Legislation and the Negative Impact on Cybersecurity in Healthcare

Jesse Daniels and Sajal Bhatia*
School of Computer Science and Engineering, Sacred Heart University, Fairfield, CT, U.S.A.

Keywords: Healthcare, Regulation, Security, Privacy, HIPAA, Stark Law, HITECH, Legislation, Medical Devices, FDA.

Abstract: Healthcare is a rapidly growing industry that is continuously expanding with technological advances. Similar to many other critical industries, healthcare faces an onslaught of daily cybersecurity challenges, however is largely at a disadvantage due to outdated and antiquated legislation. As of 2019, no legislation or regulatory body in healthcare adequately cover the needs of cybersecurity. However, regulations have forced healthcare to deploy technology at an expansive rate as well as having them deploy FDA, a regulatory body, approved medical devices from the assembly line that are inherently insecure. By looking at reported incidents, the authors will examine modifications to legislation in healthcare and the impact on cybersecurity-related events facing the organizational vertical. Legislation such as the Ethics in Patient Referrals Act of 1989 adversely impacts healthcare as cybersecurity is not considered a "service," and as such, cannot be shared between two healthcare organizations. By bringing light to the inadequacies of cybersecurity in legislation and regulation of the United States healthcare system, the paper aim to bring cybersecurity to the forefront of future legislation and regulation.

1 INTRODUCTION

On Friday May 12^{th}, 2017, using leaked National Security Agency exploits, the National Health Service of the United Kingdom saw a ransomware attack that cost the organization £20 million ($25 million USD) in one week. The incident cost a total of £92 million ($115 million USD), while over 19,000 patient appointments were canceled (Field, 2018). The authors wanted to examine the correlation between the increase in cybersecurity events seen in healthcare and the regulations this industry faces. According to Beazley Breach Response, 41 percent of all cyber-related incidents tracked are from healthcare organizations, while the financial sector is a distant second at 20 percent (Beazley, 2019).

Healthcare is one of the most vital functions of society across the developed and underdeveloped world. According to CDC, 883.7 million patients visited Ambulatory Care Use and Physician office visits during 2018 (for Disease Control and Prevention, 2018) who could possibly be data breach victim. We hope that our loved ones can receive the care they need when in these facilities, but as of late the number of cybersecurity events have risen across the globe. We have seen ransomware close healthcare facilities and cause patients to seek treatment in other healthcare facilities. In 2017 the National Health Services of the United Kingdom was forced to turn away and reschedule 19,000 patients. While National Health Service representatives state no patients died during this incident, an attack of this magnitude has the massive potential to disrupt patient care, and cause harm to life (Field, 2018).

A multitude of cybersecurity threats face healthcare facilities all across the world. The most common forms of compromise are: insider threats, business email compromise, phishing, DDoS attacks, data breaches, ransomware, mobile devices, rise of the cloud, online file-sharing, encryption blind spots.

These threats are not unique to healthcare; however, they produce an array of new challenges in the healthcare arena. Unlike other sectors , there is an additional vulnerability in healthcare. Legislation and regulation have caused healthcare to have a poor cybersecurity posture. Hospitals have been forced to deploy technology at a rapid pace in an effort to not lose Medicare and Medicaid reimbursement. After the rapid implementation of Electronic Health Record systems, multiple organizations reported that during unexpected downtime of Electronic Health Record systems "an unexpected theme that emerged during the interviews was how essential tenured staff was to the organizational response and recovery from the at-

* Corresponding author.

Daniels, J. and Bhatia, S.
Legislation and the Negative Impact on Cybersecurity in Healthcare.
DOI: 10.5220/0009157906910697
In *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)*, pages 691-697
ISBN: 978-989-758-399-5; ISSN: 2184-4356

tack. This theme was mentioned by at least one stakeholder from all three facilities. The participants explained that staff who had been in healthcare longer were able to shift back to pen and paper records much easier than newer staff. This group of individuals had experience with paper charting during their careers. In contrast, the participants mentioned the hard time that younger staff had with switching back to paper charts" (Branch, 2018).

