ISSA JOURNAL

September 2017
Volume 15 Issue 9

Table of Contents

DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Feature

Articles

Also in this Issue

The ISSA Journal (1949-0550) is published monthly by
Information Systems Security Association
11130 Sunrise Valley Drive, Suite 350, Reston, Virginia 20191
703.234.4095 (Direct) • +1 703.437.4377 (National/International)

From the President

Hello, ISSA Members and Friends

Keyaan Williams, International President

Remembering Houston

Houston, Texas, is the fourth largest city in the United States by population. The recent floods and devastation caused by Hurricane Harvey affect the life and livelihood of more than 2.3 million people in Houston, plus thousands of other people in communities throughout Southern Texas and Louisiana. People affected by this storm are putting aside their differences to support, care for, and even save each other.

I invite all ISSA members and the global information security community to remember the people affected by Harvey as you go about your daily business. All contributions to the relief are appreciated to help people put their lives back together. We should do whatever we can to help these communities recover from one of the worst natural disasters in US history. If you have the means and desire to contribute financially, the North American Mission Board and the Salvation Army give 100 percent of all donations raised to relief efforts. Please contribute how you can and remember Houston!

- North American Mission Board
- Salvation Army

Healthcare security

The September *ISSA Journal* focuses on healthcare security.

From the moment you are born, you are touched by a healthcare professional who "delivers medical care in a systematic way, following prescribed protocols and procedures."[1] These procedures have been refined over hundreds of years to ensure healthcare professionals leverage the best protocols and procedures to contribute to the well-being of their patients. Advances in technology have improved the delivery of healthcare services and medical procedures in hospitals. These advances have also created an explosion of health IT solutions that provide an array of technologies to store, share, and analyze health information.

The most prominent health IT solutions include electronic health records (EHRs), personal health records (PHRs), e-prescribing, personal health tools, and online communities. These solutions improve how doctors, health service providers, and individuals use health-related information to manage everything from general health to specific medical conditions. For example, sleep apnea patients can use modern continuous positive airway pressure (CPAP) machines that automatically regulate the air pressure that keeps a patient's airway open. The devices also provide real-time updates to a pulmonologist who can monitor information and trends to ensure the treatment is effective. Similar types of solutions improve the lifestyle and health monitoring of people with diabetes, heart conditions, and a host of other medical concerns.

The benefits of health IT solutions are not limited to people with health conditions. People who are generally in good health have numerous options for wearable devices that have the capability to track important fitness attributes and provide up-to-the-moment information about sleep patterns, heart rates, and general levels of fitness. Furthermore, these wearables support synchronization with a growing catalogue of personal health apps that combine the information to provide a general picture of a person's health.

Technology is critical for modern healthcare concerns, whether the concern is personal or related to delivery of services by healthcare professionals. This explosion of healthcare technology comes with risks that the healthcare industry, device manufacturers, and the security industry must work to address. Confidentiality, integrity, and availability are all valid concerns for healthcare technology. The requirements will vary depending on the context and use of technology; however, incorporating security engineering principles in the design of this technology is critical to ensure meaningful protection is provided and access is controlled for all the data produced by this technology.

Additional reading: https://www.healthit.gov/.

Every life is valuable and precious. The systems that support life and enrich it are critical to the health and welfare of society.

~Keyaan Williams

1 Ray, L. "What is a Healthcare Professional," Career Trend, July 5, 2017 – https://careertrend.com/facts-4885886-what-health-care-professional.html.

DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

ISSA
Information Systems Security Association

Information Systems Security Association
11130 Sunrise Valley Drive, Suite 350, Reston, Virginia 20191
703.234.4095 (Direct) • +1 703.437.4377 (National/International)

The Information Systems Security Association, Inc. (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer inte raction opportunities that enhance the knowledge, skill and professional growth of its members.

With active participation from individuals and chapters all over the world, the ISSA is the largest international, not-for-profit association specifically for security professionals. Members include practitioners at all levels of the security field in a broad range of industries, such as communications, education, healthcare, manufacturing, financial, and government.

The ISSA international board consists of some of the most influential people in the security industry. With an international communications network developed throughout the industry, the ISSA is focused on maintaining its position as the preeminent trusted global information security community.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved.

ISSA JOURNAL

Now Indexed with EBSCO

Editor: Thom Barrie
editor@issa.org

Advertising: vendor@issa.org

866 349 5818 +1 206 388 4584

Services Directory

Website
webmaster@issa.org

Chapter Relations
chapter@issa.org

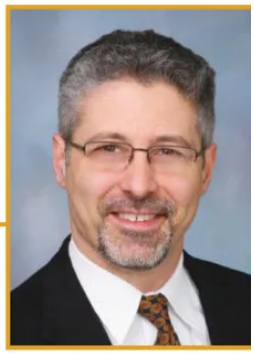
Member Relations
member@issa.org

Executive Director
execdir@issa.org

Advertising and Sponsorships
vendor@issa.org

Sabett's Brief

Healthcare and Infosec: Still a Work in Progress



By Randy V. Sabett – ISSA Senior Member, Northern Virginia Chapter

Earlier this year, I worked with a couple of my colleagues on a matter that involved researching the current state of affairs in healthcare cybersecurity. Many of the non-cybersecurity attorneys with whom I work tend to be optimists (at least when it comes to security), but they became more and more discouraged the deeper we dug. Here are just a few examples why.

Cyber attackers in the healthcare space resemble cyber attackers in any other space: they use a variety of attack vectors to inflict damage on their victims, including advance persistent threat (APT) attacks and distributed denial of service (DDoS) attacks. In "The State of Cybersecurity in Healthcare Organizations In 2016," the Ponemon Institute notes that APT attacks were reported to occur in healthcare organizations on average once every three months.

The Ponemon report found that DDoS attacks are common in the healthcare industry and cost companies an average of $1.32 million per incident. Further, in mid-2017, the United States Department of Health and Human Services (HHS) published reports of 1,857 breaches involving more than 500 patients per incident that involved more than 20 million patients overall.

One of the largest cyber attack incidents that has occurred in the healthcare industry involved Anthem, Inc. On February 4, 2015, Anthem announced a data breach involving the personal information of up to 80 million individuals resulting from a targeted cyber attack that compromised names, birth dates, SSNs, healthcare identification numbers, home addresses, and email addresses. The Anthem incident was the result of cyber attacks over the course of several weeks in late 2014 that the company did not detect until January of 2015.

Investigators now believe that the hackers responsible for the Anthem attack had access inside Anthem's corporate network for months. Access was gained via a phishing email to a company employee that allowed the hackers to gain administrator credentials, which then resulted in the loss of personal information of over 78 million customers dating back to 2004. But Anthem is not alone. In addition to the Anthem attack, Premera Blue Cross, Excellus Health Plan, and the University of California Los Angeles were all victims of hacking incidents involving health information.

Hackers aren't the only ones active in the healthcare space. The HHS Office of Civil Rights (OCR) has been actively enforcing the HIPAA security and privacy rules by either settling cases or fining entities that are in violation of the rules. Last year, HHS OCR received $23 million in payments to resolve potential noncompliance with HIPAA security and privacy rules. This was a 300 percent increase from the $7.4 million paid the prior year.

Last year also saw 13 enforcement actions, which almost doubled the number of the enforcement actions from the previous annual record of seven. In 2016, OCR also received its largest settlement to date from Advocate Health Care Network, which settled for $5.55 million for data breaches affecting the PHI of four million people.

OCR's enforcement activity produced two significant settlements in the first half of 2017, one from Memorial Healthcare Systems (MHS) and the other from Children's Medical Center of Dallas. MHS agreed to pay OCR $5.5 million for HIPAA violations resulting from unauthorized access to patient information by employees. OCR fined Children's Medical Center of Dallas $3.3 million due to failure to comply with HIPAA rules, resulting in data breaches of ePHI of over 6,000 individuals. OCR found that Children's Medical Center of Dallas failed "to implement risk management plans, contrary to prior external recommendations to do so, and [failed] to deploy encryption or an equivalent alternative measure on all of its laptops, work stations, mobile devices and removable storage media until April 9, 2013."

Many years ago a good friend of mine predicted that healthcare data would become the new target for attackers. Steve couldn't have been more right. As the old saying goes, however, hope springs eternal. Perhaps we will see tremendous strides in the healthcare space. Until then, I'm avoiding the emergency room at all costs (even though I did spend two days there over my vacation…don't ask, not a pleasant story).

About the Author

Randy V. Sabett, J.D., CISSP, is an attorney with Cooley LLP, a member of the advisory boards of MissionLink and the Georgetown Cybersecurity Law Institute, and is the former Senior VP of ISSA NOVA. He recently completed FBI Citizen Academy training and can be reached at http://rsabett@cooley.com.

Healthcare Is a Snowflake

By Branden R. Williams – ISSA Distinguished Fellow, North Texas Chapter

No industry is immune to cybersecurity threats, including health care. What makes health care unique is, unlike many other industries, loss of life is a real outcome that can happen from a cybersecurity incident. Be it from a poorly secured medical device that kills its host or a misplaced or altered digital medical record noting a drug allergy, security incidents in health care are scary.

Securing health care is challenging. Nobody wants to be open on the table when the surgeon realizes he forgot his authentication token to get access to your medical records. Conversely, when you are not on the operating table, you want your medical records to remain safe and secure.

Health care needs automated systems that follow around an individual, have constant and perfect authentication and authorization tools, and almost a dual administrative control where the patient is the ultimate grantor and the provider can see all that is relevant to them while they are providing a service. It's almost the equivalent of encasing a computer in a foot of concrete to secure it, yet providing an interface so that it is still usable: in other words, a modern cyber paradox.

Protecting health care goes beyond perfect authentication and authorization. It must include perfect patching and perfect maintenance. It's an impossible task, but one that impacts a provider's ability to save lives.

According to Verizon's *2017 Data Breach Investigations Report*, 72 percent of the malware incidents that affected health care in 2016 were ransomware related. In a number of cases, hospitals that suffered ransomware attacks simply paid the ransom to unlock the computers. WannaCry affected hospitals in the US and the UK, causing a major disruption in the UK. More than 15 British hospitals had to shut down as a result of the attack, severely impacting the National Health Service.

Medical technology is a contributor to this problem as well. Many advanced lab systems or treatments require computers to run. Those systems can be a major nightmare for information security teams to secure. We can only hope that systems running Windows or Linux are able to be updated, are hardened from within, and do not retain patient identifying records insecurely on their drives.

The reality is that ransomware often impacts the computers tied to labs and treatments because they are running outdated versions of Windows (perhaps, Windows XP?), and updates may break the software that is specific to the lab or treatment. Or, worse, updates simply cannot be applied because the system is not capable of receiving and applying them. If companies across the globe fell victim to the WannaCry ransomware as they struggled to keep their systems fully patched, how can an industry whose product may leverage outdated computing stand a chance?

Wearable medical devices are not immune either. If you have had a pacemaker installed in the last few years, there is a high probability that it communicates back to your doctor via wireless technology. That's the same way the doctor will adjust its settings as well. I certainly hope that medical device manufacturers advance their understanding of the cybersecurity threat well before one is implanted in me.

Other incidents reported by Verizon's DBIR for health care look more like just a bunch of accidents. Things like lost laptops, items mistakenly delivered to Jon Smith when they were supposed to be for John Smith, and medical files and artifacts ending up in landfills instead of the incinerator fall under that category. Technology is a great enabler for health care, but too much faith is put into the end technology by its operators. Doctors expect medical records on the go to provide top notch treatment, and they expect that the computer housing those records to defend itself against outside threats. Or, perhaps more accurately, they are ignorant to the threat that these devices must face from crimes of opportunity or passion. Unfortunately, technology is just not quite there yet. Thus, the flawed human is a big contributor to security issues in health care.

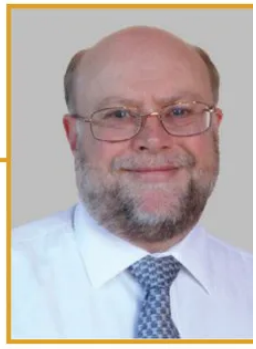
While health care might be a bit of a snowflake when it comes to information security, the solution is the same as every other industry: a top-down emphasis on information security being central to the overall operating model. Simply, build cybersecurity into everything you do. Each specific firm must understand what that means for them, how to align a security strategy with the corporate strategy, and manage the risk that cyber incidents bring to the firm.

About the Author

Branden R. Williams, DBA, CISSP, CISM, is a seasoned infosec and payments executive, ISSA Distinguished Fellow, and regularly assists top global firms with their information security and technology initiatives. Read his blog, buy his books, or reach him directly at http://www.brandenwilliams.com/.

Gray Hat

Trusted Systems in Health



By Mark Anderson – ISSA member, Australia Chapter

There are numerous examples of both security-critical and safety-critical systems related to health. It should be a no brainer to the ISSA membership that medical records attract very serious confidentiality, integrity, and availability requirements, as well as issues for embedded medical devices from heart pacemakers to drug delivery devices. Larger devices including radiation delivery machines typically now have significant software-based systems that can easily kill or maim if mishandled, thus requiring very high assurance levels when compared to the broader commercial world. Given this almost self-evident view, what could be emerging, strategic "gotcha" technologies that might be under the radar with respect to emerging health systems? I list two candidates: Formal Methods, and Machine Learning.

Our primary, very high assurance security- and safety-critical protocols are based on mathematical formal methods applied from a tightly constrained, explicit functional specification, which is itself encoded mathematically; and it's all about proving that a system will do what it is supposed to do and nothing else (think aviation integrity systems). We categorize these protocols and tools used under the heading of *Formal Methods*. Although some strides have been made in automation, the process is still very expensive to apply, especially if there is a short update cycle on code. It has languished for security systems and I recall ad hoc figures of around USD$450 per line of code from years gone by, so you really want to reduce the amount of code requiring verification.

DARPA has initiated some interesting fast formal-verification programs, but I wouldn't hold my breath that the increased size of the systems we now deal with normally will be able to cost effectively be treated on an industrial scale. Further, if you take today's devops cycle into account, the last thing you want is a constant update stream on code that must be formally verified. Traditionally, we concentrated the security-critical function into a small, formally verified "kernel" and thus limiting the exposed functionality of the system. Will this really work in future health with AI-based technologies? Even with the old Von Neumann code bases it didn't work too well in national security if the number of formally verified systems is anything to go by, and we all know it devolved to a "risk management" approach.

Further to the above, our extant logic-based techniques simply do not map directly to a machine-learned system such as a recurrent or convolutional neural network. What do you do verifying a neural network that a company shoved into a heart pacemaker? Don't worry about it since it was trained on millions of examples with a 99 percent statistical success rate? I don't think so; some readers may care to respond that driverless cars have the same issue. The best you can hope for is your own validation set, which can be used as a pseudo model checker deemed to be "proven" complete. Too bad if it misses critical examples.

Basically, with the race for AI into health our fundamental high-assurance technology toolbox for applying security- and safety-critical assurance to health is not even applicable to the emerging technologies, no matter how many dollars you place into the verification process. The math technology just isn't there. But I guess you can play a statistical game and go with a risk, that is, until you get sued; and it's a safe bet that people can be even more sensitive when it comes to malfunctioning medical devices as compared to deaths caused by malfunctioning cars in litigation.

In the same theme: it would be interesting indeed if your heart pacemaker became another device on the Internet of things and its software was updated on the fly by your doctor in a manner not unlike your iPhone or Android device with fantastic new convenience functions from the rapid cycle devops team, let alone considering hacking. Feeling comfortable?

I firmly believe that the majority would agree that good health care already "ain't cheap." Having a range of computerized systems making decisions on your health care, looking at records which might or might not affect your insurance and implantation of even more complex software-driven networked devices upon which your life may depend with safe operation is going to raise the assurance cost to a whole new level in the stratosphere. And yes, people will be looking to us to discover some magic bullet for detecting malware and just plain mistakes in technology types such as neural nets or machined-learned tensors with weight sets all at "everyday low prices" but with sequenced Von Neumann-style controls and outcomes on an asynchronous sigmoidal connectionist system. Good Luck, we are going to need it.

About the Author

Gray Hat is an ACM Distinguished Engineer and principal inventor for several patented devices and major systems for high-grade information security purposes. He can be contacted at http://msanderson@ieee.org.

