Insufficient Healthcare Cybersecurity Invites Ransomware Attacks and Sale of PHI on the Dark Web

Katelyn Swasey

Spring 2020

CENTER FOR ANTICIPATORY INTELLIGENCE

COLLEGE OF HUMANITIES AND SOCIAL SCIENCES
UtahStateUniversity

Insufficient Healthcare Cybersecurity Invites Ransomware Attacks and Sale of PHI on the Dark Web

Center for Anticipatory Intelligence
Student Research Reports

Katelyn Swasey
April 2020

Executive Summary

The threat of ransomware and other cyberattacks is a rising specter for many industries that deal with sensitive information, but the healthcare sector is a particularly high-value target for criminal hackers because of the personal-details-rich protected healthcare information (PHI) that hospitals, clinics, and other entities hold for their patients. A dire level of underinvestment in IT departments and especially cybersecurity across the healthcare sector has further invited the attention of malicious actors who seek to steal and sell highly lucrative PHI on the Dark Web. A range of proactive and responsive measures must be implemented across the healthcare sector to counter the accelerating threat of cyberattacks that jeopardize healthcare entities' ability to function, their reputations and patients' trust, and their responsibility to safeguard not only their patients' health and wellbeing but their personal information.

Patient healthcare files contain a wide range of personal information including full names, Social Security numbers, addresses, insurance information, payment/credit card details, driver's licenses, and other health information. Stolen healthcare files can be worth up to $1,000 on the Dark Web, an alternate internet that utilizes browsers like The Onion Router (TOR) to facilitate highly encrypted interactions and transactions. While not all activity on the Dark Web is illegal, some parts of the Dark Web have become a virtual hub for illicit activity, including the sale of stolen personal information.

Healthcare entities hit by major cyberattacks including ransomware face the prospect of having their regular operations crippled by the loss of access to patient files, and may have to choose between permanently losing these critical files or paying ransoms that range from the tens of thousands to millions of dollars. Furthermore, the loss of protected patient information may incur hefty government fines for violating HIPAA law and exposing patients to identity theft. The financial and reputational costs associated with failing to prevent major ransomware and other cyberattacks far outweigh the up-front costs associated with taking proactive measures to bolster system cybersecurity.

No entity can achieve perfect resistence against all cyber threats, but significant steps can be taken in the healthcare sector to reduce preventable risk and create resilience plans that will allow essential functions to continue in the event of an attack and avoid the permanent loss of patient data. The healthcare sector must act now to prioritize caring not only for the bodies and minds of patients but their identities and critical personal information as well.

Introduction

Cyberattacks are part of an ever-evolving and dynamic threat landscape that aims to undermine and exploit many industries. The healthcare industry is not exempt from this, and over recent years has become a primary target for attack. Due to a lack of resources and focus within the industry, many entities within healthcare are not properly equipped to identify and prevent cybersecurity events from occurring. The primary goal of the healthcare industry is to care for people at their most vulnerable moments in life, and therefore most resources are put towards cutting-edge research, modern machines, and expert physicians and staff. But this logical allocation of finite resources toward improving quality of care often leaves IT departments critically lacking, inviting cyberattacks and theft of critical patients' protected health information (PHI), which is a highly lucrative commodity for illicit sale on the dark web given its rich saturation of identity and financial information. While there is no way to completely eradicate the cyber threat to the healthcare sector, the importance of cybersecurity in healthcare cannot be overstated, and there are actionable ways to better prepare for and weather these threats.

Encryption and Anonymity Set the Dark Web Apart, Attracting Illicit Activities

Introduction to the TOR Browser

The World Wide Web can be separated into three distinct sublevels: the Surface Web, Deep Web, and Dark Web.[1] The Surface Web contains all indexed pages on the internet and is accessed by users all over the world at any time. The Deep Web is approximately 400-500 times larger than the Surface Web[2] and consists of sites requiring login credentials for access, such as banking, university, and healthcare sites.[3] The Dark Web makes up a very small portion of the Deep Web and cannot be accessed through common search browsers such as Google.[4] In order to access the Dark Web, users are required to use specialized browsers such as The Onion Router (TOR) browser, named for the type of encryption it uses.

The TOR browser was originally created as a project between the Defense Advanced Research Projects Agency (DARPA) and the United States Navy.[5] The idea behind the project was to find a way for law enforcement and undercover agents to use the internet without their IP addresses being tracked through government traffic logs.[6] In 1997, the TOR browser was released into the public domain in order to saturate the browsing tool with civilian users. This was done to mask law enforcement and intelligence agency users, furthering their anonymity on the internet.[7] Today, TOR is maintained through the TOR Project, a 501c3 nonprofit organization,[8] which utilizes a set of "core staff" to maintain the browser and continue research. The TOR Project also utilizes volunteers across the globe who host TOR servers to support functionality.[9]

How Onion Routing Works

The TOR browser utilizes onion routing to encrypt data. Onion routing is a "layered data structure that specifies properties of the connection at each point along the route."[10] This is a multilayer encryption system (hence the name "onion" routing): messages and users are directed along randomized paths across the globe through servers hosted by volunteers. The path is made up of three layers and flows through the same number of servers called the entry, middle, and exit nodes.[11] When a user wishes to visit a site or send a message, the browser connects to a randomly selected public entry node and goes through a randomly assigned path towards the exit node.[12] Once a connection has been made, data can be sent in both directions using the algorithms and keys that were specified in the onion by the initiator.[13]

At the entry node, the first layer is decrypted using its shared key, then the next destination is discovered and the message is passed along.[14] In this system, each of the nodes knows the preceding and succeeding destinations but does not have access to any other nodes in the system or the message that is being sent.[15] The middle node, also known as the data movement stage, follows the same steps as the entry node to decrypt its own layer. When the data reaches the exit node, there is only one layer of encryption left and the shared secret key is used to decrypt the data and forward the data in plain text to the destination server.[16]

If users are utilizing a specific connection, the data that is being sent will be protected from decryption if intercepted because of an added layer of encryption. If another user were to intercept the data after the exit node in order to gain access to the plain text data, they would not be able to see the data because the outgoing data from the exit node is encrypted and the key to decrypt it is one that only the sender and destination knows.[17] When the final destination is reached and the plain text is visible, the information may furthermore be in a foreign language. This is the result of Onion Encryption and how it blocks IP address tracking by transferring the information through servers across the world—the web thinks that the user is in a location that does not reflect reality.[18] The layered cryptography over data makes each onion look different to each onion router and better resists traffic analysis.[19]

Crime on the Dark Web

The deflection of IP address tracking combined with the level of encryption offered through Dark Web browsers like TOR draws many kinds of people to use it, including cybercriminals. The virtually complete anonymity makes it a perfect platform for the buying and selling of illegal substances and materials as well as organized crime. Reported crimes that have taken place on the Dark Web include drug trafficking, child pornography, malware trading, and sale of personal account information and other personal identifying information.[20] It is not illegal to access the Dark Web, and not everything hosted on the Dark Web relates to illegal activities; one survey from 2015 estimates the proportion of illicit content is approximately 40 percent.[21] The platform has just become a popular tool for criminals wishing to remain anonymous to law enforcement to do business in a sheltered location, not dissimilar from crimes committed in dark alleys or motels. The dilemma surrounding the Dark Web can be summed up by TOR Project officials in an interview following the discovery of a neo-Nazi, white supremacist group:

> We are disgusted, angered, and appalled by everything these racists stand for and do. We feel this way any time the Tor [sic] network and software are used for vile purposes.[22] Cars and phones are also used for vile purposes, but that doesn't mean cars and phones are bad, Same with Tor. Tor was developed to protect people, and that's why most people use it, including journalists, human-rights advocates, lawyers, researchers, marginalized groups, and privacy conscious individuals.[23]

While the Dark Web can be a place for good, and the majority of the content is legal, the risks it can pose to the public's information and safety are clear and present, particularly as it relates to the threat of personally identifiable information being bought and sold on the Dark Web.