Security rules written into legislation are sixteen years old, and medical devices are the "wild west" of security flaws. This begs the question of what have lawmakers and policymakers done in the wake of the significant rise in attacks on the healthcare industry? Well, the answer is quite simple- nothing.

The main contributions of this position paper are to unpack the negative consequences that legislation and regulation produce in the cybersecurity of healthcare. The authors feel that legislation such as HIPAA, HITECH, and the Stark Law have inherently created a state of disrepair in healthcare cybersecurity. By bringing to light these legal inadequacies, the authors would like to see future legislation consider potential cybersecurity ramifications moving forward.

Rest of the paper is organized as follows: Section 2 summarized the recent security breaches and events in healthcare. Section 3 gives an overview of the Stark Law which is intended to prevent physician self-referral; however, this legislation prevents the donation of cybersecurity goods and services to other healthcare facilities. Section 4 presents the HIPAA healthcare privacy and accountability legislation, while unpacking the lack of updates to the Security Rule. Section 5 delves into the HITECH legislation which is directly attached to the adoption rate of technology in the healthcare sector. Section 6 makes reference to the U.S. Food and Drug Administrations regulations on medical devices, causing inherent vulnerabilities in the ever increasing interconnected healthcare environment. Section 7 summarizes the paper and gives directions for future research work in this area.

2 RECENT CYBERSECURITY EVENTS IN HEALTHCARE

Healthcare has been under siege by cyber adversaries for years. According to the Office of Civil Rights (OCR), in 2014, there were 31 hacking incidents in healthcare affecting 1,786,630 individuals (Bitglass, 2016). By 2015 56 hacking incidents affected 111,803,342 individuals, as shown in Figure 1. Figure 2 shows individuals affected by breach incident type for 2014 and 2015 (Bitglass, 2016).

Type of Breach	Individuals Affected **2014**	Individuals Affected **2015**
Hacking or IT Incident	1,786,630	111,803,342
Loss or Theft	7,273,157	750,802
Other	3,504,350	646,243
Total Individuals Affected	**12,564,137**	**113,200,387**

Figure 1: Bitglass Healthcare Breach Report 2016 (Bitglass, 2016).

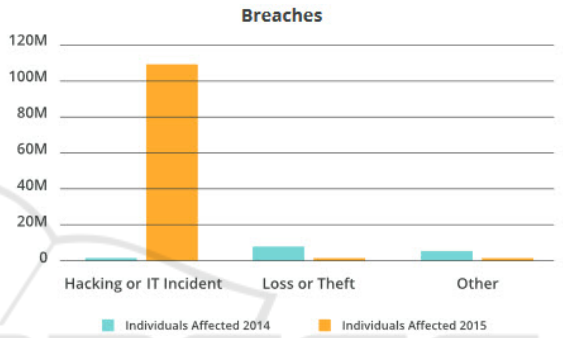

Figure 2: Bitglass Healthcare Breach Report 2016.

According to the Office of Civil Rights, which is required to post breaches affecting 500 individuals or more, 12,385,888 individual records became compromised due to hacking/IT incidents from healthcare providers between November of 2017 and November of 2019. The largest of these breaches submitted to the Office of Civil Rights occurred on July 13^{th}, 2019 when a staggering 10,251,784 individual records were stolen after Laboratory Corporation of America Holdings dba LabCorp was hacked (OCR, 2019). Figure 3 shows the total individual affected between 2017 and 2019 according to the OCR (OCR, 2019).

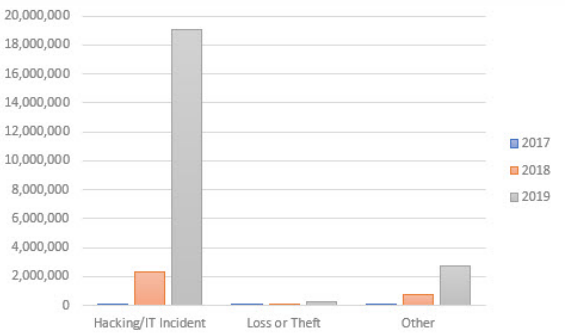

Figure 3: OCR Breaches of healthcare providers between 2017 and 2019.

