HITECH AND HIPAA'S Impact on the Cybersecurity Posture of the U.S. Healthcare Sector

by

Amy Zuniga

A Capstone Project Submitted to the Faculty of

Utica University

August 2023

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Cybersecurity

Abstract

The purpose of this research was to evaluate ransomware events in the medical industry to develop a three-step strategy to prevent successful attacks that expose patient data. It is in the best interests of the U.S. Government to protect the critical infrastructure throughout the U.S. The Health Care and the Public Health Sector is one of 16 industries in the U.S. protected by the government. It is expedient for the U.S. Government to protect the healthcare industry because it affects Americans' national economic condition and public health and well-being. To improve the availability and ensure the privacy of patient data, the U.S. Government instated the Health Information Technology for Economic and Clinical Health (HITECH) of 2009. Through HITECH, in conjunction with cybersecurity initiatives already enacted in Health Information Portability and Accountability Act (HIPAA), the government mandated non-federal healthcare organizations to transfer hard copies of patient data to electronic record systems. The Healthcare Industry responded to the law, and HITECH effectively improved data availability by pushing valuable patient information online. Nearly 15 years have passed since the legislature passed HITECH, and the rise in ransomware attacks against the healthcare industry from 2016-2021 seemed to illustrate that healthcare organizations struggled with obtaining a strong cybersecurity posture. This paper examines the rise in ransomware attacks, discusses how HIPAA and HITECH protected patient data and considers obstacles healthcare organizations face that block their ability to protect patient data.

Keywords: Dr. Cynthia Gonnella, Cybersecurity, Cyber Law, Cybercriminals, TOR Network, Cyber Attacks, Medicine, Medical Field, Business, Administration, Information Security, Computer Science, Social Science, Cyber Warfare

Table of Contents

List of Illustrative Materials

Statement of the Problem

Dr. Steve G. Langer (2017) of Cleveland Mayo Clinic described how the start of the Health Information Portability and Accountability Act (HIPAA) became the legislating vehicle for directing healthcare providers to move patient medical records to authorized medical centers without betraying patient confidentiality among unauthorized representatives (2017). Kanchan Pant (2022), Professor at GBUA&T, and others discussed in the *Journal of Integrated Care* how the problem with the requirement was that HIPAA did not establish a method to ensure the availability of the information and maintain the data's veracity (2022).

More than ten years later, the American government approved legislation called the Health Information Technology for Economic and Clinical Health (HITECH) of 2009 in connection with the American Recovery and Reinvestment Act (ARRA) (Langer, 2017). According to Shikha Modi (2023), Professor at Auburn University, and others in the journal for *JMIR Medical Informatics*, the HITECH Act revolutionized how healthcare facilities created, used, shared, and managed healthcare data (2023). The *Federal Register* (2009) documented how the HITECH Act in Sections 13400-13424 endeavored to address the privacy and security concerns HIPAA failed to address in connection with the transmission of electronic health record systems (EHR) (2009). According to Health IT.gov (2022), EHR contains an electronic version of a patient's medical history. Healthcare providers manage the EHR to ensure it contains valuable administrative data containing the patient's personal information, clinical data, demographic information, progress reports, problems, treatments, past medical issues, and laboratory and radiographic results.

Anthony Minnaar (2021), Professor of Criminal Justice Studies at the University of Limpopo, South Africa, and others, acknowledged in *The African Journal of Criminology and*

Victimology journal how the new provisions of the HITECH Act addressed the security concerns at the time, yet, in hindsight, the act's security provisions lacked the technical elasticity and scope to prevent the ransomware debacle that occurred when the global surge of successful ransomware attacks climaxed to unprecedented 102% increase during the COVID-19 pandemic (2021). Hillary Tuttle, author of the peer-reviewed magazine *Risk Management*, reported a 71% increase in targeted attacks against US-based providers in October 2020 (2020). Shanying Zhu (2020), an Associate Professor with the Department of Automation at Shanghai Jiao Tong University, and other researchers pointed out how the ransomware attacks of 2020 and the dire consequences of the attacks demonstrate how the diverse coordination of data sharing between multiple technologies, including artificial intelligence and cloud sharing, comprises patient data by leaving the information vulnerable to malicious cyber actors in their article for *The Electronic Library*. Consequently, the development of medical cyber-physical systems, which consists of a network of medical devices connected to a single network, critical to continuous high-quality healthcare, adds another level of vulnerabilities the HITECH Act failed to account for, as Dr. Nilanjan Dey (2018), an Associate Professor in the Department of Computer Science and Engineering, at Techno International New Town Kolkata, India, and other researchers urged in their article for *The Journal of Medical Systems*.