Open Forum

The Open Forum is a vehicle for individuals to provide opinions or commentaries on infosec ideas, technologies, strategies, legislation, standards, and other topics of interest to the ISSA community. The views expressed in this column are the author's and do not reflect the position of the ISSA, the ISSA Journal, or the Editorial Advisory Board.

Don't Blame the Victims

By Karen Martin

Target's 2013 data breach exposed 70 million customer records! The Mirai botnet attack blocked access to Twitter, Spottify, and Reddit! WannaCry ransomware infected over 300,000 computers!

Every time a cyber attack makes headlines, we hear the same story—we must improve our defenses. *The Economist* magazine recently pointed out that technical solutions do not prevent all attacks and recommended that we turn to economic tools—regulations and standards, insurance policies, and liability laws—to give users an incentive to take security seriously.[1]

But those tools are already available, and attacks still succeed. If they are not working, perhaps they do not make economic sense. Users will only change their behavior if the proposed changes cost less than the problems they prevent, and that is not always the case.

Consider the Target data breach. Target was taking measures to protect customer data before the breach. They were certified as compliant with the PCI/DSS standard, a process that probably costs them millions of dollars a year. They were using antivirus software and a $16 million malware detection system. Yet attackers were still able to find a way into Target's network.

This incident cost Target roughly $200 million, but it is not clear that additional spending on security technologies would have prevented the attack or lowered the cost. Target was also able to absorb the loss—their stock price and sales recovered in less than a year. Can we blame them for making a trade off between defense costs and security risks?

Software development is a good example of cost and security trade offs. Errors in software can leave systems vulnerable to cyber attacks. It is possible to write nearly error-free software, but it cannot be done quickly or cheaply. The US space shuttle's software, for example, was extremely reliable, but cost the government 20 times more per line than average code,[2] and updates required 15 months of rigorous testing.[3]

There are few applications critical enough to justify that cost. Avionics, industrial control systems, and possibly automobile control systems may need expensive, reliable, extensively tested software. But should we expect businesses and consumers to pay for that level of reliability in laptops, cell phones, and Internet-connected appliances?

Research suggests[4] cybercrime's direct cost to society is relatively low, amounting to only a few dollars per citizen per year. How much are you willing to pay to avoid losing a few dollars a year? We may already be paying too much. The same research points out that we sometimes spend more on defense than the hackers are earning from their attacks. eBusinesses spent more than a billion dollars on anti-spam measures in 2010, while the botnet behind roughly one third of the spam probably only earned a few million dollars for its creators. Similarly, the recent WannaCry ransomware attack that apparently infected hundreds of thousands of computers had raised less than $100,000 during the window for victims to ransom their files.[5] It is too early to tell how much damage WanaCry caused, but damage recovery will certainly cost more than $100,000.

In the face of the significant imbalance between attackers' profits and defenders' costs, it might make more sense to try to change the attackers' behavior. Prosecuting hackers might be more cost-effective than almost all defensive technologies. But hackers often work from countries that shield them from prosecution for crimes against citizens of other countries, just as privateers were sheltered during the 17th century. It took decades for the then global powers to decide that piracy was costing them all too dearly and cooperate in hunting them down. Perhaps ransomware attacks will tip the balance in favor of more rigorous efforts to punish hackers, and the criminals will pay, instead of the victims.

About the Author

Karen Martin is a San Jose-based technical writer with extensive experience in information security. She may be reached at kjlmartin@gmail.com.

1 "Why Everything Is Hackable," The Economist, April 8th, 2017, pp 69-71 – https://www.economist.com/news/science-and-technology/21720268-consequences-pile-up-things-are-starting-improve-computer-security.

2 Jenkins, D. (2001, April 5). "Advanced Vehicle Automation and Computers Aboard the Shuttle," NASA. Retrieved May 21, 2017 from https://history.nasa.gov/sts1/pages/computer.html.

3 Dunbar, B. (2010, June 28). "Shuttle Computers Navigate Record of Reliability," NASA. Retrieved May 21, 2017, from https://www.nasa.gov/mission_pages/shuttle/flyout/flyfeature_shuttlecomputers.html.

4 Anderson, R., Barton, C., Bohme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., Savage, S. (n.d.). Measuring the Cost of Cybercrime. Retrieved May 21, 2017, from http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf.

5 Elliptic, "WannaCry": Elliptic Enterprises estimate of the amount paid to Bitcoin addresses designated to receive ransom payments as of 3:40 am UTC, May 21, 2017, Elliptic. retrieved from https://www.elliptic.co/wannacry/.

Perspective: Women in Security SIG

WIS SIG Mission: Connecting the World, One Cybersecurity Practitioner at a Time

Minimizing Risk in an Ever-Increasing Connected Health World

By Rhonda Farrell – ISSA Fellow, Central Maryland, National Capital, Northern Virginia Chapters

Nowhere is the threat to life higher than within the cybersecurity realm associated with the healthcare sector. The recently released 2017 *Report on Improving Cybersecurity in the Health Care Industry* outlines the security and privacy problem space, offers an historic view on cybersecurity, characterizes risks into six major areas, bucketizes remediation recommendations and actions into six major imperative areas, and offers a unique opportunity for deployment of a wide spectrum of information and service offerings geared towards this specialized industry population.

Snippets of the report focus area follow, to guide the readers to where the greatest opportunity space may be from an awareness, knowledge transfer, and service delivery perspective, with the intent that the analysis provided by the report would allow our SIGs, chapters, and community members to better serve this valued industry segment.

Problem space

Elements that exacerbate the cybersecurity attack and threat landscape include the rapid deployment of technology within the sector, the heightened severity of attacks in recent years, and the exponentially increasing amounts of automation supporting medication delivery systems as well as the volume of connected medical devices. Additional issues include lack of clarity on the chain of command governing preparation and response; incohesive industry oversight and knowledge sharing; obstacles to leveraging relevant standards and regulations; legacy system resiliency; small and rural organizational cybersecurity challenges; supply chain induced problems, as well as inconsistent data digitization and supporting access protections.

Lastly, unique culture characteristics pose significant security and privacy issues, including breadth of stakeholders, consumers, and touch points in the health-service delivery life cycle; longer access to potential unsupervised and unlocked IT devices given urgency of staff calls to action; continuous availability of operational infrastructures and locations; sheer number of non-known or identifiable persons traversing these organization's locations; as well as the constant rotation of staff and volunteers with different levels of security awareness and operational security training.

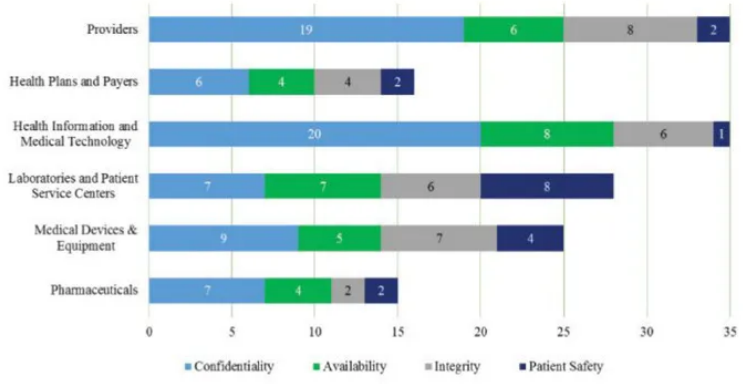


Figure 1 – Healthcare subsector risks across the value chain

Cybersecurity historic view

The report findings indicate that current organizational culture does not understand, support, or adequately fund cybersecurity programs or related technologies, and oversight and policy gaps between industry players are numerous and problematic.

Categorized risk areas

The report collected and categorized 151 potential risks across the value chain: 68 confidentiality, 34 availability, 33 integrity, and 19 were patient safety oriented, as indicated in figure 1. Fifty-five percent of the risks are related to protected health information (PHI).

Recommendations and action buckets

Lastly, the report organized the set of corresponding recommendations and follow-up action items into six high-level imperative buckets, per table 1 (page 31).

Given the complexity, risk, and broad scope of these findings, the associated recommendations and follow-up actions seem to be perfect fodder for our ISSA International Global SIGs (Health care especially) to further explore. In particular, the report's collection and distribution of documented cybersecurity best practices from other critical infrastructure sectors would certainly bear examination for applicability and prioritization towards achieving remediation-oriented action within the healthcare sector.

Continued on page 31

News That You Can Use…

Compiled by Joel Weise — ISSA Distinguished Fellow, Vancouver, BC, Chapter and
Kris Tanaka — ISSA member, Portland Chapter

Commentary: Why Information Security Is a Patient Safety Issue

http://www.healthcareitnews.com/blog/commentary-why-information-security-patient-safety-issue

Although this is an industry-focused blog with a lot of "motherhood and apple pie," it is useful none the less. If you have been in the information security business, even for a little while, you will recognize a number of areas that you would assume have already been addressed. Surprisingly, according to the blog, we're not there yet. For example, "Without having experienced a costly breach…the value of robust security practices was often hard to even articulate…Many security professionals and organizations have difficulty demonstrating the importance of cyber..." Really?

St. Jude Pacemaker Gets Firmware Update 'Intended as a Recall'

https://www.darkreading.com/iot/st-jude-pacemaker-gets-firmware-update-intended-as-a-recall-/d/d-id/1329769

Faulty car parts, contaminated food, unsafe toys. These are some of the things that frequently receive recall notices. Now we can add IoT medical devices, like the STM pacemaker, to the list. Although it is comforting to hear that there is now an FDA-approved fix for the vulnerabilities that were discovered last year, it is also a little nerve-racking to think what might happen if you don't get the update. After all, you can't just toss out your pacemaker like you would bad food.

IoT Medical Devices a Major Security Worry in Health Care, Survey Shows

https://www.darkreading.com/threat-intelligence/iot-medical-devices-a-major-security-worry-in-healthcare-survey-shows/d/d-id/1329631?

Well, if this isn't troubling, I don't know what is. Information security in health care is tough enough, but I think the intersection of IoT and health care is one area that needs more emphasis. One statement that really stands out is worth repeating: "Medical devices present several security challenges to the industry. Manufacturers can be slow to provide patches…Security basics are frequently overlooked: it's not uncommon to find medical devices using obsolete operating systems like Windows XP, insecure protocols, and simple passwords."

Feds Demand Data on Visitors to Anti-Trump Protest Site

https://www.cnet.com/news/feds-demand-data-on-visitors-to-anti-trump-protest-site-inauguration-riots/

This is scary. People who clearly incite violence or rioting should be prosecuted whenever possible. However, are the data demands from the Justice Department going a little bit too far? Furthermore, how will that information be handled? It's a slippery slope. Food for thought.

Faulty Firmware Auto-Update Breaks Hundreds of "Smart Locks"

http://thehackernews.com/2017/08/firmware-smart-locks.html

You knew this was going to happen. Here is a perfect example why we need to change control and quality assurance for IoT devices. Not that 500 is a big number, but this certainly demonstrates how easy it is to muck up IoT technology.

Uber Settles US Allegations over Data Privacy

https://www.reuters.com/article/us-uber-usa-idUSKCN1AV1VB

Being a privacy freak, I am appalled whenever I see a big, well-known company breached. I know there are a lot of smart people at Uber so I would ask "How is this even possible?" According to this article, Uber "failed to protect the personal information of drivers and passengers and deceived the public about efforts to prevent snooping by its employees." The FTC even stated that Uber "did not take reasonable, low-cost measures that could have…prevent[ed] the breach."

After Hackers Leak Game of Thrones Script, HBO Reportedly Offers $250,000 As "Bug Bounty"

http://www.thenewsminute.com/article/after-hackers-leak-game-thrones-script-hbo-reportedly-offers-250000-bug-bounty-66740

With a bug bounty set at $250,000 (wow), I'm not sure if HBO is looking for more trouble or if this is an extortion payment. Money like that could incent hackers to really start digging. This will not end well.

Identity Thieves Hijack Cellphone Accounts to Go after Virtual Currency

https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html?hp&action=-click&pgtype=Homepage&clickSource=story-heading&module=second-column-region&region=top-news&WT.nav=top-news

We all know that we need to protect sensitive information like our account numbers and our passwords, but now it appears that we need to be careful of who has our cellphone numbers. Companies had good intentions when they incorporated phone numbers into their multifactor authentication processes. However, as this article shows, hackers are turning that security piece into a potential access point in order to steal your data and your money.

Letters

To the Editor

I want to post a complement on the August Journal*...there are some well-written articles on two topics that I follow.*

Blockchain (distributed ledger):

"Blockchain: Considerations for Infosec," by Gerry McGreevy and "Crypto Corner: Blockchain Versus the GDPR," by Luther Martin

The McGreevy article is a nice infosec overview. My only complaint would be under his "availability" section; it does not flag the performance problem. Bitcoin is a very tiny data packet, but each transaction adds cryptographic history to the point where a transaction now takes four minutes. Imagine the processing load of a financial balance sheet or a personal medical history after a few years of transactions. There may be new algorithms (like Iota tangle) that may fix the performance problem, but they are a long way off.

The Martin article provides a "wow" moment. I had not considered that a regulation that enforces "confidentiality" may mean "no" to distributed ledgers. The rule that errors or expunged details must be erased is incompatible with a blockchain.

Internet of things:

"Battening Down for the Rising Tide of IoT Risks," by Anthony J. Ferrante

This was a good introduction for infosec folks. IoT is a rapidly evolving threat with an exponential growth in the number of cheap, very capable devices. I do have trouble with the suggestion that we can apply standard security practices.

The standard approach begins any assessment of a threat surface by gathering an inventory of devices on the surface and developing a plan to monitor and maintain each. In the past all the devices (mainframes, servers, PCs) were company owned, and you could read company POs to create a spreadsheet. We gave in a little with cell phones and allowed "bring your own device," but there was a formal registration process.

With IoT, devices on the threat surface show up without warning. They appear as Internet-connected appliances in the lunch room, toys on staff desks, and an M2M network that manages the HVAC and office environment. We can no longer get an inventory for the attack surface. A basic engineering principle is "you cannot control what you cannot measure," and by that definition IoT will always be "out of control."

To get more specific: any device with gesture and voice control has a camera and a microphone and is spyware. That $5 air freshener in the conference room that puts out a puff of perfume with a Harry Potter wave or an "Alexa please..." is a surveillance device. No one budgeted for it,; your infosec staff does not know it exists; and it will leak company plans.

Infosec will need to come up with a reactive surveillance approach to IoT threats. That new standard will be radically different to the change control and patch management practices we grew up with.

~Dean Styles
Vancouver, BC, Chapter

Association News

ISSA
SPECIAL INTEREST GROUPS

Special Interest Group Webinars

Want to hear more from ISSA's Special Interest Groups? Join free.

SIM 2017 Cybersecurity Virtual Summit
9/28/2017; 11 AM to 5 PM EST: Cybersecurity Uncertainty 2018 & Beyond–Moving from Defense to Building Resilience

Financial SIG
9/15/2017; Noon to 2:00 PM EST: NIST & Other Regulations

Health SIG
9/14/2017: Noon to 1 PM EST: Collaboration to Achieve Medical Device Security

Women in Security
9/11/2017: 4-5 PM EST: Mentoring Success around the Globe Series - Part III
9/14/2017: Denver, Colorado: 5-7 PM MST: Denver ISSA Women in Security SIG - September Meeting
9/20/2017: 4-5 PM EST: 2017 Leadership Meeting

On-demand Webinars
ISSA SIG web conferences bring together ISSA SIG members from around the world to share leading industry presentations and answer members' questions. Each SIG event is designed to address the timely needs of our SIG members through a live, online event and a subsequent recorded version for on-demand viewing.

2nd Annual Global Research Survey

ISSA and Enterprise Strategy Group have joined forces again to launch the second annual "Global Research Survey," which provides the collective voice of cybersecurity professionals. This ground-breaking research survey gained enormous media attention in 2016 because of the value placed on qualified responses from individuals who are experienced cybersecurity professionals – You, our ISSA members.

Based on your feedback, this year's survey has been streamlined and will be easier and faster to complete. Please join your 10,000 ISSA colleagues from around the world to have the voice of the profession heard and ensure your perspectives are earmarked for further development and analysis.

We invite you to participate in the research survey. We look forward to sharing the results with you this fall, at which time you will have an opportunity to receive a copy of the report.

Click here to complete the survey.