Abysmal Healthcare Cybersecurity Standards Jeopardize Privacy and Security of PHI

The healthcare industry has historically lagged behind other industries in the adoption of online resources and the cybersecurity practices that accompany these changes.[24] According to one survey conducted in 2013, less than 10 percent of nearly 2,000 primary-care physicians surveyed had electronic systems that met the US rules for "meaningful use."[25] This means that less than 200 physicians surveyed utilized systems that are aligned with government standards regarding how electronic health records are exchanged between providers, insurers, and patients.[26] Only 43.5 percent of those surveyed reported having a basic computerized system in place to manage patient populations.[27] Since then, there has been an explosion of healthcare facilities putting patient protected health information (PHI) onto online clinic websites and databases. Doctor visits, prescription renewals, insurance claims, and much more are processed online every day. Patient medical records are tracked and maintained in various databases and can be shared with prospective physicians or the patient in an instant. This explosion of data entering the internet draws attention to the need for cybersecurity in the healthcare industry.

According to the Hippocratic oath, an important historical document that many in the healthcare industry hold sacred,[28] medical professionals vow that "Whatever, in connection with my professional practice or not, in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret."[29] This means that those working in the healthcare industry, whether physicians or other support personnel or staff, are held to a standard of privacy regarding patient information. It is the duty of the healthcare industry to protect and serve the public, including by protecting their healthcare information. A more modern guideline regarding patient privacy was introduced in 1996 and is known as the Health Insurance Portability and Accountability Act (HIPAA). HIPAA provides guidance and regulation for healthcare providers and covered entities on the disclosure of protected health information. This includes to whom the information can be given and under what circumstances the information is available.[30]

Today, the healthcare industry is still lagging behind other industries in cybersecurity. In 2018, healthcare providers spent approximately 5 percent of their IT budgets on cybersecurity, lower than other industry averages.[31] Not only are healthcare IT departments underfunded in regard to cybersecurity, IT teams are often understaffed or are outsourced from small IT firms. A survey conducted in 2018 revealed that 39 percent of healthcare IT staffs consisted of fewer than 10 people.[32] Doug Brown, founder of Black Book Market Research, noted that "cybersecurity is a newer line item for hospitals and physician enterprises and budgets have not evolved to cover the true scope of human capital and technology requirements yet."[33] The lack of resources combined with sometimes outdated systems can lead to vulnerabilities in the system.[34] In 2018, one survey noted that 28 percent of respondents stated that their organization does not scan for cyber vulnerabilities—this was the most frequent response as well.[35] Future outlooks were not promising: "Only 12 percent of hospitals and 9 percent of physician organizations expressed optimism that a Q2 2019 assessment would find their network safer than it is today—nearly a quarter actually reported believing that their situation would worsen."[36]

Healthcare cybersecurity must become a priority because of the sensitive nature of the data that is stored by healthcare providers. Part of caring for patients is taking care of their information so that it does not fall into the wrong hands and cause harm. The current vulnerabilities and lack of financial and physical investment in cybersecurity signals to criminals and other malicious actors that the PHI being held by healthcare entities is an easy target. Consider all the information doctors' offices collect at an initial new patient visit: full names, Social Security numbers, emergency contacts, insurance information, payment/credit card information, a copy of driver's licenses, and other health information. That information is promptly loaded onto computer programs that are accessed online by the employees and doctors. Without proper cyber security measures, all this information is vulnerable to cyber theft.

Comprehensive PHI Maintained by Healthcare Entities Becomes Target of Ransomware

Hackers' Motives for Placing PHI on the Dark Web

The sale of personal information on the Dark Web can be very profitable for hackers who obtain it. In general, criminal hackers will typically target vulnerable organizations who maintain sensitive information and are incentivized to pay ransoms quickly.[37] Ransoms are the result of ransomware attacks, a form of malware designed to encrypt information until a payment has been made. Social Security numbers can be sold for $1-$5 each, credit and debit cards can be sold for approximately $100 each, and Driver's License information sells for around $20.[38] If a file has multiple mediums of information about a single person, both its value and illicit selling price increases. Because a wealth of information is maintained in a single healthcare patient file—date of birth, credit card information, Social Security number, address, email, signature, insurance numbers, prescription information, and so forth—these files become a high priority target for hackers wishing to sell personal information on the Dark Web.[39] Patient health files sell for approximately $1000 on the Dark Web depending on completeness.[40]

Ransomware attacks are one of the most frequently used cyberattacks deployed against the healthcare industry to steal patient information.[41] Attacks are generally executed through the use of phishing emails with links or attachments. The files are innocently named with typical hospital communications such as "updated patient list" or "billing codes,"[42] but once accessed the infected files release ransomware malware into the host system, encrypting files until the ransom has been paid. Victims generally pay ransoms via Bitcoin, further anonymizing the hackers.[43] Ransomware is especially utilized against healthcare facilities because they utilize less cybersecurity than other industries, they hold sensitive data, and they are willing to pay quickly in order to regain access to critical patient information.[44]

Hospitals are especially susceptible to ransomware attacks. The data that they maintain regarding PHI is essential to ensuring their patients are properly cared for—this is often information that could mean the difference between life and death in critical care cases. Hospitals' willingness to pay combined with their vast reserves of complete patient records creates financial incentive for hackers to prioritize them as targets. Not only do hackers receive the hospital's ransom payment, but they can copy the records they are holding and sell them on the Dark Web for further profit. In general, experts caution against paying ransoms when a cyberattack occurs because it is possible that files will not be fully recovered if at all. This industry advice reinforces healthcare facilities' position as a higher priority target for hackers because these entities have shown their willingness, out of desperation, to pay ransoms.[45]

Ransomware Attack Statistics

There has been a sufficient increase in the number of ransomware attacks against the healthcare industry in recent years that the Federal Bureau of Investigation (FBI) and other security entities consider hospitals and healthcare facilities to be primary targets for attack.[46] In 2018, Sutter Health, one of many healthcare networks in the United States, reported 87 billion cyberthreats.[47] A survey conducted in 2018 found that of nearly 2,500 healthcare security experts, 96 percent think that bad actors are outpacing the defenses of their facilities.[48] From 2015 to 2016, the rate of successful patient medical file theft increased from 55 percent to 64 percent, resulting in 172 reported attacks in 2016.[49] Between the first and third quarters of 2019, ransomware attacks against healthcare targets jumped 60 percent.[50] Between 2019 and early 2020, there were 491 successful ransomware attacks against US-based healthcare providers.[51]