Lorenz Bohn and Dirk Schiereck (2022), researchers for the Technical University in Germany, asserted how many modern attack modes used by cybercriminals today were not even conceptualized, let alone protected, when the U.S. Congress approved either HITECH or HIPAA. Consequently, the U.S. had to establish more laws and infrastructure to respond to the looming number of data breaches due to more active cybercriminals, as Deborah Farringer (2019), Associate Dean for Academic Affairs & Associate Professor of Law at Belmont

University, emphasized. Derrick Tin (2023) of Harvard Medical School, and other researchers, described a data breach as the impermissible use or disclosure that compromises the security or privacy of the Protected Health Information (PHI). By 2015, the U.S. government announced the Cybersecurity Information Sharing Act (CISA) 2015, where, according to Agnes Yang (2020) from the University of Minnesota and other researchers, cybersecurity firms were encouraged to report cyber incidents so the government could disseminate cyber threat information. The idea for CISA was to spread widespread information about data breaches to deter cyber warfare. However, Yang and other researchers observed that although the U.S. Government was working hard to enforce defensive cybersecurity measures across multiple organizations, including healthcare organizations, the legislation backfired. For example, the law seemed to enable cyber security firms to shift the responsibility of enhancing their cyber security initiatives from themselves to the government, and cybercriminals continued their destructive attacks. Thus, the CISA legislation ultimately failed to enhance organizations' cyber defenses, and legislation proved to have minimal impact on preventing cybercriminals from committing their attacks (2020).

T.R. Reshmi (2021), a Scientist at the Society of Electronic Transactions and Security (SETS), observed that ransomware is one of the most prevalent and aggressive forms of cyber threat to digital information. Susan Kiser (2021) of Sam Houston State University and other researchers defined *ransomware* as malignant programs created and utilized by cybercriminals to inhibit computer system access until the victimized host pays a ransom fee. Aaron Zimba (2019), who holds a Ph.D. in Computer Science, and other researchers, maintained that ransomware-as-service (RaaS) organizations, and even un-affiliated malicious actors, can make an outstanding multi-billion-dollar profit if they can manage to hold an organization's information until the

company pays their ransom demands. Hakon Meland (2020) and other researchers from the Norwegian University of Science and Technology explained that RaaS models allow attackers with limited programming skills to participate and earn money through ransomware. For example, a cybercriminal without programming experience will hire RaaS organizations or providers to obtain customized ransomware for their prospective victims. RaaS providers and organizations receive a 20-30% cut of the ransom fee for creating the ransomware. The attacker will then use the customized malware to extract a ransom fee on their victims. Thus, RaaS is a malignantly collaborative method of ransomware because the malware accelerates the infection rate while simultaneously hiding the cybercriminals' identity (2020). Hannah Neprash (2022) of the University of Minnesota, and other researchers, explained that ransomware attacks could also damage the financial reputation of a medical organization if the ransomware enables the malicious actor to gain access to Personally Identifiable Information (PII) from the healthcare organization's employee and patient databases or steals authorization to view a patient's Protected Health Information (PHI). Zhicong Chen (2022), a Professor at the University of Hong Kong, and other researchers maintained how malicious actors often sell PII and PHI on networks such as The Onion Router (TOR) network, otherwise known as the dark web, that uses anonymity to help cybercriminals disguise their identity and make their activity untraceable to government officials. Paul Nadrag (2021), a software developer for Capsule Technologies, warned how the price for PII and PHI on dark web networks could range from $250 to $1000 each, costing organizations around $740,000 to remediate the losses.