Don't miss this opportunity to contribute to the future of the profession. Join us and have your voice heard! All responses are completely confidential and only aggregate findings will be shared.

2016 Survey Results

PART I: The State of Cyber Security Professional Careers

PART II: Through the Eyes of Cyber Security Professionals

CSCL Pre-Professional Virtual Meet-Ups

So, you think you want to work in cybersecurity? Not sure which way to go? Not sure if you're doing all you need to do to be successful? Check out Pre-Professional Virtual Meet-Ups to help guide you through the maze of cybersecurity.

September 21, 2017: 11:00 am–12:30 pm ET. **A Day in the Life of an Ethical Hacker**

Everybody wants to be an ethical hacker. Find out what it is really like – the pitfalls and the glory. It's not as easy as you'd think!

Upcoming virtual meet-up:

- October 30, 2017: **Success Stories from former Pre-Professionals**

Don't miss out on the 20+ archived meet-ups:

ISSA.org => Learn => Web Events => CSCL Meet-Ups

ISSA
CISO FORUM

ISSA.org => Learn => CISO Executive Forum

The CISO Executive Forum is a peer-to-peer event. The unique strength of this event is that members can feel free to share concerns, successes, and feedback in a peer-only environment. Membership is invitation only, subject to approval.

San Diego, CA – October 11-12, 2017
Payment Strategies: The Game Has Changed

For information on sponsorship opportunities, contact Monique dela Cruz mdelacruz@issa.org.

ISSA CISO Virtual Mentoring Series

LEARN FROM THE EXPERTS! If you're seeking a career in cybersecurity and are on the path to becoming a CISO, check out the following webinar or view the 25+ archived presentations.

September 14, 1:00 PM - 2:00 PM EST: Health Care Needs Your Help! How to Become the Next Security Leader or Information Security Officer.

Our CISO executives will help you envision the security enterprise leader of tomorrow and the path it takes to reach that pinnacle. This will guide CISO up-and-comers in what it takes to land this role, what the CISO of the future looks like, and steps you can take to build a CISO career.

ISSA
CAREER CENTER

The ISSA Career Center offers a listing of current job openings in the infosec, assurance, privacy, and risk fields. There are currently 1073 job listings [9/3/17].

Visit the ISSA Career Center today.

ISSA International Web
CONFERENCE

Mobile App Security

2-Hour Live Event: Tuesday, September 26, 2017
9 a.m. US-Pacific / 12 noon US-Eastern / 5 p.m. London

Along with the explosion of mobile devices and the crowded marketplace for applications comes a vast threat landscape. How can security adapt to an environment teeming with independent programmers and time-critical business models as groups look for the next killer app? Especially when security is the last consideration of development.

CLICK HERE TO REGISTER.
For more info on this or other webinars: Click here.

THE EAB CORNER

ISSA Journal Scholastic Writing Award for Best Student Article

The ISSA Journal Editorial Advisory Board is announcing its annual ISSA Journal Scholastic Award for the best article submitted by a current university student.

The submission period is now open and the board will accept articles until October 1, 2017. We encourage students to follow the published editorial calendar but will consider any submission that is focused on information security.

The board will select the best article that meets our professional standards for publication and will feature it in the January 2018 "Best Of 2017" issue of the *ISSA Journal*. Recipient must be attending an accredited college or university full time and actively pursuing a degree. Submit your article and application to editor@issa.org by October 1, 2017.

Click here for more information. Questions can be directed to editor@issa.org.

ISSA Partners with ASIS 2017

ISSA and ASIS International (ASIS), the leading association for security management professionals, have formed an event partnership that will advance our shared missions—to heighten the knowledge, skills, and professional growth of security professionals across the globe.

For 2017, ISSA will be fully integrated into all facets of ASIS International 63rd Annual Seminar and Exhibits (ASIS 2017), convening September 25-28 in Dallas, Texas.

ASIS 2017 ISSA Member Discounts
Full: $225 off–IS17FULL; Single Day: $145 off–IS17SING

Learn more about the event at securityexpo.asisonline.org and use the codes above to redeem your member discount.

Support ISSA Education Foundation Fundraisers that provide scholarships to the next generation of Cybersecurity professionals

ISSA EDUCATION FOUNDATION
www.ISSAEF.org

A Donation of $5 enters you in our drawing for an Amazon Echo, a SANS course, a RING Doorbell Camera or a $100 Amazon gift card! Visit us at Booth #112

Access Control Capabilities and Healthcare Informatics Needs

By Marcelo Carvalho – ISSA member, Brasil Chapter

This article discusses access control in the healthcare environment. Role-based access control capabilities and examples of dynamic requirements for controlling electronic health record systems in the context of healthcare professional use are described.

Electronic health records (EHR) convey a set of health information on systems designed to assist healthcare practitioners. EHR systems hold records of various types including patient demographics, treatment behaviors and evolution, procedures performed, international classification of disease (ICD-10) diagnoses, laboratory tests, and other inputs. The required degree of health information and details needed to be registered may vary according to medical specialty or system purpose.

The patient is the sole owner of all this information; therefore, accessing it to deliver the required medical attention demands privacy boundaries to be established, defining who is allowed to see what EHR portion on the system. We must consider that the patient may be assisted by a number of professionals from different fields (nurses, physicians, surgeons, physical therapists, radiographers, radiotherapists, etc.). Also, the patient may not necessarily go to the same hospital or medical center, and hence the information is not only spread as chunks among various professionals' specific interfaces and containers but also divided among different users in different devices (mobile device, other systems…) and locations.

Nowadays, part of a patient's EHR can even be found on his mobile phone and health cards. Thus, the challenge of health information management is not only related to privacy limitations or access restrictions but also integrating the information as a whole for a more complete view. Personal health information (PHI) access is restricted and should be disclosed under specific conditions to healthcare practitioners as temporary information custodians. This includes not only patient treatment but also supporting healthcare management and planning through statistics for field researchers using anonymized/pseudonymized data for analysis, or even law enforcement official requests. Disclosure regulations and security requirements examples for that matter include the Personal Health Information Act (PHIA) from Canada [1], the US Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rule [2], the NHS-Data Protection Act from England [3], and the Brazilian Society of Health Informatics (SBIS) certification program in Brazil [4].

Access control plays an important role in information access restrictions with the above-described scenario—more technically speaking, authorization capabilities of applied access control on information systems. Authorization is the third phase in a generic access control, occurring after the identification and authentication processes. During authorization, the objects (information, system functions, etc.) are mapped to user permissions so they may be controlled. Authorization deploys security policy based on what the authenticated user is allowed to do on the system. Generally, it is performed by mapping existing objects and permissions in an access control matrix table. Depending on the implemented authorization of access control on an EHR system, security policies are applied differently. Formal options include mandatory access

control, discretionary access control, and non-discretionary access control.

- **Mandatory access control** (MAC) refers to a centralized access-decision model based on an object (target) label. Access controls implementing this model do not allow users to change the object settings or account security attributes.
- **Discretionary access control** (DAC) refers to the data-owner's ability to transfer part or all of the available system authorization to other users. DAC implementations allow security policies to be initially dictated by an administrator and then assigned to users to propagate among other users accordingly (under owner discretion).
- **Non-discretionary access contro**l (NDAC) is another option of centralized administration and is based on roles or tasks related to users for access decisions. The most common example of NDAC on systems is role-based access control (RBAC). In this type of implementation, authorization is assigned to roles instead of users directly. Therefore, the roles can be seen as an authorization umbrella that suits or describes the permission needs of a healthcare professional or a specific employee position within the organization's staff hierarchical structure reflected in that information system. In other words, RBAC addresses the needs for authorization control over objects, adding maintenance/administration features of grouping users that have the same permissions/needs into roles.

Currently, RBAC is globally the most commonly used access control model to cope with EHR requirements [5]. It´s been around for roughly 20 years, formalized in 1992 and published by the US National Institute of Standards and Technology (NIST) in 2000 [6]. It was added as a mandatory requirement in 2016 for certified EHR systems (EHRS) under Brazilian SBIS scope. Actually, in a recent Brazilian online survey designed to map current access control models in order to foresee next-generation EHRS implementation intentions in the Brazilian market (138 respondents,) we see this data confirming various RBAC models totaling nearly 40 percent of respondents, although in our scenario basic access-matrix-based implementations are still present (see table 1). Considering our questions asking for future implementation prediction (access control change in short-, medium-, or long-term planned implementation), DAC-MAC hybrid, RBAC full, and RBAC mixed extensions (time and context based) are what we should see for EHR systems in the near future.

AC model	Current implementation	Currently satisfies industry needs	Planned implementation		
			<12m	<36m	>36m
AC matrix basic	14.2%	6.7%	1.5%	0	0
DAC	1.5%	1.5%	0	0	0
MAC	8.2%	6.0%	0	0	0.7%
Hybrid (above)	8.2%	7.5%	1.5%	6.0%	0.7%
RBAC (Core)	16.4%	12.7%	0.7%	3.0%	1.5%
RBAC full	5.2%	5.2%	0.7%	0.7%	2.2%
RBAC time-based	15%	0.7%	0	0	0.7%
RBAC context-based	3.0%	2.2%	0	1.5%	0
RBAC mixed	13.4%	11.2%	3.0%	6.0%	0.7%

Table 1 – Survey responses considering current and planned access control implementation on Brazilian EHR systems

Healthcare routine access control demands

In a recent literature review exploring articles related to security and privacy trends for EHR, I've found different specific concerns related to the healthcare industry. To highlight severe impact challenges to the authorization process, example scenarios are described for discussion below.

Least privilege

Interconnected systems, healthcare treatment dynamics and multidisciplinary medical specialties related to professionals, and emergency situations all present varying access control demands imposed by healthcare routines. Considering the most common access control model—RBAC—one important healthcare security demand is the ability to promote least privilege best practices.

In this sense, RBAC roles may not have the ideal granularity for that purpose. The RBAC model comprises four major components: core, hierarchical, static separation of duty, and dynamic separation of duty relations. The core component represents basic access control features related to role creation and attribution to users. By using hierarchy, administrative tasks could be saved but least privilege may be compromised. That's because managing permissions using this feature results in adding authorization that needs to be carefully applied. In figure 1, medical director, cardiologists, and rheumatologists share doctor and resident permission sets. Cardiologists and rheumatologists share specialists permissions. All three have their own permission sets. Users can be bound to many roles that have many permissions to EHRS-mapped objects. By receiving hierarchical authorization, a user's resulting conjunction of roles may represent more than those necessary to perform specific duties, even considering that the individual roles applied in the chain were created using the minimal permission concept in mind while viewed separately.

The very nature of healthcare treatment is dynamic. It's not easy to strictly define healthcare practitioner needs in terms of access to EHR systems information or functions because routines cannot always be predicted. The same user may have specific functional needs while working at a triage station but later a broader view while attending to emergency room tasks. Also, due to medical plurality in terms of specialties, a user may act as a clinical physician in the morning, therefore requiring diagnostic system features. But during the following shift the system interaction may be related to gastroenterology, therefore requiring a whole new set of system functions. This example shows how complex the achievement of least privilege using RBAC alone can be. Time-based or context-based RBAC extensions are proposed in the literature to address dynamic environments. These adaptations promote transient access-decisions to cope with occasional permissions needs on an EHR system. Actually, NIST is currently providing case studies to understand industry-specific needs. Examples of a working group related to the healthcare industry can be seen at NIST "Role Engineering and RBAC Standards [7], which includes the following: HL7 Security and Accountability SIG, VA RBAC and Role Engineering site, Healthcare Role-Based Access Control Task Force, HIPAA Security Requirements, HIPAA Advisory on RBAC, and HIPAA rules.

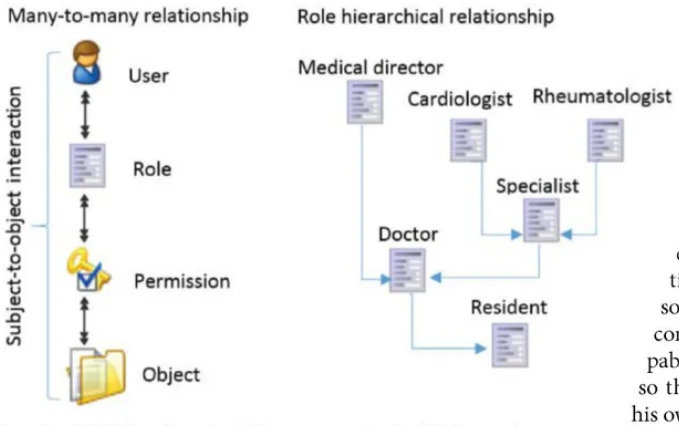


Figure 1 – RBAC hierarchy authorization representation for EHR-S scenario

Emergency access and PHI disclosure

The Hippocratic Oath and the swearing of putting patient care above all other interest (or other ethics pledge) are commonly seen as medical students transition to doctors. Although this is more an idealistic process, and the "do no harm" has literally little or no impact on a doctor's behavior in real life, patient priority is indeed what needs to be considered in any system access-control constraint. After all, these days a doctor will not be able to treat anyone without the need of systems interaction simply because clinics, smaller facilities, and hospitals—virtually all healthcare facilities—are driven by electronic authorizations.

In such cases, the EHR system needs a way to ensure authorization control so a patient can be treated. This feature can be seen in the literature as a "breaking the glass" emergency function. Advised emergency practices usually advocate two-step activation (different users) for this state to be declared (so collusion can be avoided) and include a tightened audit trail. That's because this special condition needs to actually be an exception so authorization sets are not overruled simply to ease daily processes in terms of access constraint. Notice, though, that even during this phase the healthcare professional may face blocked access to patient data because the electronic health record has privacy locks that demand explicit authorization by its owner (the patient). RBAC has no native feature for that purpose, so common suggestions to solve the issue involve combining the discretionary function from DAC capabilities, treating the patient as a regular EHRS user so that he could edit access control permissions over his own data objects. If patient is unresponsive, "breaking the glass" is enforced.

Warfare has advanced considerably since the Middle Ages, but in many ways the principles of fortification remain the same. The great castles of antiquity were ingeniously designed to protect their inhabitants from persistent enemy threats. Their carefully planned and creative defensive measures provide rich metaphors for today's cyber guardians. SecureWorld attendees will enjoy exploring and learning from the historical anecdotes and tactics in this year's conference theme.

Join like-minded security professionals in your local community for high-quality, affordable training and education. Attend featured keynotes, panel discussions and breakout sessions, and learn from nationally-recognized experts. Network with fellow practitioners, thought leaders, associations and solution vendors.

Don't go it alone. Register for a SecureWorld conference near you.

www.secureworldexpo.com

Our Fall 2017 event schedule will kick off with the first annual Twin Cities conference. Mark your calendars and make plans to attend!

EARN CPE CREDITS

Fall:

Twin Cities, MN	Sept. 6
Detroit, MI	Sept. 13-14
St. Louis, MO	Sept. 20-21
Bay Area, CA	Oct. 5
Dallas, TX	Oct. 18-19
Cincinnati, OH	Oct. 24
Denver, CO	Nov. 1-2
Seattle, WA	Nov. 8-9

Interconnection of systems

Interconnected EHR systems represent another challenge in promoting access control. RBAC was not originally developed to cope with multiple security policies. That´s because the centralized access decision point (ADP) is not able to map the different users' attributes and system objects that are not locally bound. The scenario is described as "cross-border" access control in the literature, where a few workarounds are proposed. ISO 22600, for instance, includes adding a neutral third-party (certification authority) PKI entity to issue mutually accepted (from both hospitals, for example) identification to users. The advised issuing procedure incorporates special tags (attribute certificates) to identify healthcare professional specialties and government issued IDs, broadly characterizing the users in a way both ADPs could differentiate and apply corresponding authorization restrictions.

The other workaround is a little trickier because local system objects are too particular to be standardized. Data dictionary (database collection of information descriptions) and system functions exemplify the particularity of objects that would be "controlled" by the outer EHRS. On top of that, we need to consider the information classifications deriving security policies that will be used to compose the ADP access-matrix, which are unique to each facility/organization. The challenge is more complex than the simple domain or forest of trust we see today in Active Directory trusted domain objects (TDO) [8], allowing authenticated users to connect to external realms and shared objects (depending on the trust direction configured) to translate local ADPs to cross borders accordingly.