Ransomware attacks result in the loss of significant quantities of both PHI and other Personal Identifying Information (PII).[52] From 2018 to 2019 there was an increase of almost 38 percent in the number of records breached, resulting in the loss of approximately 41 million records.[53] As of November 2019, approximately 11.64 percent of the US population had had their healthcare information exposed that year,[54] and the top five largest data breaches of 2019 affected over 28 million individuals.[55] On February 11, 2020, NRC Health—estimated to work with 75 percent of the 200 largest hospital chains in the United States—was hit with a cyberattack.[56] According to the breach report, at least 63,581 people were impacted as a result.[57]

Attacks against the healthcare industry can also be fueled by external events that create opportunity for cyberattackers. Between February 2020 and April 2020, there was a 667% increase in phishing emails due to the COVID-19 pandemic.[58] In April 2020, Google identified and blocked 240 million spam messages and 18 million phishing emails relating to the COVID-19 pandemic.[59] On March 16, 2020 between 10:00am and 5:00pm CET alone, there were 2,500 infections of malware related to COVID-19 as the result of email scams.[60] Pandemics are an extremely stressful time for the healthcare industry, with resources and time desperately strained trying to respond to cases and make decisions in order to keep the public safe. During such times, cybersecurity is surely at the back of the minds of first responders and caregivers. However, pandemics and public health crises provide an opportune moment for hackers precisely because the healthcare industry is off guard. It is essential during times of pandemic or disaster for the healthcare industry to prepare for and place attention on cybersecurity.

There are enormous financial impacts for healthcare entities hit by ransomware attacks and data breaches. One recent study found that the size of ransom payments increased by 13 percent in the third quarter of 2019 to $41,198, six times higher than the fourth quarter of 2018.[61] The average ransom doubled again in the fourth quarter of 2019 to $84,116, with many organizations facing ransom demands in the millions of dollars.[62] It is estimated that ransomware attacks will have cost all paying victims $11.5 billion in 2019—approximately 30 percent higher than the nearly $8 billion paid in 2018.[63]

PHI data breaches are a violation of HIPAA and there are government-imposed penalties for healthcare sector entities related to the loss of patient data. The Office for Civil Rights enforces HIPAA Rules and refers possible criminal violations to the Department of Justice.[64] There are four penalty tiers ranging in severity from being unaware of a HIPAA violation to willful neglect of HIPAA rules. Civil penalties can range from $100 to $1.5 million depending on the tier classification involved with the data breach. Appendix A gives a thorough breakdown of the civil and criminal penalties involved.[65] The majority of ransomware attacks fall under Tier 1 or Tier 2; these are lower level infractions and range in civil penalties between $100 and $50,000. Covered entities may also be required to pay restitution to patients whose information has been stolen and defrauded.[66] When a breach does occur, covered entities will be added to a breach portal, also known as the "Wall of Shame," and can result in a decrease of future business and image rating decline.[67] Not properly securing PHI can lead a hospital or business to lose thousands of dollars in ransom payments and government sanctions. Covered entities may also face litigation from patients and decrease their future potential patient base.

Preparation for Future, Sophisticated Cyberattacks Needed to Ensure Continuation of Care

The breach of patient PHI is a very serious error, and whether lost by accident or malicious hacking incident, it can cost the healthcare entities involved thousands of dollars. These errors are not only a financial burden to systems, but they also undermine the trust between patients and their healthcare providers. Patients trust healthcare systems with their wellbeing and oftentimes their lives. This includes trust that their healthcare providers will take upmost care in protecting their personal information. Ransomware attacks are often unpreventable, incredibly difficult to track, and create additional chaos in an already stressful environment. However, the healthcare industry can take small steps that have the potential to lead to big differences in cybersecurity standards.

Healthcare entities must begin to fortify their systems in order to resist ransomware attacks and prevent as many attacks as possible from being successful. There is no way to completely eliminate, or have perfect *resistance*, against ransomware attacks against the healthcare industry. But healthcare entities can better control their destinies by following expert cybersecurity guidelines and proactively preparing against the threat of attacks. In order to do so, they must outline a *resilience* plan that allows them to continue key operations in the midst of an attack. This may include beginning to integrate backup files and servers into current systems to preserve PHI in multiple places. Once a ransomware attack has occurred, it is essential to move quickly to *recover* the stolen information—utilizing law enforcement support to locate and protect patient identities and prevent the sale of patient information on the Dark Web. Finally, it is important that after an attack occurs affected entities learn from their own and others' mistakes and successes in order to identify *resurgence* measures that will help create more robust protection and response plans that are ready to face future attacks with minimized risk.

Resistance Measures

First, healthcare entities need to allocate more funds to their internal IT departments, which are widely understaffed and underfunded. By limiting the resources put into IT departments, hospitals and clinics are limiting the quality of outputs that can be produced. In order to perform well, IT departments need to be well staffed with knowledgeable experts who know how and where to search for vulnerabilities. Not only do qualified professionals need to be employed, but they need to be given the necessary tools in order to be successful at their job. In this domain, IT departments specifically need more funding for cybersecurity in their annual budgets. A very low percentage of annual budgets are allocated to cybersecurity in the healthcare industry—the healthcare sector spends approximately 5 percent of IT budgets on cybersecurity compared to just over 7 percent in the banking and financial sector, and 6 percent in the retail and wholesale sector.[68] If the healthcare industry were to increase budgets by even 1-2 percent, it could potentially save millions of patient files from ending up on the Dark Web.

New funding should in part be directed toward the creation of more robust cybersecurity infrastructure. Many healthcare entities are running on legacy systems, some even decades old.[69] These outdated systems are especially susceptible to hacking and are in desperate need of updating. Along with updates, these systems would benefit from purchasing additional protection against ransomware attacks through software that can scan for vulnerabilities. Additional funding can also be invested in employee training. Because the majority of ransomware attacks are the result of email phishing scams,[70] entity-wide training against cybersecurity threats would help to greatly reduce the number of successful ransomware attacks. Phishing emails no longer from faux Nigerian princes; they come from ostensibly familiar sources such as vendors, physicians, or colleagues. At first glance they look legitimate, and in some cases, it may take carefully studying the email to determine if it is a fraud.[71] Appropriate training would equip all hospital or clinic employees, from physicians to administrators and support staff, with the skills necessary to prevent the spread of ransomware by not clicking infected links.

These suggested prevention tactics will take time, significant funding, and in some cases changes in organizational culture in order to be successful. These investments may detract from other funding priorities within healthcare, but it is a necessary cost that will have crucial benefits. If new procedures are not implemented and a major ransomware attack occurs, the cost could be astronomical. Between ransoms, lawsuits, and government-imposed fines, covered entities are facing the prospect of paying millions of dollars in restitution. The investment in cybersecurity today will prevent escalating costs tomorrow in the wake of a successful ransomware attack.