In 2016 we saw the rise of ransomware attacks against healthcare facilities. On February 5^{th}, 2016 Hollywood Presbyterian Medical Center staff reported that they were unable to access electronic resources. Their network had become infected with the ransomware Locky, and the malicious actors were demanding 40 Bitcoin, worth approximately $17,000 at the time of the event (Winton, 2016). A study regarding ransomware and cryptocurrencies determined "that the ransomware family that generated the largest direct financial impact in our data-set is Locky, which received payments totaling $7,834737.00 USD" (Paquet-Clouston et al., 2019).

During this incident, doctors reported the inability to access patient medical histories, share medical imaging, and access test results. Several patients were also diverted to nearby hospitals for treatment. Hollywood Presbyterian Medical Center paid the demanded ransom and reported that services were restored ten days later on February 15^{th}; however, the damage to the hospital's system and reputation in the public eye remained (Winton, 2016). Figure 4 shows the total payments received by the top 15 ransomware families (Paquet-Clouston et al., 2019).

Family	Addresses	BTC	USD
Locky	6827	15 399.01	7 834 737
CryptXXX	1304	3339.68	1 878 696
DMALockerv3	147	1505.78	1 500 630
SamSam	41	632.01	599 687
CryptoLocker	944	1511.71	519 991
GlobeImposter	1	96.94	116 014
WannaCry	6	55.34	102 703
CryptoTorLocker2015	94	246.32	67 221
APT	2	36.07	31 971
NoobCrypt	17	54.34	25 080
Globe	49	33.03	24 319
Globev3	18	14.34	16 008
EDA2	23	7.1	15 111
NotPetya	1	4.39	11 458
Razy	1	10.75	8073

Figure 4: Received payments per ransom family (Top 15).

Just one month after the events in California, The Ottawa Hospital was infected with a variant of Cryptolocker in March of 2016. Fortunately, The Ottawa Hospital had sufficient backup and restoration processes in place to bring their systems back online without paying the ransom fee. The Ottawa Hospital stated that four systems out of 9,800 were affected (Spence et al., 2017).

One year later in March of 2017, we saw the rapid spread of WannaCry. This ransomware attack was the most significant cyberattack against the healthcare industry. As a result, the National Health Services of the United Kingdom had services wholly disrupted. During this incident, 19,000 patients were impacted as medical services were disrupted and thousands of appointments were canceled and rescheduled. The Department of Health in the United Kingdom estimated that the total financial cost of the Wannacry event cost £92 million ($115 Million USD) (Field, 2018).

The year of 2019 started with UCONN Health in Connecticut reporting that 326,000 patient records became breached after a cyber-attack. While conducting its incident response investigation, the health system had determined that an unauthorized third party had accessed various employee email accounts. UCONN Health manually reviewed 285,000 emails and attachments to find what patients and which information became breached. Patients were notified roughly six months after the breach occurred in late 2018 (Davis, 2019b). The simplicity of phishing is an easy way to bait healthcare employees to submit their valid credentials to malicious actors. In a recent study, ten major incidents were found where phishing allowed unauthorized access to patient records. The research found that 74,910 individuals had their Personally Identifiable Information (PII) breached (Wright et al., 2016).

In summary, an ever increasing trend can be seen in Protected Health Information(PHI) breaches caused by "Hacking or IT Incident". The authors begin dissecting legislation in Section 3 to see the adverse affects of legislation on healthcare cybersecurity.

3 THE "TONY" STARK LAW

The United States Omnibus Budget Reconciliation Act of 1990 included a bill entitled "Ethics in Patient Referrals Act." The law would become commonly referred to as "Stark I" in the namesake of the primary author United States Congressman Pete Stark, D-CA. The United States Omnibus Budget Reconciliation Act of 1993 would see amendments added to the original Stark Law, which was later coined "Stark II" (Salcido, 2000)

The initial motivator behind the Stark Law was to prevent physician self-referral. The primary concern was physicians ordering unnecessary testing by referring patients to testing centers to which they had a financial relationship. While this bill intended to keep the cost of health services down, it inherently created an issue before the Internet, and Electronic Medical Record systems were in extensive use.