Meaningful use and object identifiers, semantic web, linked open data (LOD) [9], and cross-origin resource sharing (CORS) are examples of possible ways to commonly map objects within confederated systems. The sensitivity of each object also needs to be commonly established between parties, though, so trust between domains can be fully incorporated, including authorization control.

Separation of duties

The ability to control and divide system functions so single users cannot perform certain system activities (those not specific to their professional duties) is particularly important in health care. That´s because system functions can offer functionalities that represent conflicts of interest if conducted by the same user. These functions/tasks should therefore be specifically mapped within the system to allow conflict identification. The first task is to locate or create checkpoints along the system flow and processes to help enumerate user responsibilities and accountabilities. Users able to insert health planning and request treatment procedures to be executed should not be those able to authorize them or forward provider reimbursement in case of insurance or government payers-based healthcare systems. That´s because requesting and authorizing functions denote clear conflict of interest. Function-based privilege management can be asserted upon legislation, professional regulation, or other task-oriented specifications to achieve separation of purpose due to legal, ethical, or other conflict. Manual identification of conflict of functions, while composing roles for later assignment, is an administrator task and prone to error. This is a very sensitive process and requires additional care leveraging separation of duties (SoD) in EHR systems.

RBAC was created with SoD in mind. Static separation of duty (SSoD) and dynamic separation of duty (DSoD) components can be used natively to separate functions that can be performed by single users. The use of static and dynamic components is referred to as RBAC restrict mode. Static validations are performed by system security administrative tasks while creating new roles. Dynamic validations may be needed during system use to identify conflicted roles on user's sessions in case of multiple role assignment. The second case needs particular attention on EHR systems, a common scenario in the case of users with multiple roles assigned being prompted to choose which role is to be used in the current session. The problem arises when the EHR system fails to map the history of user action in such a SoD-protected function [10] so in the next session an error is not alerted if that user selects a different role that alone shows no conflict. Dynamic SoD is commonly determined to be not compliant on security audits when such behavior is discovered.

Access delegation

Access delegation (user grants) is also related to accountability and professional regulation issues and can make use of dynamic access control capabilities. In this case, slightly different from previously described problems, user discretion is used to forward grants temporarily to another user with the intention of allowing treatment to continue in case of his absence. An EHRS feature for that purpose usually allows part or all user grants to be "delegated" to the chosen user.

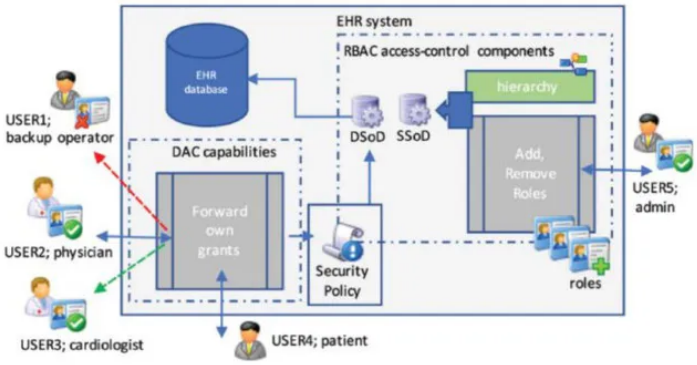


Figure 2 – RBAC components and connections to the cited access control threats on EHRS

For instance, an IT user responsible for backup operations on the system could allow another user to perform these actions. In this case, necessary training is required. Notice, though, that for some type of users (healthcare professionals, for instance) this operation must be accompanied by role vetting, considering the professional title or other identification, because the accountability in this case is legally bound to the healthcare procedures that the professional is authorized to perform. A possible solution to this specific access control threat could be adding a table or ontology/taxonomy that describes healthcare specialties (ie., American Board of Health specialities [11]) and related professional tasks/duties in a way that could be later translated to an existing system function list for additional access control decisions. Using this suggested flow, a grant delegation will be processed only if role and professional duties match: a physician could never delegate his grants to an IT user for instance. In figure 2, USER2 can delegate grants to USER3 but not to USER1 due to professional duties restrictions incorporated into the authorization access decision.

Conclusions

Role-based access control (RBAC) is the most prevalent access control method mediating healthcare professionals on EHR systems. Emergency access, access-delegation, cross-border scenarios, PHI privacy control, least privilege, and separation of duties are examples of security challenges to access control in the healthcare industry. Some can be addressed using native security components of RBAC, while others require adaptations. Variations of the RBAC original components and the use of hybrid models or mixed RBAC extensions are possible solutions found in research literature to cope with health informatics specific scenarios when it comes to authorization issues.

Update our survey

Please consider updating our Brazilian survey with an international perspective of the current use and future expectation for access control implementation on electronic health record systems. Our English-translated survey can be found here. When prompted, please provide the following #ID: 435348-2 that characterizes respondent profile as an *ISSA Journal* reader.

References

1. Personal Health Information Act (PHIA), "Chapter P-7.01: An Act to Provide for the Protection of Personal Health Information," Queen's Printer, St. John's, Newfoundland and Labrador, Canada (Assented to June 4, 2008) - http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm.
2. HIPAA Security and Privacy, "Part 164—Security and Privacy," US Government Publishing Office (10/1/07) – https://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-part164.pdf.
3. Data Protection Act, Gov.UK – https://www.gov.uk/data-protection/the-data-protection-act.
4. "EHR-S Certification Manual," Brazilian Society of Health Informatics – http://www.sbis.org.br/certificacao-sbis (Portuguese only)
5. Señor IC, Fernández--Alemán JL, Lozoya PÁ, Toval A. "Access Control Management in electronic Health Records: A Systematic Literature Review," Gac Sanit. 2012 Sep-Oct;26(5):463-8. doi: 10.1016/j.gaceta. https://www.ncbi.nlm.nih.gov/labs/articles/22424969/.
6. Sandhu R, Ferraiolo DF, Kuhn DR. "The NIST Model for Role-based Access Control: Toward a Unified Standard," Proceedings, 5th ACM Workshop on Role-based access Control, July 26-27, 2000, Berlin, pp.47-63 – http://csrc.nist.gov/groups/SNS/rbac/documents/sandhu-ferraiolo-kuhn-00.pdf.
7. NIST RBAC Working Groups, "Role Engineering and RBAC Standards," NIST – http://csrc.nist.gov/groups/SNS/rbac/standards.html.
8. Active Directory Trust, "Understanding Trust Types," Microsoft Windows Server – https://technet.microsoft.com/en-us/library/cc730798(v=ws.11).aspx.
9. W3C, "SweoIG/TaskForces/CommunityProjects/LinkingOpenData," W3C – https://www.w3.org/wiki/SweoIG/TaskForces/CommunityProjects/LinkingOpenData.
10. Wang DWD, Liu WLW, Lu JLJ, Ma XMX. "A History-Based Constraint for Separation-of-Duty Policy in Role-based Access Control Model. 2009," Int Conf E-bus Inf Syst Secur. 2009;(section 3). http://ieeexplore.ieee.org/document/5137873/.
11. "ABMS Guide to Medical Specialties 2017," American Board of Medical Specialities – https://www.abmsdirectory.com/pdf/Resources_guide_physicians.pdf.

About the Author

Marcelo Carvalho, CISSP, CISA, CRISC, has 17 years of information security experience at telecom and digital certificate companies and is currently an IS auditor for information assurance security and a IT/IS professor at various universities. He may be contacted at marcelo.carvalho@ieee.org.

ISSA DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Cybersecurity Risk in Health Care

By Barry S. Herrin – ISSA member, Metro Atlanta Chapter

This article discusses the current state of healthcare data privacy and security, the legal issues requiring attention, risks of the growing use of remote and wearable technologies, and cybersecurity insurance.

Abstract

The need for constant availability and integrity of patient data means that many organizations compromise on privacy and security, often to their detriment. This article discusses the current state of healthcare data privacy and security, examines the legal issues requiring attention, discusses risks of the growing use of remote technologies, mHealth, and wearable technology, and finally discusses cybersecurity insurance as a way to mitigate the financial costs of breach.

The current state

Notwithstanding the imperative of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its Privacy and Security Rule,[1] the era of interoperability has created a de-emphasis on the confidentiality of medical information while, at the same time, creating a tremendous emphasis on integrity and availability.

Findings from the Health Care Industry Cybersecurity Task Force in its final report of June 2, 2017,[2] show that "of the three aims of cybersecurity (confidentiality, integrity, availability), availability is the most important. You cannot take care of patients without having availability of information. Having high availability of patient information is especially important with hospitals that operate 24x7 and 365 days a year." Second to availability was integrity of data. The HCIC report specifically stated that "integrity of data is important for protecting patient safety," which is "directly implicated when it comes to connected medical devices and patients whose health can be directly impacted by the operation of the medical device." However, the report recognizes that the drive to interoperability has resulted in the confidentiality of medical information being de-prioritized and asserts that "healthcare data confidentiality must remain top of mind."

A 2017 KLAS survey reports that 41 percent of respondents said their health systems dedicate less than three percent of the IT budget to cybersecurity, primarily because IT leadership has been focused on implementing electronic health record systems and dealing with interoperability challenges.[3]

Task Force Imperative 4 calls for an "increase [in] healthcare industry readiness through improved cybersecurity awareness and education." However, the increase in readiness "requires a holistic cybersecurity strategy. Organizations that do not adopt a holistic strategy not only put their data, organizations, and reputation at risk, but also—most importantly—the welfare and safety of their patients."

In the healthcare industry specifically, the financial impact of cybersecurity breaches is grim. One in three Americans was affected by healthcare breaches in 2015, according to a report from Bitglass.[4] That's more than 113 million individuals. Each lost or stolen medical record costs a healthcare organization

1 45 CFR Parts 160 and 164; the enabling legislation is found at 42 U.S.C. Section 1320a-7c.

2 "Report on Improving Cybersecurity in the Health Care Industry," Health Care Industry Cybersecurity Task Force (June 2017) – https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

3 Center for Connected Medicine report, "The Internet of Medical Things: Harnessing IoMT for Value-Based Care," July 2017 – https://www.connectedmed.com/files/assets/common/downloads/publication.pdf.

4 Bitglass. "Bitglass Healthcare Breach Report 2016," Bitglass – https://pages.bitglass.com/BR-Healthcare-Breach-Report-2016_PDF.html.

$363 per record on average, per a Ponemon Institute report.[5] The anecdotal record is not any more pleasant: Hollywood Presbyterian's information systems were held hostage in February 2016 for $3.6 million in Bitcoin,[6] and more and more healthcare enterprises are creating reserves for data ransom. A 2016 IBM study quoted by *SC Media UK* showed that in the United States 70 percent of businesses receiving a ransomware demand paid to get their data back, with 50 percent of those paying more than $10,000 and a further 20 percent paying more than $40,000.[7]

No matter the technology used in the healthcare industry today—e-signature software, EHR platforms, wearable devices, smartphones, tablets, or other software or hardware—providers can either work to mitigate risk or watch the organization spiral into potentially uncontrollable vulnerability. Today's electronic environment leaves little room for laissez-faire security efforts if a healthcare provider wants to remain safe from attack and protected from the financial consequences of the inevitable.

Why HIPAA still matters

HIPAA in general, and the Security Rule in particular, imposes specific compliance burdens on healthcare "covered entities." Any use or disclosure of electronic protected health information (ePHI) not in compliance with the Privacy and Security Rules or more stringent state law constitutes a violation of HIPAA.[8] The failure of a covered entity to implement sufficient security measures regarding the transmission of and storage of ePHI to "reduce risks and vulnerabilities to a reasonable and appropriate level" is also a violation.[9] Likewise, a failure to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of its facility, and the movement of these items within its facility, are violations.[10] And, once a security incident occurs, the failure to "timely identify and respond to a known security incident, mitigate the harmful effects of the security incident, and document the security incident and its outcome" are all violations.[11]

At the time of writing, most of the Security Rule fines and penalties assessed by the US Department of Health and Human Services Office for Civil Rights (OCR) relate solely or primarily to either (1) theft of devices containing unsecured ePHI or (2) failure to conduct a security risk assessment that is discovered when another privacy or security breach is investigated. Examples of such "traditional" enforcement activity in recent times include the August 2015 announcement of a $750,000 settlement against Cancer Care Group, P.C., for the theft of an employee laptop containing ePHI on 55,000 individuals, the December 2013 announcement of a $150,000 settlement against Adult & Pediatric Dermatology, P.C., for

5 Larry Ponemon, "Cost of Data Breaches Rising Globally, Says '2015 Cost of a Data Breach Study: Global Analysis,' " Security Intelligence, May 27, 2015 – https://securityintelligence.com/cost-of-a-data-breach-2015.

6 Vincent Lanaria, "Hackers Hold Hollywood Hospital's Computer System Hostage, Demand $3.6 Million As Patients Transferred," Tech Times, 16 February 2016 – http://www.techtimes.com/articles/133874/20160216/hackers-hold-hollywood-hospital-s-computer-system-hostage-demand-3-6-million-as-patients-transferred.htm. The hospital eventually paid $17,000 in Bitcoin.

7 Max Metzger, "Your Money or Your Files: Why Do Ransomware Victims Pay Up?" SC Magazine UK, May 25, 2017 – https://www.scmagazineuk.com/your-money-or-your-files-why-do-ransomware-victims-pay-up/article/664211/.

8 45 C.F.R. §§ 160.103 and 164.502 (a). NOTE: CFR 45, Parts 160 and 164 can be found at US Electronic Code of Federal Regulations: Title 45—Public Welfare, Subchapter C—Administrative Data Standards and Related Requirements: 160-164 – https://www.ecfr.gov/cgi-bin/text-idx?SID=fbc57ba7be313c69e19aa1e78ac97adf&mc=true&tpl=/ecfrbrowse/Title45/45CsubchapC.tpl.

9 45 C.F.R. §164.308(a)(1)(ii)(B)

10 45 C.F.R. § 164.310(d)(1)

11 45 C.F.R. § 164.308(a)(6)(ii)

the theft of a thumb drive containing ePHI on 2,200 patients, and the announcement of settlements by Idaho State University and University of Washington Medicine for failure to conduct privacy and security risk assessments and failure to adequately adopt security measures. Were this still the level of involvement by OCR in ePHI enforcement, a shrug of the CIO's shoulders and a promise to encrypt all ePHI data at rest would be the universal response.

However, in recent times the enforcement focus has shifted to more "core" system security functions and away from the "low hanging fruit" of lost or stolen data-carrying devices. For example, a $850,000 settlement paid by Lahey Clinic Hospital in 2015 specifically references the failure "to assign a unique user name for identifying and tracking user identity" with respect to a particular workstation,[12] failure to have a working audit trail capability with respect to workstation activity,[13] and the failure to restrict physical access to workstations generally to authorized personnel. A similar enforcement activity against South Broward Hospital District in February 2017 resulted in a $5,500,00 settlement payment based on improper access to ePHI by over a dozen individuals exposing in excess of 80,000 patient records and the failure of the covered entity to "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports"[14] and "to implement policies and procedures that establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."[15] Several enforcement activities also resulted in settlements for failure to have business associate agreements in place with third-party vendors responsible for storing ePHI.[16] Just as the environment for bad cyber behavior has matured, so has the OCR's level of understanding of system and enterprise failures of the healthcare community.

Eighty-four percent of health applications for smartphones that were approved by the FDA were found to create HIPAA violations and were "hackable."

The healthcare Internet of things

The task of HIPAA compliance and compliance with cybersecurity "best practices" is being made harder with the proliferation of Internet-connected devices in the healthcare industry. As recently as 2012, a Ponemon Institute survey reported that 69 percent of respondents did not even address the security of US Food and Drug Administration (FDA) approved medical devices in their IT security or data protection activities.[17] Since that time, over five billion devices—*not including smartphones*—have connected to the Internet, and that number is expected to grow to between 25 billion and 50 billion by 2025.[18]

The healthcare industry has particular patient safety risks associated with these devices, as revealed in a 2012 US Government Accountability Office report on the lack of action by the FDA to expand its consideration of information security for medical devices.[19] A November 2015 Wired.com survey listed the seven healthcare device types most vulnerable to hacking or other violation, which included drug infusion pumps, Bluetooth-enabled defibrillators, blood refrigeration units, and CT scanners—the failure of any of which would create tremendous patient risk. We have grown far beyond the fear of hacking the vice president's pacemaker.[20]

The fact that smartphones are not included in this total is worrisome, as the growth in potential cyber risk due to smartphone use is even more troubling. Eighty-four percent of health applications for smartphones that were approved by the FDA were found to create HIPAA violations and were "hackable."[21] Also worrisome is the continued increase in the use of smartphones to transmit and receive unsecured ePHI

12 45 C.F.R. § 164.312(a)(2)(i)

13 45 C.F.R. § 164.312(b)

14 45 C.F.R. §164.308(a)(l)(ii)(D)

15 45 C.F.R. § 164.308(a)(4)(ii)(C)

16 As examples, see the July 18, 2016 Resolution Agreement with Oregon Health & Science University in which $2,7 million was paid and the September 23, 2016 Resolution Agreement with Care New England Health System in which $400,000 was paid.