Resilience Measures

While there is no way to prevent every ransomware attack on the healthcare industry, the industry can work to create a system that will continue to perform more securely during an attack. Medical entities able to maintain backup files of their patient data on a secure (often offsite) backup server preserve the ability to function without the need to pay a ransom. According to an interview with a cloud backup service company, when one of their healthcare customers lost access to 14 years' worth of files in an attack, the victim did not have to pay the ransom because they were able to utilize their backup services to regain access to files and continue operations.[72] In some cases, when ransoms are not paid, hackers are less likely to target the same system again in the future because it has not proven a lucrative target. System backups also provide a way for victimized entities to wipe their compromised systems if necessary and restore it with backup files.[73]

The implementation of backups must be thought about carefully in order to provide adequate security. Some ransomware attackers will gain entry through a desktop system and look for backup systems that are connected to the desktop to encrypt those files as well.[74] An example of this took place in November 2018, when according to the US Department of Justice two Iranians utilized malware to extort approximately $30 million from 200 victims, including hospitals, by encrypting backup files.[75] In some cases, backup files are not necessarily sought out, but if the ransomware malware comes across a backup file on the target system, it will encrypt it.[76] In order to mitigate these risks, it is important to have a secure redundant system with several backups and proper security protocols for these backups.[77] Health systems should consider implementing multiple and various authentication procedures to access backups. Authentication can include passwords, security badges, or verification using a mobile device. The databases should also be kept in separate locations, physically distant from the primary system. In the event of a ransomware attack, if the data is far removed from the targeted system it will less likely to be affected by the attack. The more layers of security that are utilized, the safer the information will be against attack.

Recovery Measures

When files have been stolen and posted on the Dark Web, patients have no way of knowing their information has been leaked until it is used on the Surface Web. Former FBI Analyst Willis McDonald stated, "The best thing that you can do is monitor your accounts, monitor your credit history, monitor your bank accounts, and know what's going on … Because it's almost safer to assume that way that your information has already been stolen."[78] For many patients, this is regrettably a very safe assumption because of the number of patient records that have been leaked or stolen in recent years. Hackers have also started to steal the records of deceased patients.[79] This can be especially dangerous because there is no longer someone to monitor what is being done with their information, and nobody to report fraud to police.

Dark Web cybercrime has been a challenge for law enforcement in the past due to the anonymity offered there.[80] However, law enforcement agencies across the world have been working to remove criminal communities from the Dark Web.[81] In 2015, the FBI seized the server running the largest pedophile child pornography site on the Dark Web. The FBI then ran the site in a sting operation, via their own servers, and utilized a tool to identify approximately 1,300 IP addresses that visited the site.[82] The FBI has also been successful in seizing several other Dark Web sites that host criminal activity, including one that ran an underground black market.[83] A similar mechanism could be utilized to seize major sites that host the selling of PHI and other personal information. The FBI would need to successfully track activity on the Dark Web and identify the sites dealing in stolen health files, then could perform a similar takeover to the one used to close down the child pornography site and track illicit customer IP addresses before the information can be sold. A former FBI analyst stated, "…a cyber-criminal would need only 5 to 10 seconds before locating stolen patient medical records for sale."[84] This likely means that the FBI could identify prominent vendor sites and shut them down to prevent any future PHI files being sold on those platforms. When the larger sites are seized, it may deter buyers from purchasing from smaller vendors due to the threat of being identified by law enforcement. There is no way for any one agency to completely eradicate all PHI sales on the Dark Web, but the tools available to remove large vendors from the market should be utilized.

Resurgence Measures

Resurgence is the practice of improving a system by learning from an entity's own mistakes and successes as well as those of others. By improving upon past mistakes, healthcare entities can take proactive measures to become more cybersecure and experience less of an impact during an attack. A useful case study for resurgence is one of the largest healthcare data breaches resulting from a cyberattack, which occurred in early 2015. Anthem Blue Cross, a healthcare insurance company through which one in nine Americans have insurance coverage,[85] was hit with a cyberattack resulting in the loss of 78.8 million patient records.[86] The stolen information included names, dates of birth, addresses, income data for employees, Social Security numbers, and healthcare ID numbers.[87] As of 2016, the FBI was still investigating the attack and found no evidence that the information stolen had been sold or utilized.[88] If the hackers were to sell the information, it could be years before the information is used for gain on the Surface Web. The attackers got hold of credentials, gained access to the IT system,[89] and were able to steal the information by logging into the company's database.[90] Anthem announced the breach in January 2015; however, the incident actually began in December 2014 and five employees had their credentials compromised.[91] Security experts note that the stolen information was vulnerable because Anthem did not encrypt the data maintained internally as they would have if the information were shared outside the database.[92]

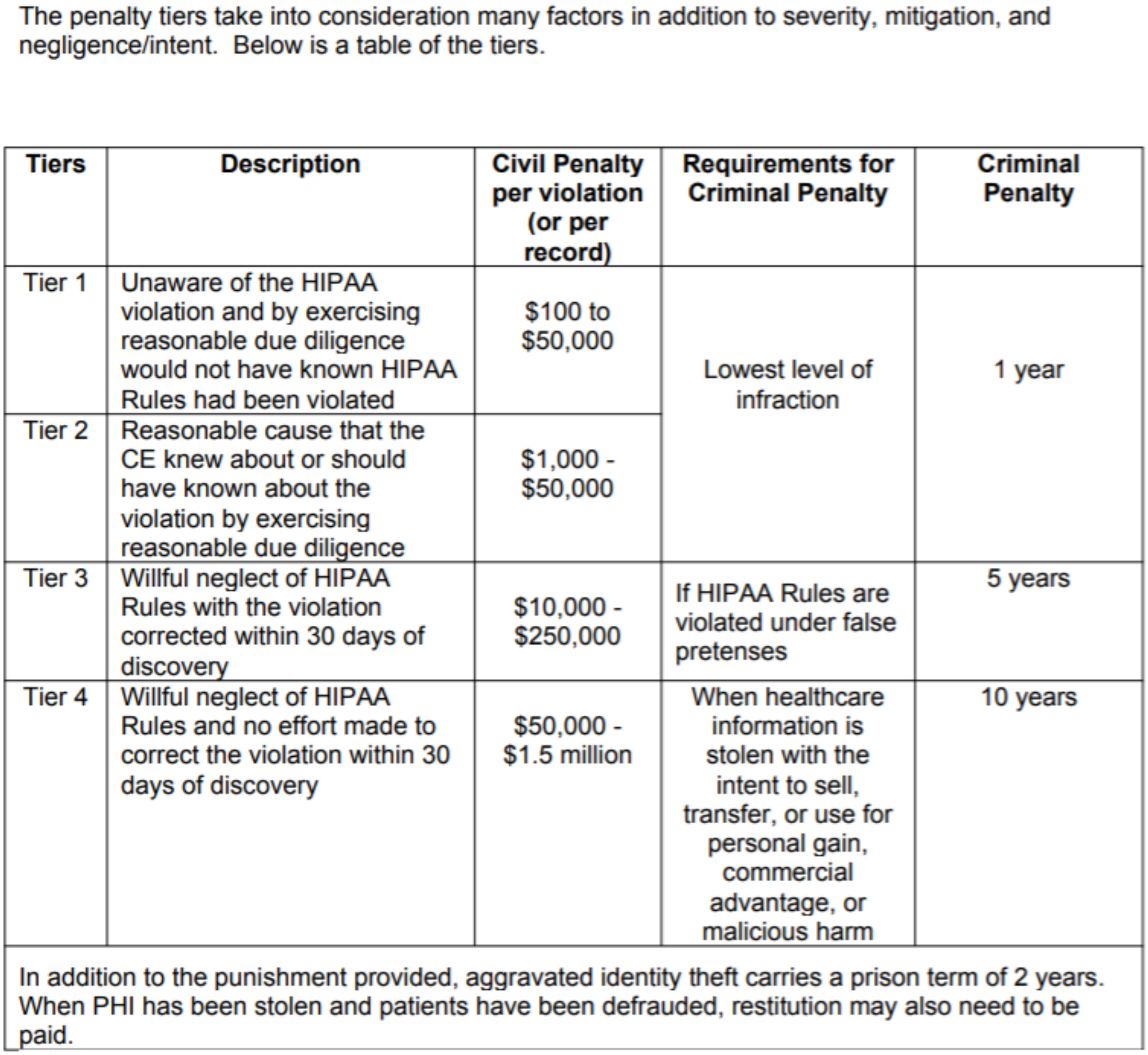
During this breach, Anthem did several things right in dealing with law enforcement and the public. They notified the FBI immediately and hired a cybersecurity firm to review what happened.[93] They also provided "identity protection services" to each of the individuals impacted by the breach.[94] However, there was a rather lengthy stretch of time between the point when the incident took place in December and when Anthem began to notify officials and start investigations in January. Regular monitoring of security systems could have helped to notify IT professionals of anomalies that might have been potential vulnerabilities. Some companies are also utilizing self-audit capabilities to provide a record of an employee's credential use.[95] This would have been beneficial for Anthem, as it would have enabled their IT team to identify their exposed vulnerability before so much data was stolen.