While the financial losses incurred by ransomware attacks on medical facilities are significant, it is small compared to the threat it has on the medical provider's ability to care for their patients (Neprash et al., 2022). Neprash et al. drew observations from a study of healthcare

facilities where 44.4% of ransomware attacks against medical organizations caused electronic system downtime and patient care delays (2022). Maxim Chernyshev (2018) of Edith Cowan University and other researchers also discussed how healthcare providers could not access PHI of their patients during the system downtimes that occurred during the ransomware attacks. The research also demonstrated the strain physicians faced as they struggled in vain to access (EHR). Because these physicians had no way to access PHI, they could not make urgent decisions regarding their patient's care, and healthcare organizations that fell victim to ransomware attacks also experienced an increase in patient mortality rates (2018). In addition to the assertions made by Neprash et al. and Chernyshev et al., Proofpoint and Ponemon Institute researchers surveyed more than 600 healthcare facilities where data showed that ransomware attacks intensified patient illnesses, extended hospital stays, and increased mortality rates among healthcare organizations victimized by ransomware attacks (Ponemon Institute, 2021). Thus, ransomware attacks against healthcare organizations threaten healthcare organizations and their patients (2021).

A high-profile example of a ransomware attack that threatened hospitals occurred in February 2016 and should have indicated to U.S. governmental authorities that the HIPAA and HITECH Act alone was insufficient to cover secure PHI or PII from cybercriminals (Minnaar et al., 2021). During the February 2016 attack, cyber criminals used ransomware to encrypt computers at the Hollywood Presbyterian Medical Center in Los Angeles, CA. The cyber attackers demanded a ransom of 3.4 billion dollars in bitcoin and held laboratory work on computers, pharmaceutical computers, and emergency computers offline. Consequently, the healthcare providers sent their patients to other hospitals. Physicians had to write up patient orders by hand and fax patient information between various medical departments. Although the

hospital called in computer forensic experts from the Federal Bureau of Investigations (FBI) and Los Angeles Police Departments (LAPD) to recover the systems, the hospital CEO Allen Stefanek settled with the cyber criminals and paid them $17, 000 in Bitcoin to obtain the decryption key (2021). This prolific ransomware attack illustrated the potential depth of damage a significant ransomware attack could have against the healthcare industry. The incident also should have signaled the need for more extensive security measures to protect against future attacks on America's healthcare system (2021). Adil Hussain Seh (2022) of the Department of Information Technology in Lucknow, India, and others explained how ransomware is the most severe threat to the health industry compared with other cyber incidents because malicious actors predominantly use ransomware to leverage attacks against these organizations.

Cybercriminals also use advanced technology to create ransomware (Chernyshev et al., 2018). Cybercriminals are using a more aggressive ransomware technology called "crypto blockers." Crypto blockers encrypt user data and backup locations so malware writers can more control their system host (Chernyshev et al., 2018). Due to the looming issues surrounding the danger of ransomware, some researchers emphasized how the nation's healthcare infrastructure intensified cybersecurity risk (Farringer et al., 2019). According to Farringer et al., the industry's lack of guidance from the government concerning the communication of risks, threats, and mitigations contradicts the government's efforts to protect patients' PHI (2019). In the past six years, not only has the U.S. government struggled to devise the infrastructure to secure patient data, but cybercriminals have continued their aggressive ransomware attacks on healthcare organizations and gained access to the PHI of 42 million people (Neprash et al., 2022). Meanwhile, Huseyin Tanriverdi (2020), an Associate Professor at the University of Texas, and other researchers attempted to study the antecedents and mitigation mechanics of data breaches

which led them to conclude that it was the complexity of how multihospital systems controlled and managed the data breaches that increased the risk of ransomware attacks within the healthcare industry. However, He Li (2019) of Clemson University and other researchers discovered that healthcare administrators' tendency to have a low budget for security investment funds increased the likelihood of data breaches occurring via ransomware attacks.

Another concern when protecting patient data includes identifying which individuals and third-party organizations are authorized to examine, communicate, analyze, and regulate patient data, as Blake Murdoch (2021) of the Health Law Institute pointed out (2021). A leading factor that invites even further vulnerabilities into the equation is how third-party organizations, such as Google, Apple, IBM, Microsoft, and others, are responsible for equipping healthcare companies with data privacy technology. Gareth Lacobucci (2017), reporter and editor for the general practitioner's *Pulse*, confirmed how, in the past, nations such as Great Britain had seen a rise in healthcare institutions sharing an inappropriate amount of patient data with Google. Zhiyuan Yu (2021), Professor at Pennsylvania State University, and others also emphasized how the sharing of data to third-party vendors increases the attack surface for threat actors to perform their malicious attacks against healthcare information increases with every budding third-party organization promising to provide data protection (2021). The medical industry has proposed and developed technologies to prevent malware attacks. For example, Zhiyan Xu (2020), a researcher from the Hubei Co-Innovation Center of Basic Education Information Technology at the University of Wuhan, China, and other researchers, documented how one medical center investigated creating certificate-less signature schemes to mitigate security issues surrounding patient data's digitalization. However, the developments failed to protect healthcare organizations from malware attacks (2020). Shahid Shah (2020), and other researchers in

the *IEEE Access Journal*, noted that while standards and frameworks help health organizations ensure adequate security, more is needed to meet the demands of ever-evolving malware attacks.