17 John Glaser, "The Risky Business of Information Security: With Growing Threats to Patient Privacy and Increasing Sanctions by Regulators, Make Data Security Central to Your Business," Hospitals & Health Networks, August 12, 2014 – http://www.hhnmag.com/articles/4064-the-risky-business-of-information-security.

18 The Florida Bar, "8th Annual FUNdamentals: The Legal Implications of the 'Internet of Things,'" Course 2232R (September 16, 2016)

19 GAO, "Report to Congressional Requesters: Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices," United States Government Accountability Office, August 2012 – http://www.gao.gov/assets/650/647767.pdf.

20 Lisa Vaas, "Doctors Disabled Wireless in Dick Cheney's Pacemaker to Thwart Hacking," Naked Security, Sophos, 22 Oct 2013 – https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/.

21 Ibid.

(primarily by text message) for patient treatment by healthcare professionals, in spite of HIPAA's requirements and facility rules attempting to limit such activity.[22] Most health care enterprises gave up the fight over "bring your own device," or BYOD, rules due to provider pressure a long time ago anyway. Although study results vary, as of 2014 "upward of 90 percent of healthcare organizations permit employees and clinicians to use their own mobile devices to connect to a provider's network or enterprise systems."[23]

One has to wonder what OCR's response to all of this would be in light of the settlement agreements mentioned earlier: the decision not to impose device accountability for provider convenience may be fertile ground for future fines and penalties. And there is always the modern privacy paradox: health care consumers voluntarily share endless amounts of personal health information with applications on their smartphones, resulting in data being stored who-knows-where on the Internet without them thinking if it is convenient for them[24]; however, these same consumers continue to resist the same sharing activities by their own healthcare providers, even if such activity would result in faster and better health care.[25]

Cybersecurity insurance

In October of 2002, *The Economist* magazine opined[26] that "total security was impossible" and that insurance would be the way that businesses mitigated the financial risk caused by this lack of security. Since that time, both security defenses and security attacks have proliferated, changed, and become more aggressive and complex. However, the cybersecurity insurance market, though maturing, is not developing at as rapid a pace. Some issues that remain to be explored are due to the relative newness of the coverage and the lack of good predictive actuarial models.[27]

While the market matures, there are various factors that potential insureds should evaluate closely as they shop for and price out cybersecurity insurance. The first and most important of these coverages should be the coverage of costs related to managing breaches, to include expenses related to the investigation, remediation efforts, and patient notification. Other costs that may also be incurred are credit monitoring services,[28] damages associated with identity theft, damages associated with recovery of data, damages incurred due to

22 Ibid. (citing a 2015 University of Chicago survey finding that over 70 percent of its medical residents improperly sent ePHI by text messages).

23 John Glaser, "The Risky Business of Information Security: With Growing Threats to Patient Privacy and Increasing Sanctions by Regulators, Make Data Security Central to Your Business," Hospitals & Health Networks, August 12, 2014 – http://www.hhnmag.com/articles/4064-the-risky-business-of-information-security.

24 Shannon Barnet, "Millennials and Healthcare: 25 Things to Know," Becker's Hospital Review, August 04, 2015 – http://www.beckershospitalreview.com/hospital-management-administration/millennials-and-healthcare-25-things-to-know.html. 71 percent of Millenials surveyed by Harris would use a mobile app to share health care data with providers. See also Mintel, "Sixty Percent of Millennials Willing to Share Personal Info with Brands," Mintel, March 7, 2014 – http://www.mintel.com/press-centre/social-and-lifestyle/millennials-share-personal-info, in which the study reports that 60% of Millennials would be willing to provide details about their personal preferences and habits to marketers, and, of those that would not initially provide such information, 30% would do so after receiving an incentive offer such as a discount off future purchases.

25 Denver Nicks, "Survey: Millennials Care about Privacy (But Not So Much in Japan), Time, Nov. 07, 2013 – http://techland.time.com/2013/11/07/survey-millennials-care-about-privacy-but-not-so-much-in-japan/. Only 4% of respondents would be comfortable with data being used for a purpose outside of its original context. The study also says that these preferences vary by economic status, with high-income worried more about data privacy than low-income people.

26 "Putting It All Together," The Economist (October 24, 2002)

27 Koo, "More Incident Data Needed for Cybersecurity Insurance," Bloomberg BNA (March 28, 2016)

28 Even though there is almost a universal recognition in the law enforcement and security communities that these programs do no good at all, as the sophisticated hacker knows to wait out the 1-2 years of service before making use of the stolen data.

having to reset EHR systems, and damages to reconstruct or recover websites and other Internet presences. Business continuity expenses related to workarounds or loss of revenue due to a cybersecurity incident might also need coverage, especially as most commercial policies of this type are figuring out how to exclude cyber-related risks from their covered losses. Finally, but not least importantly, coverage for rogue employees and insider threats needs to be a part of the insurance package.

The type of coverage a healthcare enterprise can obtain, and the premiums therefore, may be affected by certain underwriting considerations, all of which should inform the enterprise's compliance efforts:

- The enterprise should be able to show that it is in compliance with HIPAA, including those provisions that require security and privacy risk assessments and proof of a plan of mitigation and remediation. Insurers likely will not cover losses resulting from a gap in HIPAA compliance, especially because there is a legal obligation on the enterprise to find out what those are.
- The potential insured needs to know what the insurer's requirements are for encryption beyond those mandated by HIPAA. Some coverages require more secure and more robust email systems that are more resistant to phishing and spoofing, and even other coverages may require intentional phishing attacks by the insured's IT department or vendors to gauge compliance with training.
- The training requirements for new employee onboarding and access by non-employee contractors may need to meet certain criteria beyond HIPAA workforce awareness training.
- Insurers may require that contractors providing "business associate" services be separately insured as a first layer of defense against cost.
- The potential purchaser needs to be on the lookout for what is referred to in the industry as "cannibalizing" coverage, in which the costs of defense reduce the limits available to pay damages or judgments. The best coverage separates costs of defense from claims expenses.
- The purchased coverage, as with certain types of malpractice insurance, should be based on the "date of detection" as opposed to "date of intrusion." It is so difficult, even with the best system monitoring tools, to determine when a breach or incident actually first occurred, so the enterprise does not want to be locked into a technical dispute with the insurer about when the hack "should have been" detected.
- The prospective insured needs to know whether offshore operations will be covered. Significant risks are associated with outsourcing certain data manipulation and management functions to countries or regions that have stronger privacy and data security rules than the United States. In particular, the European Union takes a dim view of American-style discovery and most likely will not permit the compelled return of data from an EU vendor in litigation pending in United States courts.

Conclusions

The growth of connected devices, connected physicians, and connected patients will continue to push healthcare facilities to provide more interoperability for health data than ever before. These same technological pressures will make it more and more easy for cybercriminals and disgruntled employees to compromise the data upon which everyone relies for reliable patient care, because an increase in interoperability in most cases creates an increase in gaps in security. Healthcare systems need to recognize this risk as a direct threat to patient care, and not just to its financial and technology resources. A holistic security approach, combining effective cybersecurity practices, HIPAA training and compliance, and appropriate insurance coverages will be the best way to address this growing area of opportunity—and risk—in the future.

About the Author

Barry S. Herrin, JD, FAHIMA, FACHE, is the founder of Herrin Health Law P.C. in Atlanta, Georgia. Herrin has over 25 years of experience practicing law in the areas of healthcare and hospital law and policy, privacy law and health information management, among other healthcare-specific practice areas. He is both a Fellow of the American College of Healthcare Executives and a Fellow of the American Health Information Management Association. He may be reached at barry.herrin@herrinhealthlaw.com.

ISSA DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Healthcare Security Ailments and Treatments the World Needs to Know

By Jon Sternstein - ISSA Member, Raleigh Chapter

This article provides insight into the immense data breach problem affecting the healthcare industry and closes with actionable solutions that all healthcare organizations should be accomplishing to minimize the risk of data breach.

Abstract

This article provides insight into the immense data breach problem affecting the healthcare industry. It also analyzes healthcare breach trends and shows how the threat landscape is changing in recent years. It proceeds to discuss a 2017 healthcare data breach in which protected health information went up for sale on the dark market. The discussion closes with actionable solutions that all healthcare organizations should be accomplishing to minimize the risk of data breach.

174,635,373

That is the total number of healthcare records that have been lost in US breaches from 2009 until July 13, 2017 [6]. Think about that for a minute. 174 million protected health information records is a number so large, it is difficult to comprehend. The entire United States population is only 321.4 million individuals. The most populous state, California, has only 39 million individuals, a number that is dwarfed by the number of patient records lost since 2009. This large number only includes breaches that are of 500 or more records. This is a large problem, and it is going to take a significant effort to stop this trend.

Your patient record contains your full name, Social Security Number, address, phone number, birth date, medical condition, family information, and more. Unlike payment card data, protected health information (PHI) cannot be replaced or reissued. This makes healthcare breaches the most costly out of any industry. Ponemon's *2017 Cost of Data Breach Study* lists healthcare breaches at a staggering $380 per record lost, a number that continues to increase each year [13]. Healthcare breaches cost $135 more per record than the next closest industry. The average data breach size in the 2017 Ponemon study was 24,089, which would cost a healthcare organization $9,153,820 (24,089 x $380). Not only are these breaches costly to the organization, but they also impact the patients. The victims in these cases are people who trust the healthcare organization with their lives and their most sensitive information. They should not be troubled with identity theft on top of medical issues.

Healthcare breaches cost $135 more per record than the next closest industry.

Breach trends

Health and Human Services (HHS) categorizes healthcare breaches into five main groups: hacking/IT incident, improper disposal, loss, theft, and unauthorized access/disclosure. Each of these categories can be summarized as follows:

- **Hacking/IT incident:** An intruder breaks into a computer system containing patient information, or a server is misconfigured and allows remote access to patient data.
- **Improper disposal:** The insecure disposal of patient information. Examples include recycling paper healthcare records without shredding first, or donating computers without securely erasing (or destroying) the hard drives.
- **Loss:** Unintentionally misplacing patient information. A common example is a physician losing an unencrypted flash drive with patient information.

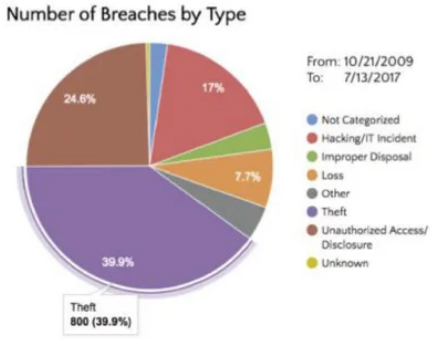


Figure 1 – Number of healthcare breaches by type

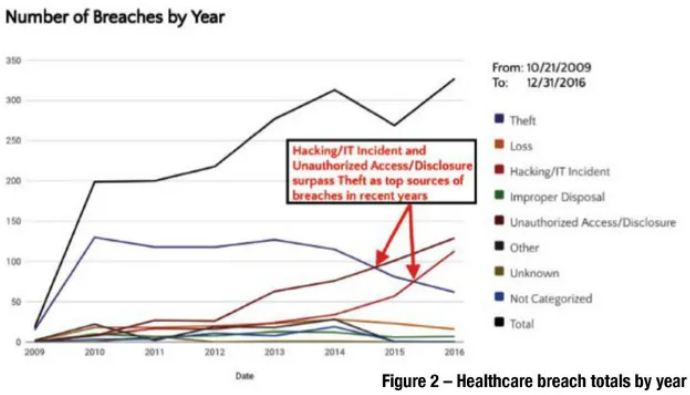


Figure 2 – Healthcare breach totals by year

- **Theft:** Physically stealing patient information.
- **Unauthorized access/disclosure:** An individual accesses information he does not have authorization to view. Examples include patient records sent to an incorrect individual or a healthcare employee who views the healthcare records for patients that are not under his care. Some of the breaches in this category could be interpreted as hacking/IT incident breaches.

Since 2009, most of the reported healthcare breaches have been due to theft (figure 1). Many of these theft breaches have occurred because unencrypted laptops or flash drives were stolen. It is difficult to eliminate theft of computer equipment; however, most of these breaches would not need to be reported if the affected organization simply encrypted their drives. Both Microsoft and Mac OS offer completely free full-disk encryption with their operating systems, so there really isn't any reason why this protective measure is not in place. We can almost eliminate this risk with completely free solutions.

While it is clear that most reported healthcare breaches since 2009 have been due to theft, this trend is drastically changing. It would be a grave mistake to only focus on encrypting drives in order to protect patient information. Over the past two years, hacking/IT incident and unauthorized access have both passed theft as the top causes of healthcare data breaches (figure 2). Additionally, breaches due to theft have been declining.

There are several reasons for these trends. First let's examine why breaches due to theft are declining. Organizations are getting better at encrypting hard drives, thus reducing the amount of reportable breaches due to theft. This may also explain the decrease of breaches due to "loss" as well. However, organizations need to remember to encrypt desktops and flash drives as well, not just laptops. And there are still a large number of paper records stolen. Theft will continue to be a large threat while there are unencrypted devices and paper records available.

The increase in hacking and unauthorized access/disclosure breaches could be due to more attacks occurring and increasing reliance on technology to manage our healthcare data. We may also see more reportable breaches due to these categories because we're simply getting better at detecting these types of incidents. So hacking is probably increasing, but we're also getting better at discovering these compromises as they occur.

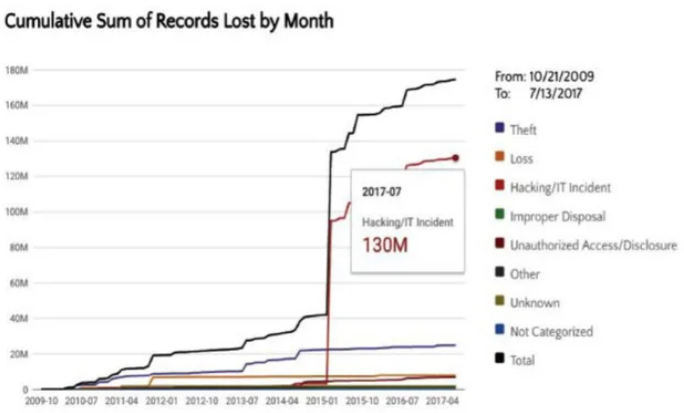


Figure 3 – Most PHI have been breached by hacking/IT incidents

Patient data for sale

Why would anyone want to steal patient information? I was asked this many times when I was a healthcare security officer. People can generally see why a thief would steal cash or a credit card, but what can they do with a patient record? Since protected health information (PHI) is your full identity, a thief could use that information to open new credit cards, make false insurance claims, sell for ransom, and more. Let's look at a recent real-life example.

In March 2017, a behavioral health center was hacked in Maine, USA. This breach was unique in that the PHI immediately appeared for sale on the dark web. The criminal stated he had PHI for 4229 individuals, and the information contained names, addresses, phone numbers, employers, birthdays, social security numbers, and therapy notes. In addition to the listing the price, the criminal stated that the stolen data could be used for ransom and specifically noted the breached health provider's $4 million insurance policy. The thief further implied that the data could be used to target affected individuals as the data contained full psychiatric information on "everyone from bank presidents to garage mechanics [3]. The criminal was selling the data for a minimum of $10,000 for the full set or $3 per individual's name, address, date of birth, and social security number. This case is a prime example of how stolen protected health information is used and shows how criminals have complete disregard for how this information can affect the lives of the individuals. Healthcare data is incredibly sensitive and is unfortunately being compromised at an alarming rate.