Whether breaches occur as the result of persistent cyberattack or from ransomware, the security standards remain the same. Internal encryption is needed to help prevent the loss of patient healthcare information. Additionally, regular monitoring and system testing is also required to identify security vulnerabilities. Once identified, IT teams should make patching the network a priority and begin testing again to ensure the fix is successful. In ransomware attacks—but also in the case of the Anthem breach—once there has been a human breach, there is little hope to prevent the spread of the attack. All entities in the healthcare industry should implement employee education for phishing emails, ransomware attacks, and cybersecurity measures to help reduce the danger of human error. Many of these attacks begin with an internal employee's misplaced click. If all members of a healthcare entity are aware and looking for suspicious activity on their personal computers or systems, it can prevent many of these instances from happening. Anthem received great public embarrassment and loss many consumers' trust. No company wants to be in such a situation, especially when prevention can be relatively simple. The healthcare sector can learn from these mistakes and create more robust and secure systems.

Conclusion

Healthcare cybersecurity is under perpetual threat of attack by malicious actors. The tactics of these actors have evolved beyond the defenses currently employed by healthcare entities, and hackers are far outpacing hospital and other healthcare industry cybersecurity efforts. These attacks have far reaching consequences that extend beyond the walls of the institution targeted and impact millions of households through the loss and fraudulent use of personal information. Often there is no way to prevent the sale of PHI once stolen, and it is only a matter of time before it surfaces again in the hands of someone planning to use it maliciously. Healthcare cybersecurity is not a lost cause, there is much that can be done to better care for and protect the sensitive information maintained in healthcare institutions. The implementation of simple training procedures, more proactive planning, increased budget commitments can greatly reduce the number of successful attacks. As the focus is shifted to cybersecurity, healthcare entities will be able to learn from past mistakes to better prepare for the future. Ransomware and other cyberattacks are part of an ever evolving, dynamic threat landscape, and the healthcare industry needs to be on high alert and prepared to continue essential functions for its vulnerable patients in the midst of an attack. The lifesaving work of healthcare cannot be jeopardized by failing to meet the rising tide of cyber threats against this critical sector.

Appendix A



The penalty tiers take into consideration many factors in addition to severity, mitigation, and negligence/intent. Below is a table of the tiers.

Tiers	**Description**	**Civil Penalty per violation (or per record)**	**Requirements for Criminal Penalty**	**Criminal Penalty**
Tier 1	Unaware of the HIPAA violation and by exercising reasonable due diligence would not have known HIPAA Rules had been violated	$100 to $50,000	Lowest level of infraction	1 year
Tier 2	Reasonable cause that the CE knew about or should have known about the violation by exercising reasonable due diligence	$1,000 - $50,000		
Tier 3	Willful neglect of HIPAA Rules with the violation corrected within 30 days of discovery	$10,000 - $250,000	If HIPAA Rules are violated under false pretenses	5 years
Tier 4	Willful neglect of HIPAA Rules and no effort made to correct the violation within 30 days of discovery	$50,000 - $1.5 million	When healthcare information is stolen with the intent to sell, transfer, or use for personal gain, commercial advantage, or malicious harm	10 years

In addition to the punishment provided, aggravated identity theft carries a prison term of 2 years. When PHI has been stolen and patients have been defrauded, restitution may also need to be paid.

Endnotes

[1] Kehoe, Shawn R. "The Digital Alleyway: Why the Dark Web Cannot Be Ignored." *Police Chief Magazine,* June 12, 2018. https://www.policechiefmagazine.org/the-digital-alleyway/

[2] Thompson, Cadie. "Beyond Google: Everything You Need to Know About the Hidden Internet." *Business Insider,* December 16, 2015. https://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11

[3] Choudhury, Saheli, R. "The 'deep web' may be 500 times bigger than the normal web. It uses go well beyond buying drugs." *CNBC,* September 6, 2018. https://www.cnbc.com/2018/09/06/beyond-the-valley-understanding-the-mysteries-of-the-dark-web.html

[4] Kehoe, Shawn R. "The Digital Alleyway: Why the Dark Web Cannot Be Ignored." *Police Chief Magazine,* June 12, 2018. https://www.policechiefmagazine.org/the-digital-alleyway/
Thompson, Cadie. "Beyond Google: Everything You Need to Know About the Hidden Internet." *Business Insider,* December 16, 2015. https://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11
Clarke, Laurie. "What is the dark web? Our guide to the dark web." *TechWorld,* July 4, 2018. https://www.techworld.com/security/what-is-dark-web-3645157/

[5] Jacoby, Corianna. "The Onion Router and the Darkweb." *Tufts.edu,* December 15, 2016. https://www.cs.tufts.edu/comp/116/archive/fall2016/cjacoby.pdf
Clarke, Laurie. "What is the dark web? Our guide to the dark web." *TechWorld,* July 4, 2018. https://www.techworld.com/security/what-is-dark-web-3645157/

[6] Jacoby, Corianna. "The Onion Router and the Darkweb." *Tufts.edu,* December 15, 2016. https://www.cs.tufts.edu/comp/116/archive/fall2016/cjacoby.pdf

[7] Clarke, Laurie. "What is the dark web? Our guide to the dark web." *TechWorld,* July 4, 2018. https://www.techworld.com/security/what-is-dark-web-3645157/
Jacoby, Corianna. "The Onion Router and the Darkweb." *Tufts.edu,* December 15, 2016. https://www.cs.tufts.edu/comp/116/archive/fall2016/cjacoby.pdf

