluminous false positives that plague other privacy auditing systems through the use of expert systems, statistical inference, and machine learning. The Protenus system also provides an easy-to-use interface for forensic investigations, allowing compliance officers to resolve more cases in less time, with all the information they need at their fingertips. https://www.protenus.com

SPHER

SPHER™ is the frontline defense against the day-to-day threat of patient privacy violations resulting from inappropriate access to Patient Health Information (PHI). As required by HIPAA, under MACRA and by every cyber-security insurance clause: Comprehensive security compliance strategies must include User Activity Monitoring, a requirement that SPHER is specifically designed to achieve. SPHER monitors ALL of the daily activity that occurs within an EMR/EHR for suspicious behavior through the analysis of system audit logs.

Symantec Corporation, the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Symantec operates one of the world's largest civilian intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com/healthcare.

Notes

1. The 2012 ANSI/SFG/ISA report is available for downloaded at https://webstore.ansi.org/phi/. ANSI, SFG, and ISA were not involved in the preparation of this update to that report though some of the same industry volunteers were involved in authoring both documents.
2. https://webstore.ansi.org/phi/?gclid=CLnY04_T0dMCFQx7fgod3PEGeA
3. https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php#appendix
4. https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf
5. https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-interoperability-2015.php
6. https://www.healthit.gov/sites/default/files/briefs/oncdatabrief28_certified_vs_basic.pdf
7. http://www.beckershospitalreview.com/healthcare-information-technology/physician-ehr-adoption-update-7-statistics.html
8. https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf
9. https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-interoperability-2015.php
10. The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security
11. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
12. http://www.gartner.com/newsroom/id/3165317
13. Federal Register; https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
14. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/
15. https://www.federalregister.gov/documents/2017/01/18/2017-00614/department-of-labor-federal-civil-penalties-inflation-adjustment-act-annual-adjustments-for-2017
16. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html?language=es
17. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/pilot-program/index.html
18. https://iapp.org/media/presentations/13Summit/S13_Lessons_Learned_OCR_PPT.pdf
19. OCR Launches Phase 2 of HIPAA Audit Program; https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html
20. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html?language=es
21. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/
22. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm
23. https://www.hrsa.gov/hr/cybersecurity-2015-06-update.html

24. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/semc/index.html

25. https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

26. https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

27. https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

28. https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

29. https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

30. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/index.html

31. The New Mexico citation is still awaiting signature by the Governor but will go into effect immediately upon signing. It requires notification within 45 days, reporting to AG for breaches impacting over 1000 individuals. This law does have a HIPAA exemption, which allows HIPAA covered entities acting under the requirements of HIPAA to be deemed in compliance with the requirements in the State law.

32. http://money.cnn.com/2010/01/13/news/economy/health_care_fraud/

33. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

34. http://www.eweek.com/news/utah-health-care-data-breach-exposed-about-780-000-patient-files

35. http://www.modernhealthcare.com/article/20160809/NEWS/160809906

36. https://www.wsj.com/articles/newkirk-products-reports-data-breach-1470437381

37. https://www.databreaches.net/21st-century-oncology-notifies-patients-of-data-security-incident/

38. https://www.linkedin.com/in/angela-mckay-35b98b59

39. https://media.scmagazine.com/documents/232/sixth_annual_benchmark_study_o_57783.pdf

40. http://lpa.idexpertscorp.com/acton/attachment/6200/f-04aa/1/-/-/-/-/Resources%20-%20Sixth%20Annual%20Benchmark%20Study%20on%20Privacy%20and%20Security%20of%20Healthcare%20Data%20.pdf

41. https://www.ropesgray.com/newsroom/alerts/2016/September/Small-Breach-Focus-Shows-Growing-Scope-Of-HIPAA-Probes.aspx

42. http://www.agg.com/Heighten-Importance-for-March-1-2017-HIPAA-Small-Breach-Reporting-Deadline-01-30-2017/

43. Ibid.

44. http://athensorthopedicclinic.com/important-news-for-patients/

45. http://www.healthcareitnews.com/news/dark-overlords-offer-500-patient-records-stolen-athens-orthopedic-clinic-black-market

46. Statistic presented by FBI at two 2016 events: PPN 2016 conference in Philadelphia and again at a Los Angeles Chamber of Commerce presentation.

47. The Dark Web consists of hidden websites and services that are only accessible via anonymous browsers such as Tor and I2P

48. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup

49. http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet

50. HIMSS Analytics. The Healthcare Information and Management Systems Society. "2016 Telemedicine Study." April, 2016.

51. http://www.pwc.com/us/en/health-industries/top-health-industry-issues/assets/2016-us-hri-top-issues.pdf

52. http://www.mobihealthnews.com/32232/in-depth-mobile-adoption-among-us-physicians

53. http://www.securityweek.com/mobile-malware-shows-rapid-growth-volume-and-sophistication

54. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

55. Homeland Security Office of Cyber and Infrastructure Analysis. "Risks to Critical Infrastructure that Use Cloud Services." March 2017.

56. Shadow IT is defined as "people installing and using their own, non-company-sanctioned apps and software at work." http://itbizadvisor.com/2016/08/shedding-light-on-shadow-it/

57. https://www.ciphercloud.com/resources/shadow-it-management-guide/

58. Ibid.

59. http://blogs.cisco.com/cloud/gartner-report-says-shadow-it-will-result-in-13-of-security-breaches

60. § 164.502 (1)(e)(1)(i) Standard: Disclosures to business associates.

61. Ibid.

62. https://www.hhs.gov/hipaa/for-professionals/faq/business-associates

63. Ibid.

64. http://www.hhs.gov/hipaa/for-professionals/faq/2003/are-we-required-to-certify-our-organizations-compliance-with-the-standards/index.html

65. https://info.wombatsecurity.com/cost-of-phishing

66. https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html

67. FDA Issues Unprecedented Alert Over Medical Device Cyber Security Risk; https://www.swlaw.com/blog/product-liability-update/2015/08/17/fda-issues-unprecedented-alert-over-medical-device-cyber-security-risk/

68. Doctors Still In the Dark After Electronics Records Hack Exposes Data on 4 Million – posted July 31, 2015; https://securityledger.com/2015/07/doctors-still-in-the-dark-after-electronics-records-hack-exposes-data-on-4-million/

69. https://www.fda.gov/RegulatoryInformation/Guidances/ucm077812.htm; https://www.himssconference.org/sites/himssconference/files/pdf/20.pdf

70. Payment Card Industry Data Security Standard

71. Gramm-Leach-Bliley Act

72. Sarbanes–Oxley Act of 2002

73. Federal Trade Commission

74. http://lpa.idexpertscorp.com/acton/attachment/6200/f-04aa/1/-/-/-/-/Resources%20-%20Sixth%20Annual%20Benchmark%20Study%20on%20Privacy%20and%20Security%20of%20Healthcare%20Data%20.pdf

75. http://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=1

76. http://www.healthcareitnews.com/news/teaching-hospitals-are-prime-targets-data-breaches