The Stark Law states that a healthcare facility cannot provide services or goods to a physician practice without charging "fair market value." Exceptions were made in 2006 to allow healthcare facili-

ties to "donate" EMRs to physician practices, but no clauses were added for cybersecurity and computer-related technology. Under the current Stark Law, a facility upgrading to a more extensive firewall that did not have end of life products could not donate their old infrastructure to a facility in need. By not allowing smaller practices that interconnect with more extensive facilities appropriate access to cybersecurity-related hardware and software, the healthcare sector is inherently less secure.

4 LET'S TALK ABOUT THE HIPAA IN THE ROOM

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was signed into law by former United States President Bill Clinton on August 21st, 1996. The primary intention of HIPAA was to protect Personally Identifiable Information (PII), and to prevent fraud and theft while allowing individuals to request a copy of their medical records. On February 20^{th} 2003, the Final Rule on Security Standards was added to HIPAA. The Security Rule was designed to complement the Privacy Rule by explaining how Electronic Protected Health Information (EPHI) is managed and maintained. Components of the Security Rule include Administrative Safeguards, Physical Safeguards, and Technical Safeguards were components of the Security Rule (Assistance, 2003).

The Technical Safeguards implemented by the Security Rule boil down to the following:

- Systems containing PHI have protections in place to prevent intrusion.
- Explaining the encryption requirement for electronically transmitting PHI over open networks.
- A covered entity must ensure data integrity and prevent data manipulation.
- Entities must maintain access records providing authentication.

Since this amendment, HIPAA was modified one last time in 2013 with the Final Omnibus Rule Update. This juncture in time would have been an opportune point in time to add regulations regarding cybersecurity. Instead, it added the requirement to report breaches to the Office of Civil Rights, implemented severe penalties for violations of privacy and allowed waving of the HIPAA Privacy Rule during a natural disaster.

During the ten years between the two amendments, several cybersecurity events have happened, which should highlight the need to implement some form of cybersecurity standards.

- 2003 - The Slammer worm begins to spread to SQL servers quickly.
- 2004 - MyDoom quickly develops as one of the fastest spreading mass-mailer worms.
- 2005 - The Gpcoder Trojan is discovered, which encrypts data files and requires a $200 payment for the decoder.
- 2006 - A Veterans Affairs Department employee loses a laptop with the PII of 26.5 million active-duty troops and veterans.
- 2007 - The FBI finds over 1 million botnet victims.
- 2008 - The United States was a victim of a cyber-attack when an infected USB drive was left in the parking lot of a Department of Defense facility in the Middle East.
- 2009 - The Conficker worm rapidly spreads infecting millions of PCs worldwide.
- 2010 - The discovery of the first cyber weapon Stuxnet targets Iran's nuclear facilities.
- 2011 - Sony's PlayStation Network is breached and goes offline. The total of individuals affected by the PII breach was approximately 77 million.
- 2012 - LinkedIn is hacked, and 6.5 million user accounts and passwords were stolen.
- 2013 - Tumblr is hacked, and over 65 million unique emails and passwords were leaked.

While these significant cybersecurity events happened, the Security Rule in HIPAA was written at a period where Windows XP Service Pack 1 was only one year old. As highlighted in Section 7, the authors would like to see Security Rule reviewed and amended annually, to encompass the latest innovations in technology, while ensuring lessons from major cybersecurity events are taken into consideration.