[8] n.a. The Tor Project, about us. n.d. https://www.torproject.org/

[9] Jacoby, Corianna. "The Onion Router and the Darkweb." *Tufts.edu,* December 15, 2016. https://www.cs.tufts.edu/comp/116/archive/fall2016/cjacoby.pdf
Jayasekara, Deepal. "Deep Dive Into TOR (The Onion Router)." *Medium*, November 25, 2016. https://blog.insiderattack.net/deep-dive-into-tor-the-onion-router-6de4c25beba7

[10] Goldschlag, David. & Reed, Michael. & Syverson, Paul. "Onion Routing for Anonymous and Private Internet Connections." January 28, 1999. https://www.onion-router.net/Publications/CACM-1999.pdf

[11] Jayasekara, Deepal. "Deep Dive Into TOR (The Onion Router)." *Medium*, November 25, 2016. https://blog.insiderattack.net/deep-dive-into-tor-the-onion-router-6de4c25beba7

[12] Porup, J.M. "What is the Tor Browser? And how it can help protect your identity." *CSO United States,* October 15, 2019. https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html

[13] Goldschlag, David. & Reed, Michael. & Syverson, Paul. "Onion Routing for Anonymous and Private Internet Connections." January 28, 1999. https://www.onion-router.net/Publications/CACM-1999.pdf

[14] Jayasekara, Deepal. "Deep Dive Into TOR (The Onion Router)." *Medium*, November 25, 2016. https://blog.insiderattack.net/deep-dive-into-tor-the-onion-router-6de4c25beba7

[15] Dingledine, Roger. & Mathewson, Nick. & Syverson, Paul. "Tor: The Second-Generation Onion Router." n.d. https://www.onion-router.net/Publications/tor-design.pdf

[16] Jayasekara, Deepal. "Deep Dive Into TOR (The Onion Router)." *Medium*, November 25, 2016. https://blog.insiderattack.net/deep-dive-into-tor-the-onion-router-6de4c25beba7
Lee, Joel. "What is Onion Routing, Exactly?" *Make Use Of Explains,* April 5, 2013. https://www.makeuseof.com/tag/what-is-onion-routing-exactly-makeuseof-explains/

[17] Jayasekara, Deepal. "Deep Dive Into TOR (The Onion Router)." *Medium*, November 25, 2016. https://blog.insiderattack.net/deep-dive-into-tor-the-onion-router-6de4c25beba7

[18] Porup, J.M. "What is the Tor Browser? And now it can help protect your identity." *CSO United States,* October 15, 2019. https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html

[19] Goldschlag, David. & Reed, Michael. & Syverson, Paul. "Onion Routing for Anonymous and Private Internet Connections." January 28, 1999. https://www.onion-router.net/Publications/CACM-1999.pdf

[20] Clarke, Laurie. "What is the dark web? Our guide to the dark web." *TechWorld.* July 4, 2018. https://www.techworld.com/security/what-is-dark-web-3645157/

[21] Hern, Alex. "The dilemma of the dark web: protecting neo-Nazis and dissidents alike." *The Guardian,* August 23, 2017. https://www.theguardian.com/technology/2017/aug/23/dark-web-neo-nazis-tor-dissidents-white-supremacists-criminals-paedophile-rings

[22] Clarke, Laurie. "What is the dark web? Our guide to the dark web." *TechWorld,* July 4, 2018. https://www.techworld.com/security/what-is-dark-web-3645157/

[23] Hern, Alex. "The dilemma of the dark web: protecting neo-Nazis and dissidents alike." *The Guardian,* August 23, 2017. https://www.theguardian.com/technology/2017/aug/23/dark-web-neo-nazis-tor-dissidents-white-supremacists-criminals-paedophile-rings

[24] Neumayer, Patty. Interview by Katelyn Swasey. Email Interview. February 27, 2020.

[25] Nussbaum, Alex. "Most Doctors Don't Meet U.S. Push for Electronic Records." *Bloomberg,* June 3, 2013. https://www.bloomberg.com/news/articles/2013-06-03/most-doctors-don-t-meet-u-s-push-for-electronic-records

[26] Rouse, Margaret. "Meaningful Use." *SearchHealthIT,* n.d. https://searchhealthit.techtarget.com/definition/meaningful-use#:~:text=In%20the%20context%20of%20health,and%20between%20providers%20and%20patients.

[27] DesRoches, Catherine M. & Audet, Anne-Marie. & Painter, Michael. & Donelan, Karen. "Meeting Meaningful Use Criteria and Managing Patient Populations: A National Survey of Practicing Physicians." *Annals of Internal Medicine,* June 4, 2013. https://annals.org/aim/article-abstract/1692572/meeting-meaningful-use-criteria-managing-patient-populations-national-survey-practicing

[28] Shiel, William C. "Medical Definition of Hippocratic Oath." *MedicineNet,* March 6, 2018. https://www.medicinenet.com/rheumatoid_arthritis_pictures_slideshow/article.htm

[29] Editors of Encyclopaedia Brittanica. "Hippocratic Oath: Ethical Code." *Britannica,* n.d. https://www.britannica.com/topic/philosophy

[30] n.a. "What is the Purpose of HIPAA?" *HIPAA Journal,* October 18, 2017. https://www.hipaajournal.com/purpose-of-hipaa/

[31] Garrity, Mackenzie. "5% of hospital IT budgets go to cybersecurity despite 82% of hospitals reporting breaches." *Becker's Health IT,* March 12 2019. https://www.beckershospitalreview.com/cybersecurity/5-of-hospital-it-budgets-go-to-cybersecurity-despite-82-of-hospitals-reporting-breaches.html
Schencker, Lisa. "Hackers target health data: 82% of hospital tech experts reported 'significant security incident' in last year." *Chicago Tribune,* March 8, 2019.

[32] n.a. "Hospitals are vulnerable to security risks, putting patient data, care in danger." *Healthcare Business & Technology,* July 10, 2018. https://www.healthcarebusinesstech.com/hospitals-are-vulnerable-to-security-risks-putting-patient-data-care-in-danger/

[33] Black, Ryan M. "Healthcare Cybersecurity Remains 'Understaffed and Underfunded'." *Inside Digital Health,* May 14, 2018. https://www.idigitalhealth.com/news/healthcare-cybersecurity-remains-understaffed-and-underfunded-according-to-new-survey

[34] Bush, Jonathan. "Health care must ditch its attachment to outdated software." *Stat News,* January 10, 2017. https://www.statnews.com/2017/01/10/health-care-outdated-software/

[35] Black, Ryan. "Vulnerabilities are Surging, and Healthcare Cybersecurity Might Struggle to Keep Up." *Inside Digital Health,* April 5, 2018. https://www.idigitalhealth.com/news/cybersecurity-vulnerabilities-are-surging-and-health-organizations-might-struggle-to-keep-up

[36] Black, Ryan M. "Healthcare Cybersecurity Remains 'Understaffed and Underfunded'." *Inside Digital Health,* May 14, 2018. https://www.idigitalhealth.com/news/healthcare-cybersecurity-remains-understaffed-and-underfunded-according-to-new-survey
Johansen. Alison G. "What is ransomware and how to help prevent ransomware attacks." *NortonLifeLock,* n.d. https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html
Fruhlinger, Josh. "Ransomware explained: How it works and how to remove it." *CSO United States,* December 19, 2018. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