While HITECH expanded HIPAA encryption compliance, requiring healthcare providers and other healthcare associates to expand their reliance on EHR, the U.S. government scrambled to initiate more laws to protect organizations from data breaches (Tin et al., 2023). Although the government created more laws, like the CISA, to encourage organizations to strengthen their cyber defense capabilities, the CISA legislation never seemed to discourage cybercriminals from carrying out cyber-attacks (Yang et al., 2020). Such failures of the government system seem to suggest the best course of action in preventing ransomware attacks for healthcare organizations is to ensure healthcare providers, health information security professionals, and investors collaborate to develop a strategy to strengthen healthcare organizations from disastrous ransomware attacks (Neprash et al., 2022; Yang et al., 2020).

Thus, the general problem is that ransomware attacks remain a primary method of cyber-attacks against medical organizations, making it easy for cybercriminals to steal PII, PHI and withhold vital PHI from healthcare access, as Dr. Christian Dameff (2020) of the University of California – San Diego and other researchers showed. Dr. Fredrik Granholm (2022), adjunct professor at Beth Israel Deaconess Medical Center, and other researchers opined that critical importance it is to alert healthcare providers, researchers, and health information security professionals to the inadequacies of the HIPAA, HITECH, and CISA laws and to help raise awareness of how ransomware attacks affect healthcare provider's ability to care for their patients.

Literature Review

The sources reviewed for this portion considered the research from trade and academic articles, journals, and medical field expertise. The research also documents findings from reports disclosed by regulatory organizations and institutes. The pieces from scholarly and trade journals are peer-reviewed and incorporate a multi-disciplinary diversity that includes medical expertise, economic insight, business acumen, information security standards, and law. Each article combined depicted the current healthcare security environment created by legislative and private organizational measures.

The Growth of Ransomware in the Healthcare Sector from 2016-2021

From 2016-2021 the frequency of ransomware attacks has increased, endangering the healthcare sector (Neprash et al., 2022). In a cohort study of 374 ransomware attacks, data showed how the annual number of ransomware attacks against healthcare entities doubled from 2016-2021 (2022). The cohort study included the year 2020 when the threat of ransomware attacks reached a record point (Minnaar et al., 2021). The surge in ransomware attacks during the COVID-19 pandemic throughout 2020 and 2021 revealed how cyber criminals were sophisticating and evolving ransomware technology into a devastating cyber warfare technique (2021). The rise in ransomware attacks during this time also demonstrated how deadly and consequential a ransomware attack against medical systems could be (Granholm et al., 2022). Cybercriminals targeting healthcare systems during COVID-19 proved to destabilize organizations and societies and reduce the effectiveness and capabilities of healthcare (2022). Studies show the number of successful ransomware attacks increased by 51% from May 2020 – May 2021 as cybercriminals discovered they could increase their profits by launching multiple attacks against healthcare organizations (Minnaar et al., 2021).

By the year mark of May 2020 – May 2021, the international surge of ransomware attacks against the medical industry increased from 187.91 million to 304.64 million worldwide, and in the United States, cybercriminals collected more than 2.1 million dollars from successful ransomware attacks. In addition to increased ransomware attacks, cybercriminals started utilizing a new method of ransomware software called "fileless attacks" where ransomware lodged itself into the target hosts' Random Access Memory (RAM), remaining undiscoverable to antivirus software (Minnaar et al., 2021). The rise in ransomware attacks caused the U.S. federal government to develop a cybersecurity advisory and cautionary bulletin released by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) in conjunction with the Federal Bureau of Investigation (FBI). However, the legislation in place did little to establish a firm standard framework to prevent the growth in ransomware attacks (2021).