5 HITECH HIT BY LOW TECH EXPLOITS

During the recession of 2009, former United States President Barack Obama signed the American Recovery and Reinvestment Act of 2009 into law. Inside this piece of legislation was the Health Information Technology for Economic and Clinical Health Act (HITECH). The HITECH Act was enacted to have healthcare facilities implement an Electronic Health Record (EHR) system to promote interoperability

amongst healthcare facilities. The intended direction was to make healthcare facilities use a certified EHR and provide "Meaningful Use," such as e-prescribing. As part of the Obama Administration, this was an attempt to provide a stimulus to the healthcare field. HITECH authorized up to $27 billion in Medicare and Medicaid payments over the next decade to providers who implemented an EHR and met the Meaningful Use requirements (DesRoches et al., 2013).

Starting in 2011 and for the next six years, providers who adopted an EHR successfully received a promised maximum incentive for $63,750 per year from Medicaid. The EHR system had to be implemented by 2016 to qualify for this program. Medicare offered a maximum payment of $44,000 over the next five years. Any facility that did not implement an EHR by 2015 would be penalized 1% of Medicare payments with the penalty increasing to 3% over the next three years (DesRoches et al., 2013). With the incentive of being rewarded with grant and loan money, healthcare facilities began to quickly and rapidly adopt EHR. The monetary penalties of not having an EHR for Medicare and Medicaid reimbursement also impacted the haste in which EHRs became implemented by healthcare facilities.

According to the Office of the National Health Coordinator for Health Information Technology, in 2009 12.2% of non-Federal acute care hospitals had a basic EHR. In the year 2012, the number of non-Federal acute care hospitals with a basic EHR jumped to 44.4%. Of these deployments, 85.2% qualified as a certified EHR. In just three years, there was over a 300% increase in implementing an EHR. By 2015 this number jumped to 83.8% in the ever-increasing demand to implement an EHR before the penalties of Medicare reimbursements (Henry et al., 2016).

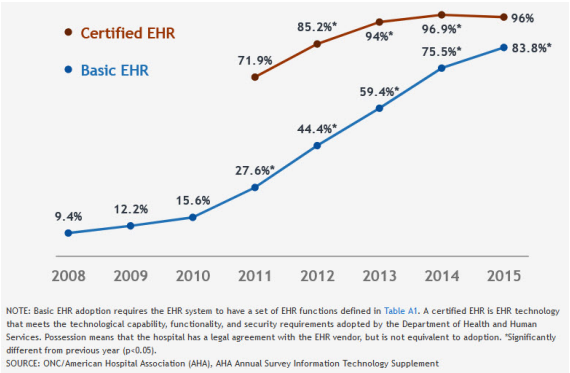

Figure 5: Non-Federal acute care hospitals with adoption of at least a Basic EHR.

Figure 5 Percent of non-Federal acute care hospitals with adoption of at least a Basic EHR with notes system and possession of a certified EHR: 2008-2015 (Henry et al., 2016).

While the implementation of EHR for interoperability is fantastic, the pace at which healthcare was forced to implement these systems meant some corners had to be cut. Many health systems could not afford an EHR, which is why only 12.2% of non-Federal acute care hospitals had an EHR before the enactment of HITECH (Henry et al., 2016). Unfortunately, security was not on the agenda of things to implement. Due to time restrictions, getting an EHR running was more imperative than appropriately implementing it with proper security controls.

According to research conducted by Texas State University in 2016, it affirmed that cybersecurity attacks on healthcare were up 125% since 2010. They found that healthcare organizations spent around 95% of their Information Technology budget on implementation and adoption, yet spent only the remaining 5% on information security. Due to the rapid technological advancements by federal policy initiatives, the healthcare sector has become the number one target of cyberattacks (Kruse et al., 2017).

One of the reason that healthcare is such a lucrative industry to attack is because of the content of medical records. A medical record contains Social Security Numbers, addresses, phone numbers, and insurance information. Unlike stolen financial data, one cannot put a freeze on their medical record or request a new medical record number. A complete medical record sells for an average on $50 on the black market (Le Bris and El Asri, 2006). Due to the sensitive information contained in a full medical record there are various forms of fraud that can be committed. With ones Social Security Number, malicious actors could open and create new lines of credit under a persons identity. With their full address information they can fully compromise their identity. By having access to their medical history and insurance information, malicious actors could use this as a method for prescription or healthcare fraud. One aspect that often goes overlooked, what will happen when the lose of protected health information causes death. While there are no reported cases, what could the opposition of a nation state gain by knowing what medications another world leader is allergic to? Will it take this lose of life before cybersecurity legislation in healthcare is taken seriously?