[37] Spence, Nikki. & Bhardwaj, Niharika. & Paul, David P. & Coustasse, Alberto. "Ransomware in Healthcare Facilities: A Harbinger of the Future?" *Perspectives in Health Information Management,* Summer 2018. https://perspectives.ahima.org/ransomwareinhealthcarefacilities/

[38] n.a. "Shining A Light On The Dark Web: How Much Is Your Personal Information Selling For?" *Pace Technical,* n.d. https://www.pacetechnical.com/shining-a-light-on-the-dark-web-how-much-is-your-personal-information-selling-for/
Kan, Michael. "Here's How Much Your Identity Goes for on the Dark Web." *PCMag,* November 15, 2017. https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web
Bond, Casey. "What To Do If Your Email, Passwords Or Bank Info Were Found On The Dark Web."*Huffpost,* July 8, 2019. huffpost.com/entry/email-passwords-bank-info-dark-web_l_5d1f8262e4b04c4814136470

[39] Garrity, Mackenzie. "Patient medical records sell for $1K on dark web." *Becker's Health IT,* February 20, 2019. https://www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html
Torrey, Trisha. "How to Get Copies of Your Medical Records." *VeryWellHealth,* March 31, 2020. https://www.verywellhealth.com/how-to-get-copies-of-your-medical-records-2615505

[40] Garrity, Mackenzie. "Patient medical records sell for $1K on dark web." *Becker's Health IT,* February 20, 2019. https://www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html

[41] n.a. "2019 Healthcare Data Breach Report." *HIPAA Journal,* February 13, 2020. https://www.hipaajournal.com/2019-healthcare-data-breach-report/
Fruhlinger, Josh. "Ransomware explained: How it works and how to remove it." *CSO United States,* December 19, 2018. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

[42] Rayome, Alison D. "How to avoid ransomware attacks: 10 tips." *Tech Republic,* July 27, 2016. https://www.techrepublic.com/article/10-tips-to-avoid-ransomware-attacks/

[43] n.a. "Ransomware explained: How it works and how to remove it." *CSO United States,* December 19, 2018. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html
Rayome, Alison D. "How to avoid ransomware attacks: 10 tips." *Tech Republic,* July 27, 2016. https://www.techrepublic.com/article/10-tips-to-avoid-ransomware-attacks/

[44] Johansen, Alison G. "What is ransomwarae and how to help prevent ransomware attacks." *NortonLifeLock,* n.d. https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html

[45] Johansen, Alison G. "What is ransomwarae and how to help prevent ransomware attacks." *NortonLifeLock,* n.d. https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html

[46] Weiss, Jason G. "Emerging Cyber-Security Threats for 2020: The Rise of Disruptionwarae and High-Impact Ransomware Attacks." *The National Law Review,* January 23 2020. https://www.natlawreview.com/article/emerging-cyber-security-threats-2020-rise-disruptionware-and-high-impact-ransomware

[47] Wetsman, Nicole. "health Care's Huge Cybersecurity Problem." *The Verge,* April 4, 2019. https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation

[48] n.a. "Hospitals are vulnerable to security risks, putting patient data, care in danger." *Healthcare IT,* July 10, 2018. https://www.healthcarebusinesstech.com/hospitals-are-vulnerable-to-security-risks-putting-patient-data-care-in-danger/

[49] Spence, Nikki. & Bhardwaj, Niharika. & Paul, David P. & Coutasse, Alberto. "Ransomware in Healthcare Facilities: A Harbinger of the Future?" *Perspectives in Health Information Management,* Summer 2018. https://perspectives.ahima.org/ransomwareinhealthcarefacilities/
Farr, Christina. "Cyberattack on NRC Health sparks privacy concerns about private patient records stored by US hospitals." *CNBC,* February 20, 2020. https://www.cnbc.com/2020/02/20/nrc-health-cyberattack-sparks-privacy-concerns-about-patient-records-in-us.html

[50] n.a. "NRC Health Ransomware Attack Prompts Patient Data Concerns." *Dark Reading,* February 21, 2020. https://www.darkreading.com/attacks-breaches/nrc-health-ransomware-attack-prompts-patient-data-concerns/d/d-id/1337116

[51] Weiss, Jason G. "Emerging Cyber-Security Threats for 2020: The Rise of Disruptionware and High-Impact Ransomware Attacks." *The National Law Review,* January 23, 2020. https://www.natlawreview.com/article/emerging-cyber-security-threats-2020-rise-disruptionware-and-high-impact-ransomware

[52] Neumayer, Patty. Interview by Katelyn Swasey. Email Interview. February 27, 2020.

[53] n.a. “2019 Healthcare Data Breach Report.” *HIPAA Journal,* February 13, 2020. https://www.hipaajournal.com/2019-healthcare-data-breach-report/

[54] Ingham, Lucy. “Healthcare data breaches expose 38 million records in 2019, highlighting ‘cultural issue’.” *Verdict,* November 26, 2019. https://www.verdict.co.uk/healthcare-data-breaches-2019/
Coble, Sarah. “Report Reveals Worst State for Healthcare Data Breaches in 2019.” *Info Security,* February 14, 2020. https://www.infosecurity-magazine.com/news/report-healthcare-data-breaches-in/

[55] n.a. “2019 Healthcare Data Breach Report.” *HIPAA Journal,* February 13, 2020. https://www.hipaajournal.com/2019-healthcare-data-breach-report/

[56] Farr, Christina. “Cyberattack on NRC Health sparks privacy concerns about private patient records stored by US hospitals.” *CNBC,* February 20, 2020. https://www.cnbc.com/2020/02/20/nrc-health-cyberattack-sparks-privacy-concerns-about-patient-records-in-us.html

[57] n.a. “NRC Health Recovering from Ransomware Attack.” *HIPAA Journal,* February 24, 2020. https://www.hipaajournal.com/nrc-health-recovering-from-ransomware-attack/

[58] Shein, Esther. “667% spike in email phishing attacks due to coronavirus fears.” *Tech Republic,* March 26, 2020. https://www.techrepublic.com/article/667-spike-in-email-phishing-attacks-due-to-coronavirus-fears/

[59] Davis, Jessica. “Google Blocks 18M Daily COVID-19-Related Phishing Emails.” *Health IT Security,* April 20,2020. https://healthitsecurity.com/news/google-blocks-18m-daily-covid-19-related-phishing-emails

[60] Brewster, Thomas. “2,500 Attacks In Less Than A Day: Coronavirus Scammers Just Went Into Overdrive.” *Forbes,* March 26, 2020. https://www.forbes.com/sites/thomasbrewster/2020/03/16/2500-attacks-in-less-than-a-day-coronavirus-scammers-just-went-into-overdrive/#2e1a615f1f0b

[61] n.a. “Average Ransomware Payment Increased 13% to $41,198 in Q3, 2019.” *HIPAA Journal,* November 5, 2019. https://www.hipaajournal.com/average-ransomware-payment-rises-to-41198/

[62] Popper, Nathaniel. “Ransomware Attacks Grow, Crippling Cities and Businesses.” *The New York Times,* February 9, 2020. https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html
Coble, Sarah. “Report Reveals Worst State for Healthcare Data Breaches in 2019.” *Info Security,* February 14, 2020. https://www.infosecurity-magazine.com/news/report-healthcare-data-breaches-in/

[63] Weiss, Jason G. “Emerging Cyber-Security Threats for 2020: The Rise of Disruptionware and High-Impact Ransomware Attacks.” *The National Law Review,* January 23, 2020. https://www.natlawreview.com/article/emerging-cyber-security-threats-2020-rise-disruptionware-and-high-impact-ransomware

[64] Neumayer, Patty. Interview by Katelyn Swasey. Email Interview. February 27, 2020.