The perfect storm - ransomware

As if the previous threats were not enough, the healthcare industry has been slammed by ransomware. Not only have there been many reported healthcare ransomware extortions, the media has covered several cases where complete hospital systems have been overrun by ransomware and had to revert to paper records. Hollywood Presbyterian Medical Center [1] and Methodist Hospital in Kentucky [11] are just two examples of hospitals that were in a state of emergency due to ransomware and reverted to paper records while regaining access to their computers. In some cases, patients had to be redirected to other hospitals.

This unfortunate trend is only increasing. In 2016, there were 10 reported healthcare breaches of 500 or more records due to ransomware [6]. Halfway through 2017, we have already surpassed 2016's number of reported ransomware breaches. This has been such a large problem that Health and Human Services released a ransomware fact sheet to help healthcare organizations [7]. With ransomware on the rise, and system compromises becoming more prevalent, it's no wonder most patient records have been lost due to hacking and IT incidents (figure 3). There is really no comparison between the number of records lost due to hacking and all other breach types combined. Breaches due to hacking are usually larger because more data can be stolen when an entire server or database is compromised as opposed to the theft of a single laptop.

Regulatory assistance

In order to protect health information, the US government issued the HIPAA (Health Insurance Portability and Accountability Act of 1996) Security Rule [4]. This lengthy document contains a list of steps that covered entities (such as hospitals) and their business associates must follow. One major requirement included in the Security Rule is HIPAA Part No. §164.308(a)(1)(ii)(A): Risk analysis. This requires organizations to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

All healthcare organizations both large and small must abide by these regulations. This is of such importance that the government has issued millions of dollars in fines for organizations that fail compliance for reasons such as failing to complete a risk analysis, or not signing a business associates agreement with a partner [9]. In April 2017, US Department of Health and Human Services, Office for Civil Rights (OCR) publicly announced a $2.5 million settlement with CardioNet for non-compliance with the HIPAA Security Rule and failing to have a risk analysis performed [5]. If there were questions about HIPAA enforcement before, you don't hear them now.

The needed treatment

At the end of the day, it is our duty as security professionals to protect the information that we are responsible for. The healthcare industry is no exception to this rule, and in many ways it contains some of the most sensitive information that we can protect. As the breach trends reflect, we have some serious work to do in healthcare, and patients are expecting us to secure their data. Healthcare breaches affect each and every one of us. However, all is not lost and we can see from the decrease in breaches due to theft that is possible to lower risk in healthcare organizations. Here are some solutions that lower the risk of healthcare data breaches:

1. **Security strategy** – All organizations need a strategy to successfully mitigate threats. A security strategy provides direction to a security program and allows the organization to measure progress and maturity. Many organizations make the mistake of purchasing security products without a complete strategy and then wonder why there are still security problems. A recommended method for implementing a strategy is to use a well-known security framework for guidance.
2. At the most basic level, the Center for Internet Security (CIS) maintains the top 20 critical security controls that every organization must implement to protect its data [2]. An organization can use this list to quickly get a high-level overview of its security program maturity. The top security control often takes many people by surprise: managing an "inventory of authorized and unauthorized devices." Organizations need to manage access to the network and keep all of those systems up to date. In our penetration testing engagements, it is often the forgotten server or the unauthorized test machine that provides the initial foothold onto the network. Now, how many organizations do you know that are not tracking all devices on their network?
3. For a more detailed healthcare security strategy, the National Institute of Standards and Technology (NIST) offers the "Framework for Improving Critical Infrastructure Cybersecurity" [12], the result of an executive order for managing cybersecurity risk. This freely available framework provides cost-effective, measurable steps that an organization can use to protect its data. At the heart of the framework are the following high-level functions: Identify, protect, detect, respond, and recover. Each function contains a series of actionable security controls. The framework also contains a tier structure to measure the maturity of a security program: "Partial" (Tier 1), "Risk Informed" (Tier 2), "Repeatable" (Tier 3), and "Adaptive" (Tier 4). Health and Human Services makes this even simpler for healthcare environments by providing cross-references between the NIST framework and the HIPAA Security Rule [8].
4. **Risk analysis** – A comprehensive risk analysis should include a review of the organization's security strategy, policies, and controls and include actual security testing to measure the effectiveness of the program. This task is often completed by trusted third parties, but can also be accomplished by knowledgeable staff. Not only is this a HIPAA requirement within the Security Rule, it is also essential to understanding the risks within a healthcare environment and implementing solutions. This is a way to evaluate the security program and should be a component of the overall security strategy.
5. **Education** – Implementing a successful security program is only possible with the right people in place. This can be difficult as there is a lack of skilled individuals, with predictions of a shortage of two million cybersecurity professionals by 2019 [10]. Training your staff is essential to improving knowledge and staying ahead of adversaries. Utilizing trusted partners is often a cost-effective way to fill those advanced roles or complete complex projects. Encouraging participation in local ISSA chapter meetings, 2600 meetings, and OWASP chapter meetings, taking courses, and attending security conferences all increase the skill levels of the team. Fostering an environment of knowledge sharing helps raise skill levels and also is great for team building. Education is so important that it is even one of the CIS Critical Security Controls: Security Skills Assessment and Appropriate Training to Fill Gaps [2].
6. **Encryption** – It should go without saying that all protected health information needs to be encrypted, but breach trends show that organizations still need work in this area. Encrypting laptops is absolutely needed, but workstations and flash drives need to be encrypted as well. PHI needs to be encrypted in transit as well as in storage. Once again, "data protection" is a Critical Security Control [2].
7. **Security testing** – Performing penetration testing on the organization and its applications is necessary for finding security problems before an intruder does. Trusted third parties usually perform these tests, while larger organizations often have internal red teams that continuously test the environment. Discovering these security holes is just the first phase of this process. The second and lengthier phase is putting a plan in place for fixing the problems. "Penetration tests and red team exercises" is another Critical Security Control, thus highlighting its importance [2].

All of the described solutions are crucial components of a well-developed security strategy. Without a plan in place, organizations will endlessly play a cat and mouse game, jumping at the next threat, but not creating a framework to contain all hazards.


ASIS 2017
63RD ANNUAL
SEMINAR AND EXHIBITS
SEPT. 25-28
DALLAS · TEXAS
#ASIS17 | securityexpo.org
Stop and Take a Look at our
NEW
EDUCATION LINEUP!
180+ Sessions
Innovative Formats
Trending Topics
FREE Expo Floor Education
Earn up to 30 CPEs
16 Education Tracks Including:
Active Shooter
Business Operations
Crime/Loss Prevention
Critical Infrastructure
Cyber Security
Current Events
ESRM
Information Security
Terrorism
Workplace Violence
...just to name a few!
Produced in collaboration with
ISSA
Information Systems Security Association International
Register by August 11 and SAVE!
securityexpo.org/ISSA

Closing

With over 174 million records lost to date, healthcare breaches are a growing epidemic that needs to be addressed. Hacking and ransomware are two growing threats continuing to slam the healthcare industry. However, there is hope as breaches due to physical theft have been declining in recent years. Theft used to be the largest cause of healthcare data breaches and if this threat can decline, so can other data breach sources. Comprehensive security strategies and risk analyses will reduce the risk of hacking, ransomware, unauthorized access, and other threats. Healthcare breaches affect every one of us and this problem will not fix itself. So let's get to work and secure this information because each of us has only one identity and it needs to be protected.

References

8. Balakrishnan, Anita. "The Hospital Held Hostage by Hackers," CNBC. February 16, 2016 – https://www.cnbc.com/2016/02/16/the-hospital-held-hostage-by-hackers.html.
9. CIS, "CIS Controls,"Center for Internet Security, 2017 – https://www.cisecurity.org/controls/.
10. Databreaches.net, "Highly confidential Psychotherapy Records from Maine Center Listed on the Dark Web," Databreaches.net, April 5, 2017 – https://www.databreaches.net/highly-confidential-psychotherapy-records-from-maine-center-listed-on-the-dark-web/.
11. Department of Health and Human Services, "HIPAA Administrative Simplification," HHS.gov. March 26, 2013 – https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.
12. Health and Human Services, "$2.5 Million Settlement Shows That Not Understanding HIPAA Requirements Creates Risk," Health and Human Services, April 24, 2017 – https://www.hhs.gov/about/news/2017/04/24/2-5-million-settlement-shows-not-understanding-hipaa-requirements-creates-risk.html.
13. —, "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," Health and Human Services – https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
14. —, "FACT SHEET: Ransomware and HIPAA," Health and Human Services, 2016 – https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.
15. —, "HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework," Health and Human Services, February 22, 2014 – https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.
16. —, "Resolution Agreements and Civil Money Penalties," Health and Human Services, 2017 – https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.
17. Kauflin, Jeff. "The Fast-Growing Job with a Huge Skills Gap: Cyber Security," Forbes. March 16, 2017 – https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/.
18. Krebs, Brian. "Hospital Declares 'Internal State of Emergency' after Ransomware Infection," Krebs on Security, March 22, 2016 –http://krebsonsecurity.com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/.
19. NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, February 12, 2014 – https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
20. Ponemon Institute, "2017 Cost of Data Breach Study," Ponemon Institute, 2017 – https://www.ibm.com/security/data-breach/.

About the Author

Jon Sternstein, CISS, is the founder and principal consultant of Stern Security, a data security consulting company headquartered in Raleigh, NC, focused on protecting healthcare organizations. Jon is the co-chair of the Privacy and Security Workgroup at the North Carolina Healthcare Information & Communications Alliance (NCHICA) and is a former healthcare security officer. He may be reached at jon.sternstein@sternsecurity.com.

Perspective: Women in Security SIG

Minimizing Risk in an Ever-Increasing Connected Health World

Continued from page 9

For those wishing to know more about the above topic, contribute to a more in-depth analysis on how ISSA Global SIGs could examine these findings in more depth, or to suggest your own topic for the Global SIG programs, we welcome your feedback and questions at SIGs@issa.org.

Imperative #	Imperative Text	Recommendation Scope
1	Define and streamline leadership, governance, and expectations for healthcare industry cybersecurity.	1.1 – Create a cybersecurity leader role
		1.2 – Create a healthcare-specific cybersecurity framework
		1.3 – Harmonization of laws and regulations
		1.4 – Scalable governance best practices
		1.5 – Impact to relevant fraud and abuse laws
2	Increase the security and resilience of medical devices and health IT.	2.1 – Secure legacy systems
		2.2 – Improve manufacturing and development transparency
		2.3 – Increase adoption and rigor of secure development life cycle
		2.4 – Require strong authentication
		2.5 – Reduce attack surface
		2.6 – Establish a medical computer emergency readiness team (MedCERT) for cyber triage purposes
3	Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.	3.1 – Enhance cybersecurity leadership and executive support
		3.2 – Cybersecurity workforce resourcing model
		3.3 – Create managed security service provider models to support small and medium-sized providers
		3.4 – Patient record and legacy system migration
4	Increase healthcare industry readiness through improved cybersecurity awareness and education.	4.1 – Develop executive education programs
		4.2 – Establish a cybersecurity hygiene posture
		4.3 – Establish a conformity assessment model
		4.4 – Expand NIST Baldrige Cybersecurity Excellence Builder for healthcare
		4.5 – Increase outreach and engagement for cybersecurity through education campaigns
		4.6 – Patient information self-management including cybersecurity and privacy grading system
5	Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure.	5.1 – Develop guidance for industry and academia on cybersecurity risk
		5.2 – Pursue research into protecting healthcare big data sets
6	Improve information sharing of industry threats, risks, and mitigations.	6.1 – Tailor information sharing for easier consumption
		6.2 – Broaden the scope and depth of information sharing
		6.3 – Encourage annual readiness exercises
		6.4 – Provide security clearances for members of the health care community.

Table 1 – Future stage recommendation and action cross-walk

About the Author

Dr. Rhonda Farrell, D.Sc., J.D., CISSP, CSSLP, CCMP, CMQ/OE, CSQE, is an Associate at Booz Allen Hamilton (BAH) and a member of the Board of Directors at ISSA International. She is the ISSA Intl Global SIG Chair and the Co-Founder of the Women in Security Special Interest Group (WIS SIG). She can be reached at rhonda.farrell@issa.org.

ISSA DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Medical Data Sharing: Establishing Trust in Health Information Exchange

By Barbara Filkins

Interoperability is a critical healthcare industry initiative. Trust, however, is a major barrier to achieving seamless medical data exchange. This article describes what a trust framework is, along with the implementation challenges associated with trustworthy sharing of health-related data.

Abstract

Interoperability is a critical healthcare industry initiative. Trust, however, is a major barrier to achieving seamless medical data exchange. An enabler of interoperability, a health information exchange relys on the concept of a trust framework to overcome this hurdle for the exchange of clincial information, a concept that has implications for the trustworthy exchange of other types of health-related information. Healthcare security and privacy professionals should be aware of what a trust framework is, along with the implementation challenges associated with trustworthy sharing of health-related data.

Few realize how dependent the healthcare industry is on the daily, secure electronic exchange of confidential information: health-related financial data, patient-created wellness data, patient summary information among caregivers and other authorized parties for treatment, aggregated information for population health analysis and management, and initiatives like precision medicine. The practice of health information exchange (HIE) facilitates this secure flow between unaffiliated healthcare entities, supporting interoperability, a leading industry initiative for healthcare [9].

Establishing and maintaining trust among organizations is a significant barrier to this goal [8]. In health care, trust is making sure that the exchanged data is secure, safe, and reliable to use for treatment and does not leak to the wrong people. Health information exchange efforts, especially at the enterprise or national levels, face this challenge directly—the privacy and security of data gathered from multiple sources must be protected, regardless of the different technologies, policies and practices, and contractual relationships involved.

Acronyms

The medical world is fraught with almost, if not more, acronyms than information security. Those outside of healthcare can quickly become bewildered by a conversation that includes what seems like an unending stream of acronyms, when – in reality – some of these short-hand notations have effectively become common nouns used by professionals in the health information exchange community. The list is actually shorter than it might sound in conversation.

BA	Business Associate
BA agreement	Business Associate Agreement
CE	Covered Entity
DURSA	Data Use and Reciprocal Sharing Agreement
EHR	Electronic health record
HIE	Health information exchange
HIO	Health information organization
PHI	Protected Health care information

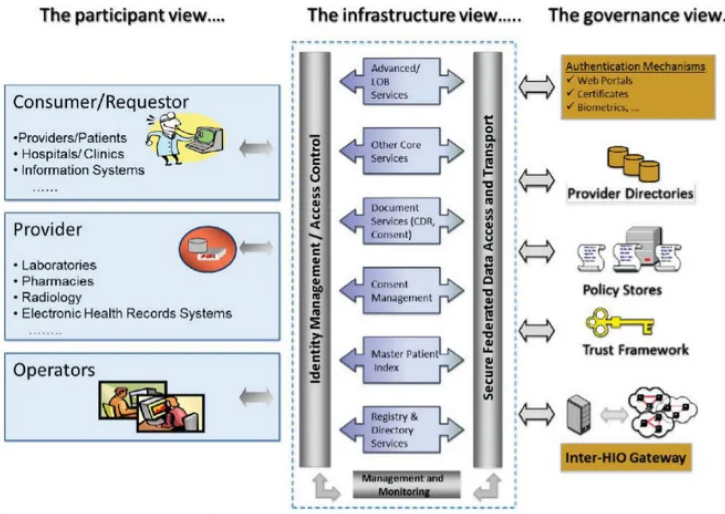


Figure 1 – HIE reference architecture

How to navigate this apparently impossible maze involving trust to enable sharing of medical information? Within the health information exchange community, a trust framework ensures the private and secure exchange of protected health information (PHI) among trading partners, meeting demands for integrity (encompassing quality and accuracy), confidentiality (in light of the privacy laws), and availability (including completeness of the record) [10].

This article explores the concept of a trust framework, detailing many initial challenges faced in implementing a set of agreements, policies, and best practice standards that data sharing communities can agree to follow, uphold, and enforce. Two enterprise initiatives are referenced: the eHealth Exchange [12] and the California Trusted Exchange Network [4].

This article represents the mainly legal and contractual agreements that must be established to ensure that a workable technical solutions will follow. A follow-on paper will detail practical insights on how an organization can assess its capabilities for health information exchange and how to engage the technical team to prepare and execute an implementation.