6 FDA (FAULTY DEVICE ARRIVED) MEDICAL DEVICES

The greatest threat facing healthcare facilities are networks of interconnected medical devices that are inherently vulnerable. These devices are crucial in patient care and could mean the difference between life and death. Such devices are diagnostic devices such as a MRI machine, infusion pumps, life support equipment, and medical monitors such as a electroencephalogram (EEG), laboratory analyzers, or insulin pumps.

In 2011 Barnaby Michael Douglas Jack showed the first exploit of a medical device at McAfee FOCUS 11 when he was able to have an insulin pump deliver the maximum dose of 25 units until all 300 units had dispensed into a test dummy. A dosage of 10 units is enough to send an average diabetic patient to the hospital. An insulin unit containing 300 units should provide a patient three to four days worth of insulin supplies (Viega and Thompson, 2012).

At the RSA Security Conference the following year, Barnaby Jack was able to once more wirelessly hack an insulin pump from 90 meters away using high-gain antenna. Later in 2012, Barnaby Jack was able to demonstrate the ability to hack a pacemaker (Viega and Thompson, 2012). He was due to present his hacking of pacemakers at Black Hat 2013, but was unfortunately found unresponsive in his apartment and pronounced dead (Leyden, 2014). While we lost one of the pioneers in medical device exploitation, Barnaby Jack highlighted just how vulnerable these devices are. Unfortunately, since Barnaby Jack highlighted the weaknesses in medical devices, security regarding them has not improved.

The United States has put the U.S. Food and Drug Administration (FDA) in charge of regulating the sale of medical device products in the United States. With the adoption rate of technology after HITECH became established, medical devices have gone from stand-alone devices to networked devices. On December 27th 2016 the FDA released its "Final Guidance: Postmarket Management of Cybersecurity in Medical Devices." Across the top of every page it states "Contains Nonbinding Recommendations" (FDA, 2016). The organization that should be assisting in securing medical devices can only make recommendations that they feel are nonbinding.

The FDA states in these nonbinding agreements that patches and update plans need to be submitted to the FDA for review. In the field of cybersecurity, patches and updates are one of the best defenses we have, especially when critical vulnerabilities such as EternalBlue or BlueKeep become commonplace. With monthly patches coming out for Microsoft Windows, it is an impossible task to re-certify every medical device monthly. The gap in patch release to deployment is immense. If there is a patch for a medical device, the vendor must perform engineering analysis before it can be submitted to the FDA for verification and validation. After release, testing must be done to ensure that target environments will not produce a negative impact on patient safety or workflows. Once completed, the deployment of the roll-out across all the vendor's customers and products must begin. This complete process can take months to patch one critical vulnerability, which is unacceptable when lives are on the line (Williams and Woodward, 2015).

7 CONCLUSION AND FUTURE WORK

As per our research, and experiences the authors have found that as healthcare becomes more interconnected and reliant on technology, cybersecurity needs to become a priority in future legislation. The current legislation and regulations that the United States has enacted on healthcare have inherently weakened the sector in cybersecurity. Healthcare has been forced to implement technology at a rapid pace to avoid financial penalties. Regulations on medical devices cause a direct hindrance to the process of securing medical devices, putting lives at risk.

The authors would like to see modifications to current legislation that adequately encompasses the needs of cybersecurity in healthcare. HIPAA, which intended to protect patient privacy and data, has not seen an update to the Security Rule since 2003. While HIPAA does not dictate security software or technology, rather patient privacy, the authors would like to see the Security Rule reviewed and amended annually, to encompass the latest innovations in technology, while ensuring lessons from major cybersecurity events are taken into consideration. When the Security Rule was authored, it stated that computer drives containing E-PHI should be destroyed using a "reasonable" method. With the advent of Solid State Drives what is considered "reasonable"? Future legislation such as HITECH that forces technology upon organizations should look at cybersecurity-related ramifications before enactment. We cannot legislate technology for the sake of advancement without these critical considerations.