[65] Neumayer, Patty. Interview by Katelyn Swasey. Email Interview. February 27, 2020.

[66] Neumayer, Patty. Interview by Katelyn Swasey. Email Interview. February 27, 2020.

[67] n.a. “Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected.” *U.S. Department of Health and Human Services Office for Civil Rights,* n.d. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[68] Garrity, Mackenzie. “5% of hospital IT budgets go to cybersecurity despite 82% of hospitals reporting breaches.” *Becker’s Health IT,* March 12, 2019. https://www.beckershospitalreview.com/cybersecurity/5-of-hospital-it-budgets-go-to-cybersecurity-despite-82-of-hospitals-reporting-breaches.html
Schencker, Lisa. “Hospitals’ spending lags on digital security.” *Courier-Tribune,* March 11, 2019. https://www.courier-tribune.com/news/20190311/hospitals8217-spending-lags-on-digital-security

[69] n.a. “10 Biggest Problems in Healthcare Cybersecurity.” *Calyptix Security,* June 13, 2017. https://www.calyptix.com/hipaa/10-biggest-problems-in-healthcare-cybersecurity/

[70] n.a. “Protect Healthcare Data from Phishing.” *HIPAA Journal,* n.d. https://www.hipaajournal.com/protect-healthcare-data-from-phishing/

[71] n.a. “How to Recognize and Avoid Phishing Scams.” *Federal Trade Commission Consumer Information,* n.d. https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

[72] Zetter, Kim. “4 Ways to Protect Against the Very Real Threat of Ransomware.” *Wired,* May 13, 2016. https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/

[73] Dobran, Bojana. “Definitive Guide For Preventing and Detecting Ransomware.” *phoenixNAP,* February 15, 2019. https://phoenixnap.com/blog/preventing-detecting-ransomware-attacks

[74] Zetter Kim. “4 Ways to Protect Against the Very Real Threat of Ransomware.” *Wired,* May 13, 2016. https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/

[75] Korolov, Maria. "How to protect backups from ransomware." *CSO United States,* January 14, 2019. https://www.csoonline.com/article/3331981/how-to-protect-backups-from-ransomware.html

[76] Korolov, Maria. "How to protect backups from ransomware." *CSO United States,* January 14, 2019. https://www.csoonline.com/article/3331981/how-to-protect-backups-from-ransomware.html

[77] Clark, T. "Attempting to Recover from Ransomware." *IBM Developer,* May 18, 2017. https://developer.ibm.com/storage/2017/05/18/attempting-recover-ransomware/

[78] Santye, Lauren. "The Deep Dark Web: Medical Records Sold on the Black Market." *Contemporary Clinic,* November 16, 2016. https://contemporaryclinic.pharmacytimes.com/news-views/the-deep-dark-web-medical-records-sold-on-the-black-market

[79] Cuthbertson, Anthony. "Hackers Steal Dead People's Medical Records And Sell Them On The Dark Web." *Independent,* July 13, 2018. https://www.independent.co.uk/life-style/gadgets-and-tech/news/hackers-dead-people-medical-records-dark-web-cyber-security-data-a8444851.html

[80] Kehoe, Shawn R. "The Digital Alleyway: Why the Dark Web Cannot Be Ignored." *Police Chief Magazine,* n.d. https://www.policechiefmagazine.org/the-digital-alleyway/

[81] Choudhury, Saheli R. "The 'deep web' may be 500 times bigger than the normal web. Its uses go well beyond buying drugs." *CNBC,* September 6, 2018. https://www.cnbc.com/2018/09/06/beyond-the-valley-understanding-the-mysteries-of-the-dark-web.html

[82] Conditt, Jessica. "FBI hacked the Dark Web to bust 1,500 pedophiles." *Engadget,* January 7, 2016. https://www.engadget.com/2016-01-07-fbi-hacked-the-dark-web-to-bust-1-500-pedophiles.html

[83] Crothers, Brooke. "FBI seizes dark web resource site, major facilitator of criminal activity." *Fox News,* May 11. https://www.foxnews.com/tech/fbi-seizes-dark-web-resource-site-major-facilitator-of-criminal-activity

[84] Santye, Lauren. "The Deep Dark Web: Medical Records Sold on the Black Market." *Contemporary Clinic,* November 16, 2016. https://contemporaryclinic.pharmacytimes.com/news-views/the-deep-dark-web-medical-records-sold-on-the-black-market

[85] Ragan, Steve. "How does a breach like Anthem happen?" *CSO United States,* February 9, 2015. https://www.csoonline.com/article/2881532/anthem-how-does-a-breach-like-this-happen.html

[86] Lord, Nate. "Top 10 Biggest Healthcare Data Breaches of All Time." *Digital Guardian,* June 25, 2018. https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time

[87] Hiltzik, Michael. "Anthem is warning consumers about its huge data breach. Here's a translation." *Los Angeles Times,* March 6, 2015. https://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html

[88] Herman, Bob. "Details of Anthem's massive cyberattack remain in the dark a year later." *Modern Healthcare,* March 30, 2016. https://www.modernhealthcare.com/article/20160330/NEWS/160339997/details-of-anthem-s-massive-cyberattack-remain-in-the-dark-a-year-later

[89] Hiltzik, Michael. "Anthem is warning consumers about its huge data breach. Here's a translation." *Los Angeles Times,* March 6, 2015. https://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html

[90] Ragan, Steve. "How does a breach like Anthem happen?" *CSO United States,* February 9, 2015. https://www.csoonline.com/article/2881532/anthem-how-does-a-breach-like-this-happen.html

[91] Ragan, Steve. "How does a breach like Anthem happen?" *CSO United States,* February 9, 2015. https://www.csoonline.com/article/2881532/anthem-how-does-a-breach-like-this-happen.html

[92] Khandelwal, Swati. "Anthem Data Breach – 6 Things You Need To Know." *The Hacker News,* February 7, 2015. https://thehackernews.com/2015/02/anthem-data-breach.html

[93] Britt, Phil. "6 Lessons Learned from Anthem Data Breach." *eSecurity Planet,* November 5, 2015. https://www.esecurityplanet.com/network-security/slideshows/6-lessons-learned-from-anthem-data-breach.html

[94] Hiltzik, Michael. "Anthem is warning consumers about its huge data breach. Here's a translation." *Los Angeles Times,* March 6, 2015. https://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html

[95] Britt, Phil. "6 Lessons Learned from Anthem Data Breach." *eSecurity Planet,* November 5, 2015. https://www.esecurityplanet.com/network-security/slideshows/6-lessons-learned-from-anthem-data-breach.html