While it might be tempting to think the COVID-19 pandemic pandemonium is not a fair indication of the efficacy of HIPAA or the HITECH Act, devastating ransomware attacks against hospitals occurred for years before the COVID-19 pandemic (Minnaar et al., 2021). Certainly, the ransomware attacks against healthcare systems during the 2016-2020 period should have indicated to U.S. government officials the ineffectiveness of the HITECH Act calling on Healthcare organizations to move their data to EHR without proper safeguards in place to prevent massive widespread ransomware attacks (Neprash et al., 2022; Yang et al., 2020; Dameff et al., 2023; Minnaar et al., 2021). For instance, the February 16, 2020, ransomware attack incident against the Hollywood Presbyterian Hospital in Los Angeles, CA, according to Minnaar et al., showed ransomware attackers they could demand any size ransom and receive the ransom and that no organization was inviolable (2021). Cybersecurity professionals, on the other hand, understood that outdated equipment and poorly skilled employees using computers created

a vulnerable security environment. However, many healthcare facilities and even most cybersecurity practitioners at the time believed that ransomware attackers unintentionally attacked hospitals while conducting a general attack on other businesses and organizations (Minnaar et al., 2021). Ryan Witt (2023) healthcare cybersecurity leader at Proofpoint maintained that during the years leading up to covid-19, healthcare CEOs assumed their organizations were caught in a crossfire between cybercriminals aggressive ransomware attacks and their "true target" for the attacks. Thus, because the healthcare sector assumed ransomware attackers did not intend to commit ransomware attacks on their organizations, they failed to establish a strong cybersecurity program to protect PHI and PII (2023). Thus, this limiting mindset ensured that healthcare organizations did little was accomplished in the private or public sector to update the security posture of healthcare organizations (2021).

Minnaar et al. related how in 2018, a ransomware attack from Europe gained access to the EHR and email servers of Hancock Health Hospital, a small hospital in Greenfield, Indiana. The attack spread a ransomware strain called SamSam that encrypted document files and images, including personal and work information. The SamSam attack also encrypted the target computers' configurations and data files so users could not perform their tasks or run applications. The officials at Hancock Health were obliged to pay a ransom to restore their systems. Thus, repeated ransomware attacks against the healthcare industry just prior to the COVID-19 pandemic illustrate how few healthcare organizations worked on updating and improving their security profile during the years leading up to COVID-19. However, healthcare cybersecurity professionals were given unsafe frameworks by the government to respond to ransomware threats, let alone mitigate financial losses incurred from paying the ransom (2021).

Just before the lockdown occurred in March 2020, Minnaar et al., documented how cybersecurity expert and news blogger, Laurence Abrams, reached out to ransomware operators and initiated an agreement where DoppelPaymer and Maze malware strain authors promised to stop targeting healthcare organizations until the pandemic ceased. However, as 2020 progressed, the ransomware attacks against healthcare organizations from these RaaS groups persisted and it was clear to cybersecurity professionals and government authorities that they could not trust the promises they received from ransomware organizations as Maze ransomware attacks continued to encrypt thousands of patients' information. The consequences of the Maze ransomware attacks were devastating. For instance, ransomware attacks forced multiple hospitals to shut down their computers, and doctors had to terminate essential procedures and operations. The ransomware attack also decreased hospital productivity since caregivers could not operate within their facilities. Lastly, the ransomware attacks forced physicians to transfer patients who had even tested positive for COVID-19 to nearby facilities, which exaggerated the overburdened, overfilled, and understaffed hospital and perpetuated the deadly COVID-19 virus (Minnaar et al., 2021). In September 2020, the number of health records exposed increased to 348% compared to the previous month (Minnaar et al., 2021). In October 2020, there was a 71% increase in cyberattacks against hospitals, which continued to increase until CISA declared the ransomware attacks against the healthcare industry a national emergency (2021). Clearly, the U.S. government was overwhelmed by the number of ransomware attacks against healthcare organizations because they did little to mediate or respond to the attacker with the aggression they deserved (Minnaar et al., 2021).

Unfortunately, ransomware attacks against the healthcare sector continue to occur, as Richard Console, Jr (2023), a personal injury lawyer, discussed in an article for a law consulting

blog. For example, on April 11, 2023, Common Spirit Health, an organization responsible for running more than 140 hospitals, reported how a ransomware attack against their EHR exposed the PHI and PII of 623, 000 patients, causing hospital staff to stop admitting patients after a ransomware attack ensued (2023). Thus, the national overwhelm of the ransomware attacks that occurred before, during, and after the COVID-19 pandemic seemed to verify the accuracy of Steve Langer's assertions that neither HIPAA extensions nor the HITECH act did much to prevent the rise in data breaches from ransomware attacks (Langer, 2017; Neprash et al., 2022; Minnaar et al., 2021). For example, a recent Verizon Data Breach study (2023) revealed that successful ransomware attacks continue to grow and have grown 37% just over the past year (2022-2023) with the ransomware demand payment exceedingly over $100, 000, and a 5.3 million average. Healthcare organizations, unfortunately, comprise the largest target for the attacks since 59% of all ransomware attacks occurring in the healthcare sector, according to a 2022 survey conducted by the Healthcare Information and Management Systems Society (HIMSS).