As additional future works the authors would like to expand out from just legislation in the United States and begin moving globally. With recent implementation of the General Data Protection Regu-

lation (GDPR) across the European Union, it sparks the question; what potential vulnerabilities has GDPR created in European healthcare? In the United States under HIPAA and organization can be fined a maximum of $1.5 Million USD, where as the highest level of fines under GDP are up to 20 million Euro or 4% of worldwide annual revenue (Hilliard, 2019).

During our research, the United States Department of Health and Human Services (HHS) proposed changes to the Stark Law that would provide a safe harbor for those that donate cybersecurity technology. Per a HHS representative "We believe that omitting a contribution requirement may allow providers with limited resources to receive protected cybersecurity donations, while also using their own resources to invest in other technology not protected by the safe harbor, such as updating legacy hardware that may pose a cybersecurity risk, or simply investing in their own computers, phones, and other hardware" (Davis, 2019a). Similar to herd immunity, when smaller healthcare facilities are secured, all of healthcare is more secure. Until these issues in legislation and regulation become wholly addressed, healthcare will continue to be the number one target of malicious threats.

REFERENCES

Assistance, H. C. (2003). Summary of the hipaa privacy rule. *Office for Civil Rights*.

Beazley (2019). Beazley breach insights - february 2019.

Bitglass (2016). what a difference a year makes.

Branch, L. E. (2018). Cyber threats and healthcare organizations: A public health preparedness perspective. *Cyber Threats and Healthcare Organizations: APublic Health Preparedness Perspective*.

Davis, J. (2019a). Hhs stark law proposal permits cybersecurity donations to providers.

Davis, J. (2019b). Patients sue uconn health over data breach caused by phishing attack.

DesRoches, C. M., Worzala, C., and Bates, S. (2013). Some hospitals are falling behind in meeting 'meaningful use'criteria and could be vulnerable to penalties in 2015. *Health Affairs*, 32(8):1355–1360.

FDA (2016). Postmarket management of cybersecurity in medical devices - guidance.

Field, M. (2018). Wannacry cyber attack cost the nhs £92m as 19,000 appointments cancelled. *The Telegraph*.

for Disease Control, C. and Prevention (2018). Summary health statistics: National health interview survey, 2018.

Henry, J., Pylypchuk, Y., Searcy, T., and Patel, V. (2016). Adoption of electronic health record systems among u.s. non-federal acute care hospitals: 2008-2015.

Hilliard, R. (2019). Hipaa versus gdpr.

Kruse, C. S., Frederick, B., Jacobson, T., and Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1):1–10.

Le Bris, A. and El Asri, W. (2006). State of cybersecurity & cyber threats in healthcare ...

Leyden, J. (2014). Atm hacker barnaby jack's death blamed on accidental drug overdose.

OCR (2019). U.s. department of health and human services office for civil rights breach portal: Notice to the secretary of hhs breach of unsecured protected health information.

Paquet-Clouston, M., Haslhofer, B., and Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. *Journal of Cybersecurity*, 5(1).

Salcido, R. (2000). The government unleashes the stark law to enforce the false claims act: The implications of the government's theory for the future of false claims act enforcement. *Health Law.*, 13:1.

Spence, N., Paul, D. P., and Coustasse, A. (2017). Ransomware in healthcare facilities: The future is now. *Marshall University Marshall Digital Scholar*.

Viega, J. and Thompson, H. (2012). The state of embedded-device security (spoiler alert: Its bad). *IEEE Security & Privacy*, 10(5):68–70.

Williams, P. and Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, page 305.

Winton, R. (2016). Hollywood hospital pays $17,000 in bitcoin to hackers; fbi investigating. *Los Angeles Times*.

Wright, A., Aaron, S., and Bates, D. W. (2016). The big phish: Cyberattacks against u.s. healthcare systems. *Journal of General Internal Medicine*, 31(10):1115–1118.