Understanding HIE landscape concepts

A trust framework depends on understanding two terms. The first, *health information exchange* (HIE) refers to the networked infrastructure that joins data consumers/requestors with data providers. The architecture supports governance across a federated network through standard-based interfaces with edge sources, electronic health record (EHR) systems, directories, and policy stores. It ensures seamless and trusted exchange of sensitive data through technical controls that address identity management and end user/system access control, secure data access and transport, and management and monitoring. (See figure 1 [4])

A HIE infrastructure can be viewed as a set of network-based services to transform and route data, match patient and provider identities, apply permissions (access according to user role and patent consent), monitor, and manage. Directed exchange is point-to-point communication between known endpoints, whether established routes for Health Level 7 message delivery or secure email (based on S/MIME) between providers with verified identities. Query-based exchange gathers data from various external sources and stores the compiled record in a central data repository. End users query this centralized repository for information about a patient, usually through a system-to-system interface between the HIE and their native EHR.

The second term, *health information organization* (HIO), is the entity responsible for "oversee[ing] and govern[ing] the exchange of health-related information among organizations according to nationally recognized standards [11]. Since the mid-1990s, HIOs have formed at local, state, and national levels including both private and public sectors entities.

An HIO represents the data-sharing network (HIE network) of its members or participants that agree to exchange PHI through a trust framework localized or unique to that community. Generally, participants include either covered entities or business associates of covered entities as defined by

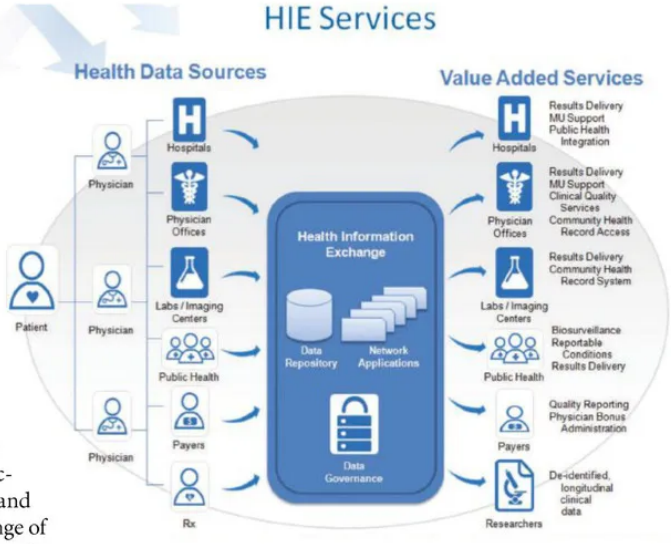


Figure 2 – The value of health information exchange (Source: www.ohie.org)

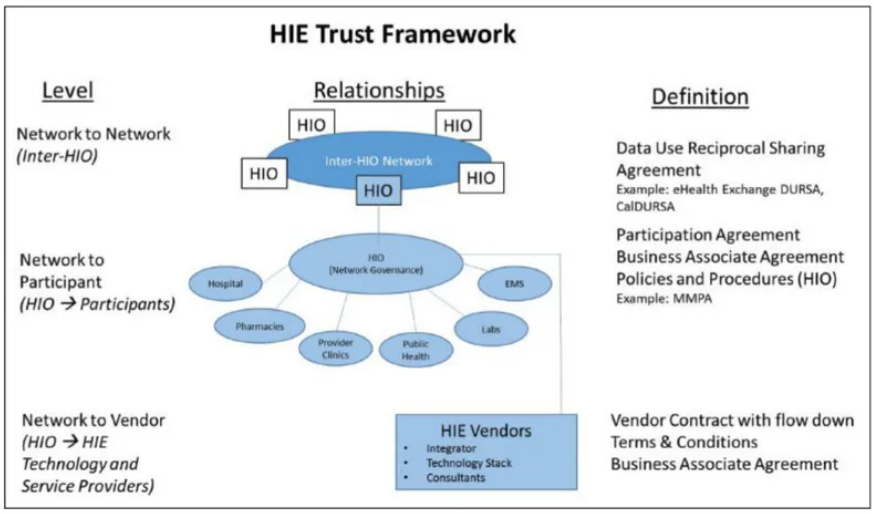


Figure 3 – Layers of trust for HIE

45 CFR §160.103.[1] The HIO manages a variety of health data sources and performs a broad range of value-added services through the HIE infrastructure that reflects the needs of its participants as shown in figure 2 (previous page).

A framework for trust

Sharing medical data, even for the same individual, can be complex. A patient receives routine care at a community clinic. Clinic staff want to access the patient's records at the local hospital but roadblocks around consent, authorization, and data sharing all stand in the way, making access to vital information difficult and time consuming. This is the scenario a trust framework is designed to prevent.

The end-to-end trust framework shown in figure 3 [5] has three levels:

- **Network to network**: establishes bilateral agreements between otherwise unaffiliated HIE networks or HIOs
- **Network to participant**: confirms relationships at the HIO level, between data providers and requestors with a common interest
- **Network to vendor**: defines the contractual relationships between an HIO and providers of HIE technology and services

Data use and reciprocal sharing agreement

Mutual data-sharing agreements are based on agreed-upon standards that encompass data governance, access, privacy, security, and intended use among other issues. Entities such as the California Trusted Exchange Network or eHealth Exchange connect individual data-sharing networks at the network-to-network level and have streamlined the process with model inter-HIO agreements, eliminating the "point-to-point" arrangement that becomes increasingly difficult, costly, and inefficient to maintain as participation increases.

A data use and reciprocal sharing agreement (DURSA) facilitates the bilateral exchange of data between individual HIO/HIE networks, overcoming differences in localized data access standards established by data providers and consumers. Without a DURSA, a data consumer/requester from one HIO may logically be denied access to a data provider from another HIO because the data provider's data access requirements, such as authentication level or minimum data policy, differ significantly from those of the consumer/requester.

A DURSA, as exemplified by the eHealth Exchange DURSA [13], assumes that each participating HIO has established relationships at the network-to-participant level, evidenced by existing end user trust or participation agreements that incorporate business associate agreements and policies and procedures applicable to that HIE network.

Participation agreements

A participation agreement defines the relationship between the HIO and its participants, outlining the terms of exchanging data between the HIE network members that share a common interest. The Model Modular Participants Agreement [3], developed by the California Office of Health Information Integrity, is an example designed to be easily tailored to meet both the governance structure and HIE technical architecture adopted by an HIO.[2]

Business associate agreements

Business associate agreements complicate the contractual landscape for health information exchange, especially as these agreements are not needed at all levels in a trust network.

A business associate agreement (BA agreement) is a written contract between a covered entity (CE) and its business associate (BA) that contains the mandatory and optional elements specified in 45 CFR 164.504(e). A BA agreement must also be established between a business associate and any of its subcontractors that may be exposed to PHI.

1 For the purposes of this article, the term "HIPAA" includes The Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), any other amendments to HIPAA, and all regulations under HIPAA.

2 An example of an executed HIE/HIO participation agreement based on a version of the MMPA can be found at http://www.redwoodMedNET.org/projects/hie/docs/rmn_participation_20100225.pdf.

Most HIO participants are either covered entities (i.e., a health plan, health care clearinghouse, or covered health care provider) or business associates of a covered entity.[1] While the US Department of Health & Human Services does not generally consider an HIO as a covered entity, it does consider it a business associate of its participants:

> "An HIO that performs certain functions or activities on behalf of, or provides certain services to, a covered entity which requires access to PHI would be a business associate under the Privacy Rule. See 45 C.F.R. § 160.103 (definition of "business associate"). [….] For instance, an HIO that manages the exchange of PHI through a network on behalf of multiple covered health care providers is a business associate of the covered providers, and thus, [according to 45 CFR §164.502(e)(1)(i)] one or more business associate agreements would need to be in place between the covered providers and the HIO."[14]

At the network-to-participant level, an HIO must enter into a business associate agreement with each participant that is either a covered entity or a business associate of one. An HIO normally provides a business associate agreement template as part of its draft participation agreement (PA). If the HIO allows unique tailoring of this template by its participants, it may be managing multiple agreements as part of its executed PAs.

At the network-to-vendor level, a HIO must enter into a BA agreement with all of its subcontractors, including the HIE technology vendors and service providers, that "create, receive, maintain, or transmit PHI on the [HIO]'s behalf." Per 45 CFR §164.502(e)(1)(ii) regarding disclosures to business associates, the HIO must obtain satisfactory assurance that its vendor will appropriately safeguard that PHI per a BA agreement compliant with 45 CFR §164.504(e)(1)(i). [2]

An important distinction, however, exists regarding the use of BA agreements at the network-to-network level. Here, the use of the agreement is not considered applicable because the relationship between the participating HIOs is bilateral. A BA agreement is intended to build a chain of trust that starts at a covered entity and extends downward to its business associates and their subcontractors. It is essentially unidirectional in nature. Rather than having an agreement between themselves, the HIOs act on behalf of their participants to facilitate inter-network exchange according to the data use and reciprocal sharing agreement (DURSA).

The approach taken in the eHealth Exchange DURSA is to restrict the exchange of information between two HIOs to a set of "permitted purposes" that include further limits to HIPAA treatment, payment, and operations; address public health activities and reporting; support/demonstrate the meaningful use of certified EHR technology, and accept uses and disclosures based on an individual's authorization.

This provides an effective escape clause from the need to execute BA agreements between HIOs in conjunction with the DURSA. Specifically, the DURSA is not intended to serve as an agreement among its participants as they are limited to exchanging information only for a permitted purpose, implying that participants do not need to become each other's business associate because of intent. The DURSA establishes HIPAA as a contractual standard of performance for participants that are not otherwise subject to HIPAA (e.g., covered entity, business associate of a covered entity, or governmental participant) [13].

Many healthcare covered entities leverage a BA agreement as a form of contractual service level agreement that addresses topics outside its regulatory purposes (i.e., the mandatory and optional BA agreement provisions laid out in 45 CFR §164.504(e)).[2] An HIO needs to evaluate provisions not required by HIPAA regulation that creep into a BA agreement. "BA agreement abuse" makes this contractual agreement a regulatory and contractual "kitchen sink," creating difficulty for an HIO to comprehend and manage its HIPAA contractual obligations, especially if an HIO has signed different BA agreements with multiple participants. [7]

An example potentially affecting the incident response professional is using this agreement to over-report incidents, often with unreasonable deadlines that are destructive to an effective working relationship between the HIO, its participants, and its vendors. While HIPAA requires a BA to report

both successful (e.g., breach) and unsuccessful incidents, it does not set time limits for such reporting, although governing or applicable law may have requirements. HIPAA does not require the same approach nor the same period for reporting successful versus unsuccessful incidents. An HIO should agree to report successful incidents promptly and in detail, while unsuccessful incidents can be aggregated and reported on in a periodic fashion.

The less that a BA agreement diverges from the mandatory requirements of the HIPAA rule, the easier it will be to administer. For agreements that diverge from the provisions laid out in HIPAA, legal counsel cannot easily rely on the regulation to clarify any interpretations for "consent," "authorization," or "breach," or help to clarify when a "security incident" is "discovered" or "should have been discovered."

The business associate agreement referenced in a trust framework should be attached to a parent agreement, such as a participation agreement or vendor contract, and be aligned with (not duplicate) the terms in that document. These parent documents must clearly establish the legal relationships between the parties according to the role and relationships involved. For example, a BA agreement might include terms around indemnification, not a HIPAA requirement. Addressing such terms and conditions in the related parent agreement (e.g., PA) allows a breach to be properly and consistently handled with all parties held responsible under terms applicable to their legal role and responsibilities in the HIE network.

Policy and procedures

A participation agreement normally incorporates HIO policies and procedures by reference, requiring terms to be "flowed down" to more operational artifacts. Two factors make developing a harmonized set of these policies and procedures across a data-sharing network a daunting task.

The first factor is the need to align HIO policies and procedures with the legal boundaries that each participant must comply with. Sections 15.01 and 15.05 of the eHealth Exchange DURSA require that the HIO "establish valid and enforceable agreements or user policies with participating organizations or users that comply with all applicable law."[13]

Within the United States, the HIPAA privacy and security rules provide a common floor for standard policies and practices governing the sharing of PHI, while state law may require more stringent controls around highly sensitive information, such as HIV/AIDS and mental health, or breach reporting.[5] An HIO should engage legal counsel to first evaluate and then keep abreast of the restrictions on privacy and security required by all elements of "applicable law."

The second factor is accommodating variation in definitions key to establishing the rules that govern how participants interact with the HIE network. The meaning of "administrator" for the HIE is not necessarily the same as for the hospital EHR that is providing or consuming data. Expectations related to authentication and authorization will also differ, making it difficult to smoothly map HIE role-based access controls across primary care providers and their behavioral health counterparts due to privacy and security concerns. An HIO must establish the proper level of actionable policy while attempting to harmonize these often disjointed elements [5].

Data, risk, policy, and governance

HIEs store and transact data in remotely-hosted or cloud-based environments, making it difficult to establish a hard network-based security perimeter. Data-oriented boundaries, such as the rules separating primary care information from highly sensitive behavioral health or substance abuse data, actually become the system boundaries in the world of health information exchange.

Data access rules go beyond a user's role and the classification of the data. For query-based exchange, the HIE must determine what results can be returned to an end user based not just user role and sensitivity of data, but on the patient's data sharing preferences as well. Only those data elements consistent with the patient's stored consent are to be shared. Consent management is an integral part of the HIE infrastructure. It is also complicated; a patient may have conflicting or overlapping consents if he has been seen by several providers throughout a community and for different reasons [5].

HIE policy development should be based on risk, but the assessment should be guided by different characteristics than a more traditional approach that encompasses physical controls and tangible critical assets such as servers and workstations. Rather, it must take into account the transaction patterns and permitted uses for the data, the complexities of data governance, and the HIE architecture (directed or query-based) that identifies threat-vulnerability pairs. Risk management should emphasize operational processes such as change management, incident response, and cyber defense as controls to mitigate concerns over privacy and security.

An HIO must establish operational procedures to ensure compliance with its policies, provide appropriate training, and require acknowledgment from its participants and their end users as to common terms and conditions before PHI is exchanged over the HIE network. Subsequent data governance must ensure that the terms and conditions of the trust framework and its agreements can be met, managed, and maintained.

What needs to be "tangible" to the end user, however, is the data that the HIE exchanges, how it is classified, and how it is used. A narrative description that tells a story familiar to its participants is often the best starting point for these activities. These scenarios can be decomposed into operational workflows using methods such as cross-functional or "swim lane" diagrams that help, at a minimum:

1. Identify participant roles that will access the data in the HIE
2. Describe edge systems (source and destination) that will provide and/or receive the data

Sponsorship information:
Monique dela Cruz
mdelacruz@issa.org

ISSA International CONFERENCE

3. Confirm the activities representing "permitted purpose" or "uses" align with trust framework agreements
4. Identify any potential vulnerabilities associated with process and data
5. Pinpoint any policies and procedures that need to be added or updated

Recommendations for the future

As healthcare moves further into the digital universe, the sharing of sensitive data across unaffiliated entities will not slow down. The rise of value-based incentives and population health demands that providers place trust in the validity, accuracy, and completeness of data. The following can help establish a trust framework needed for health information exchange:

1. Understand and resolve data governance gaps as the starting point to establish the trust required for exchange. This is perhaps the most difficult challenge to be faced by an HIO. Develop a library of possible use cases and use them to flag critical relationships between the principal actors, helping identify and prioritize the appropriate agreements needed.
2. Strive for consistency across all related documents and agreements, striving to ensure that the order of precedence across all related documents is clearly established. Evaluate all contractual relations with an emphasis on business associate agreements, keeping the agreement language as close to the mandatory and optional terms in the HIPAA Rule as possible.
3. Emphasize data and information in HIE risk assessment and management activities, balancing traditional privacy and security concerns with threats to data quality, usability, and integrity standards the HIO must uphold to meet safety concerns in patient care delivery.

Health information exchange requires a formal approach to governance that is truly holistically focused on privacy, security, and compliance. The resulting trust frameworks provide a foundation for other data-sharing efforts in health care, such as clinical trial networks where researchers, medical providers, and patients work towards new treatment options for improved clinical outcomes. The follow-on paper to this will detail some of the practical, technical considerations to execute and achieve trusted exchange.

Resources

1. 45 CFR 160.103. January 25, 2013. Accessed February 17, 2017. https://www.law.cornell.edu/cfr/text/45/160.103.
2. 45 CFR 164.502 . January 25, 2013. Accessed February 10, 2017. https://www.law.cornell.edu/cfr/text/45/164.502.
3. Boruff, Angela. "MMPA Release 2.2.1." CAHIE. April 1, 2014 – http://www.ca-hie.org/2014/04/mmpa-release-2-2-1/.
4. Dierker, Lynn. 2008. "State Connection: State-level Efforts in Health Information Exchange," Journel of AHIMA 40-43 – http://library.ahima.org/doc?oid=80242 - .WJ1N0o0m6Uk.
5. Filkins, Barbara. "Incident Handling in the Healthcare Cloud: Liquid Data and the Need for Adaptive Patient Consent Management," SANS, October 7, 2012 – https://www.sans.org/reading-room/whitepapers/hipaa/incident-handling-healthcare-cloud-liquid-data-adaptive-patient-consent-ma-34007.
6. —."Medical Data Sharing: Establishing Trust in Health Information Exchange." SANS, March 1, 2017 – https://www.sans.org/reading-room/whitepapers/hipaa/medical-data-sharing-establishing-trust-health-information-exchange-37657.
7. Hinkley, Gerry, and Allen Briskin. "Business Associate Obligations and Agreements: Aftermath of the HIPAA Omnibus Rule." Pillsbury Withrop Shaw Pittman LLP (2016) – https://www.pillsburylaw.com/en/news-and-insights/business-associate-obligations-and-agreements-aftermath-3-7-2017.html.
8. ISE, "Establishing Trust and Interoperability in the Information Sharing Environment," Information Sharing Environment" – https://www.ise.gov/mission-stories/standards-and-interoperability/establishing-trust-and-interoperability-information.
9. McCarthy, Jack. "A Guide to Interoperability at HIMSS17," Healthcare IT News, January 6, 2017 – http://www.healthcareitnews.com/news/guide-interoperability-himss17.
10. National HIE Governance Forum. "Trust Framework for Health Information Exchange," HealthIT, December 2013 – https://www.healthit.gov/sites/default/files/trustframeworkfinal.pdf.
11. The National Alliance for Health Information Technology. "Report to the Office of the National Coordinator for Health Information Technology." HITECH Answers, April 28, 2008 –http://www.hitechanswers.net/wp-content/uploads/2013/05/NAHIT-Definitions2008.pdf.
12. The Sequoia Project. "About the Sequoia Project," The Sequoia Project – http://sequoiaproject.org/about-us/.
13. —."Data Use and Reciprocal Support Agreement (DURSA)," the Sequoia Project (2017) – http://sequoiaproject.org/wp-content/uploads/2017/01/Restatement_I_of_the_DURSA_9.30.14_final.pdf?x54807.
14. US HHS. "Is a Health Information Organization (HIO) Covered by the HIPAA Privacy Rule?" US Department of Health & Human Services, December 15, 2009 – https://www.hhs.gov/hipaa/for-professionals/faq/559/is-an-hio-covered-by-hipaa/index.html.

About the Author

Barbara Filkins, an (ISC)² member and a 2017 SANS Technology Institute graduate, has been deeply involved with healthcare privacy and security issues for 20+ years. A member of the California Associations of HIEs, she is currently helping set policy at the state and community levels for health exchange. She can be contacted via filkins@impulse.net or LinkedIn.

ISSA DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Leveraging a Control-Based Framework to Simplify the Risk Analysis Process

By Bryan S. Cline – ISSA member, North Texas Chapter

In this article, the author discusses HIPAA risk analysis, its purpose, and how a controls-based risk management framework can be leveraged to satisfy due diligence and due care obligations and comply with HIPAA.

Abstract

The risk analysis required by the HIPAA Security Rule is perhaps one of the most difficult for many healthcare entities to address, especially smaller ones like physician practices. Why? Most simply do not have the expertise and often lack the funding necessary to hire a professional services firm. However, there is another approach that is easy to adopt and readily available—a framework-based approach. In this article, the author discusses the HIPAA risk analysis, its purpose, and how a controls-based risk management framework can be leveraged to satisfy due diligence and due care obligations and comply with HIPAA.

Compliance with the Health Insurance Portability and Accountability Act [7] (HIPAA) Security Rule[1] (the Rule) is arguably *the* principle driver for many organizations in the healthcare industry to implement the technical, physical, and administrative controls necessary to safeguard patient health information. However, the Rule's standards and implementation specifications for these controls generally lack the specificity required for uniform implementation across the industry; nor are they comprehensive enough to ensure adequate protection of sensitive health systems and information in an ever-changing threat environment.

Fortunately, the Rule also requires healthcare organizations[2] to conduct a risk analysis: "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information"[3] … [to] "protect against any reasonably anticipated threats or hazards to the security or integrity of such information."[4] Such a risk analysis would help organizations determine the specific safeguards they should implement to protect patient health information, regardless of what may or may not be specified in the Rule.

Unfortunately, however, the risk analysis requirement has proven problematic for many healthcare organizations. The Office of Civil Rights (OCR) cited an incomplete or inaccurate risk analysis for fully two-thirds of the organizations evaluated against the first OCR audit protocol [15], conducted as part of a program mandated under the Health Information Technology for Economic and Clinical Health (HITECH) Act [8].

Risk analysis

To understand why the HIPAA risk analysis requirement is so difficult for these healthcare organizations, one only needs to look at a typical risk analysis process as depicted in figure 1, consistent with the Rule's legislative language.

1 See 45 CFR Part 164

2 Covered entities and their business associates, as defined in 45 CFR § 164.102

3 See 45 CFR § 164.308(a)(1)

4 See 45 CFR § 164.306(a)(2)

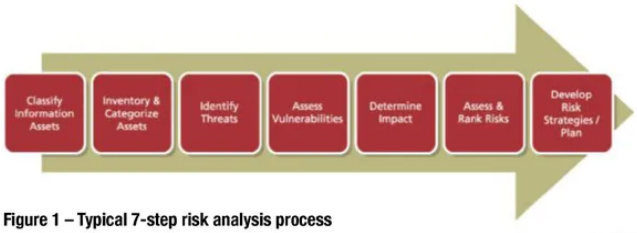


Figure 1 – Typical 7-step risk analysis process

With an asset-based approach to information protection, an organization must first determine its information protection needs and then inventory and categorize the information assets that require protection. While no easy feat, the next three steps—threat, vulnerability, and impact analysis—are even more difficult for many healthcare organizations due to a lack of skilled resources or, as in the case of many smaller organizations such as physician practices and clinics, the budget needed to outsource the analysis to a third-party consultant or professional services firm. Consider threat identification, for example. There is no generally accepted list of common threats to healthcare organizations, and resources that provide more general threat information are generally inconsistent with one another (e.g., the *Bundesamt fur Sicherheit in der Informatiionstechnik (BSI) IT-Grundschut-Catalogues* [1] and the European Union Agency for Network and Information Security (ENISA) "Threat Taxonomy" [5]) or incomplete (e.g., NIST SP 800-30 [11]). The final few steps involve calculating the risk, ranking the risks in order of severity, and developing an overall strategy to address the risks, which generally involves avoidance, acceptance, transfer, and mitigation.

The US Department of Health and Human Services (HHS) takes a slightly different approach by incorporating a controls gap analysis in the risk analysis process [6]. This approach presumes organizations already have at least some security controls in place before conducting their first analysis, but a complete set of security controls must still be specified. HHS includes this control specification in the last step along with specific remediation plans based on the control gap analysis.

Risk analysis in the risk management process

The risk management process can be represented by a general four-step process model [2] as shown in figure 2, which includes identifying risks and information protection requirements, specifying controls, implementing and managing controls, and assessing and reporting on the controls.

This first step is essentially the risk analysis process described earlier. But whether control specification occurs at the end of the risk analysis—as in the HHS model—or just after the risk analysis in the model presented here, control specification follows information classification, asset categorization, threat analysis, vulnerability analysis, and the calculation, ranking and treatment of risk (figure 3).

Figure 3 – Custom control specification based on the risk analysis process

Framework-based risk analysis

The National Institute of Technology and Standards (NIST), while taking a similar approach to risk analysis as the HHS[5] [12], specifies a slightly different risk management approach with their six-step model [13] depicted in figure 4.

5 The federal government considers the terms *risk analysis* and *risk assessment* synonymous.

Figure 2 – General four-step risk management process

Figure 4 – NIST six-step risk management model

Rather than perform the type of risk analysis first described, federal agencies categorize their information systems based on a more limited analysis focused on identifying "one of three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability)" [10]. Agencies then simply select a security control baseline appropriate for the categorization.

Figure 5 – Risk analysis supporting specification of the nist minimum security control baselines

This is possible because major elements of the risk analysis have already been performed. For all intents and purposes, NIST conducted a *general* risk analysis of a *typical* federal agency with *typical* threats to *typical* vulnerabilities of *typical* information assets, and specified three security control baselines to address three levels of risk. The risk level—and subsequently the control baseline that should be selected—is determined when an agency categorizes the impact of a potential breach as *low, moderate* or *high*.[6] This greatly simplifies the risk analysis process for federal agencies (see figure 5) and provides an "80 percent solution" for control specification.[7]

Agencies are then expected to further tailor the baseline to ensure their unique information protection requirements are addressed. The tailoring process[8] includes additional scoping to eliminate unnecessary controls, selecting compensating controls, assigning parameters for organization-defined parameters, adding controls and enhancements, and providing any additional information required for control implementation. This process can be used very granularly on a specific system or organizational element, or it can be used to create an overlay for general use, such as a general type of information system or organization.

Applying a framework-based approach to healthcare

Healthcare organizations can create their own overlay of a NIST SP 800-53 baseline by going through the tailoring process. While daunting for some organizations, it is arguably a more tractable approach than specifying a complete set of security controls based on a traditional risk analysis.

1. First, **scale the controls by selecting an appropriate baseline from which to begin.** This helps ensure time and effort is not wasted on implementing controls that aren't necessary for the level of risk mitigation required.
2. Second, **scope the scaled baseline by adding or enhancing controls,** as needed, to address applicable regulatory, legal, contractual, and other business-related requirements unique to your organization. Controls may also be removed based on organizational and financial constraints; however, no control should be removed simply as a matter of convenience.
3. Third, **specify compensating controls for baseline controls that cannot be implemented**, e.g., due to technical, architectural, or financial reasons. Ensure the compensating controls address a similar type and amount of risk as the baseline controls.
4. Fourth, **continue the tailoring process by reviewing the organization-defined parameters** to ensure the values are consistent with best practices and industry due care and due diligence requirements.
5. And finally, **review the resulting overlay periodically**, or otherwise as needed, to ensure the overlay continues to address extant and emerging threats to your information assets.

The healthcare industry already leverages the overlay concept to great benefit. For example, the Centers for Medicare and Medicaid Services (CMS) produces an overlay of all three NIST SP 800-53 control baselines for their use and that of their contractors [4]. CMS also produces a separate overlay of the NIST SP 800-53 moderate control baseline for Health Insurance Exchanges [3]. And the Health Information Trust (HITRUST) Alliance produces an overlay of the NIST moderate baseline for the industry and incorporates mechanisms to help further tailor the overlay to an organizational type based on defined risk factors [9]. This approach is also used as the basis for Healthcare and Public Health Sector guidance [16] on implementing the NIST Cybersecurity Framework [14], published under the auspices of the Critical Infrastructure Protection Program.[9]

Conclusion

Findings from the first round of OCR audits clearly indicate a traditional approach to risk analysis is difficult for many healthcare organizations. However, a controls-based framework such as the one provided by NIST can be leveraged by both public and private sector organizations to greatly simplify the risk analysis process. Such an approach helps ensure specification of a comprehensive and robust set of information security controls that complies with the HIPAA Security

6 Categorization is determined by the greatest impact to the organization from a loss of confidentiality, integrity, and availability (referred to as the "high-water mark").

7 In the vein of the "80/20" or Pareto Rule, organizations can obtain a minimum security control baseline that will address a majority (80%) of its risks for a relatively small (20%) effort from categorizing its information and information system(s).

8 The tailoring process, including in the development of overlays, is discussed extensively in NIST SP 800-53, Chapter 3.

9 Sector guidance was developed and published by the Joint HPH Cybersecurity Working Group, as chartered by the Critical Infrastructure Protection Advisory Council. For more information, see https://www.dhs.gov/critical-infrastructure-sector-partnerships.

Rule and, more importantly, helps satisfy due care and due diligence obligations for the protection of sensitive patient health information.

References

1. Bundesamt fur Sicherheit in der Informatiionstechnik, BSI. 2013, "IT-Grundschutz-Catalogues, Version 13." Bonn, GE – https://download.gsb.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf.
2. Cline, Bryan. "Risk Analysis Guide for HITRUST Organizations and Assessors," HITRUST (2017) – https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf.
3. CMS 2015, "Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges." MARS-E Document Suite, Version 2.0, Centers for Medicare and Medicaid Services, Baltimore, MD (2015) –https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-11102015.pdf.
4. —2017, "CMS Acceptable Risk Safeguards (ARS)." CMS_CIO-STD-SEC01-3.0, Centers for Medicare and Medicaid Services, Baltimore, MD (2017) – https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-30-Publication.html.
5. ENISA. "ENISA Threat Taxonomy, " European Union Agency for Network and Information Security, Heraklion, GR (2016) – https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information.
6. HHS, "Guidance on Risk Analysis under the HIPAA Security Rule," US Department of Health and Human Services (2010) – https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf?language=es.
7. HIPAA, "The Health Insurance Portability and Accountability Act of 1996," Public Law 104-191, U.S. Statutes at Large 110 (1996): 1936-2103 – https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.
8. HITECH, "The Health Information Technology for Economic and Clinical Health Act," Public Law 11-5, U.S. Statutes at Large 123 (2009): 226-279 – https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.
9. HITRUST, "HITRUST CSF Version 8.1," Health Information Trust Alliance, Frisco, TX (2017) – https://hitrustalliance.net/csf-license-agreement/.
10. NIST 2004, "Standards for Security Categorization of Federal Information and Information Systems," FIPS Pub 199, National Institute of Standards and Technology, Gaithersburg, MD (2004) – http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.
11. —2012, "Guide for Conducting Risk Assessments," NIST SP 800-30, Revision 1, National Institute of Standards and Technology, Gaithersburg, MD (2012) – http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.
12. —2013, "Glossary of Key Information Security Terms." NISTIR 7298 Revision 2, National Institute of Standards and Technology, Gaithersburg, MD (2013) – http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.
13. —2013, "Security and Privacy Controls for Federal Information Systems and Organizations," NIST SP 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, MD (2013) – http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
14. —2014, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.0." National Institute of Standards and Technology, Gaithersburg, MD (2014) – https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
15. Sanches, Linda. 2012. "2012 HIPAA Privacy and Security Audits,"2012 NIST-OCR HIPAA Security Conference – http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-2_lsanches_ocr-audit.pdf.
16. US-CERT, "Healthcare Sector Cybersecurity Framework Implementation Guide." Critical Infrastructure Protection Advisory Council, Joint Healthcare and Public Health Cybersecurity Working Group (2016 – https://www.us-cert.gov/ccubedvp/cybersecurity-framework#framework-guidance.

About the Author

Bryan Cline, Ph.D., is a former CISO with 30 years of experience in information systems and cybersecurity in the public and private sectors. Cline is a private sector co-chair of the Joint HPH Cybersecurity WG, which produced the CIPAC-sponsored guidance on implementing the NIST Cybersecurity Framework in healthcare. He may be reached at bryan.cline@csps-infoprotect.com or @IA_Doctor.

Looking Ahead – December Journal

Social Media, Gaming, and Security; Due: 10/22/17

Based on 2016 statistics, 155 million Americans play online games regularly and 78 percent of the population has a social networking profile. With staggering numbers like this, these industries will probably thrive for the foreseeable future. Being interconnected with others in the community and around the world through these vehicles can be exciting but also poses numerous risks such as predators, addiction, identity theft, malware intrusion, and social engineering.

These issues require both the vendors and consumers to become more vigilant to effectively protect themselves. Furthermore, tackling them can be complicated and time consuming and will inevitably impact this landscape. What research, experience, or best practices do you have to share in this area? The ISSA Journal is interested in hearing from you.

Submit articles to editor@issa.org.