While the rising number of data breaches seemed to testify to the ineffectiveness of HIPAA and the HITECH Act in preventing ransomware attacks against the healthcare sector, not everyone agreed with that sentiment. For instance, Niam Yaraghi (2018), researcher for the Center for Technology Innovation at the Brookings Institution and others opined how the implementation of the omnibus standards led to a reduction of ransomware attacks and worked to prevent 180 data breaches, protecting the PII and PHI of 18 million Americans from cyber criminals. The research maintained and recognized how ransomware attacks were a cause of significant concern because the attacks undermined patient security. They were emphatic when they used empirical data to show that the 2013 adjustments to HIPAA created adequate

regulatory oversight to establish sufficient provisions for maximum privacy protection. Yaraghi et al., maintained that HITECH was an excellent improvement to the HIPAA laws initially because it enabled data synchronization across multiple medical disciplines. However, their research acknowledged how implementing HITECH led to unprecedented challenges as more physicians uploaded PHI and PII to insecure EHR. The research illustrated how one of the challenges of the HITECH law was that there was no way for information security professionals or healthcare professionals to ensure protective security measures were taken as they collected, archived, adjusted, and transmitted PHI and PI (2018).

Hyeyeong Kim (2020), Daegu Haany University, and other researchers determined that HITECH was integral to meeting the health demands of the oncoming crisis the U.S. experienced that increased ransomware attacks because the act improved hospital productivity 2-3 times over. The research also focused on more current data, which led the researchers to agree that HITECH permitted healthcare organizations more flexibility between sharing PHI and PII, increasing productivity. Kim further urged that data breaches that occurred before the 2013 HIPAA changes were due to the inefficient way Healthcare Organizations implemented HITECH (2020). Lorenz Bohn (2022), from the Technical University in Darmstadt, Germany, and other researchers affirmed that HITECH was detrimental because it provided a medium where cybercriminals could exploit sensitive data such as PHI and PII. Unfortunately, the research looked at data returns from short-term stock market research and further studies are necessary to determine the long-range expenses of healthcare organizations adopting HITECH policies and procedures (2022).

What Safeguards did the Legislature Place in HITECH to Protect Patient Data?

RSI (2022) is a premier cybersecurity and compliance provider focusing on helping organizations succeed in risk management. RSI's blog post discusses major HITECH components and how they correlate with HIPAA to build on HIPAA protections. What is essential to understand here is that while HIPAA and HITECH are two separate laws, the HITECH Act in HIPAA most often refers to the changes made to HIPAA by the passage of HITECH. As particular specifications in HITECH further fortified current HIPAA standards and mandated breach notifications, HITECH is sometimes regarded by nonexperts as part of HIPAA. However, it is crucial to understand the Privacy and Security rules in HIPAA to appreciate the influence HITECH had on healthcare organizations entirely. It seems HIPAA has added two new rules establishing penalties for noncompliance and distributing the legislature across a broader demographic in the type of companies that must comply with the new legislature (2022). The goal of creating HIPAA was to protect patient data, and the legislature attempted to do this by adding the Privacy and Security Rule to HIPAA in 2005 and 2006 (2022). The Privacy rule defines PHI and the authorization status of those able to access the PHI. The rule also classified why and how those entities could access PHI. The Privacy rule also attempted to restrict all access to PHI unless those authorized to view the PHI requested the data or in the event of permitted use and disclosure conditions. Finally, the Privacy rule restricted all access to PHI on the principle of least privileged, including limiting and making the data as anonymous as possible, even to authorized persons (2022).

The Security rule established through HIPAA attempted to implement risk analysis and management to encourage confidentiality, integrity, and availability of PHI (RSI, 2022). The new Security Rule then established three frameworks to safeguard PHI. The first safeguard

established administrative precautions to check the management of processes and personnel authorized to access PHI and establish workforce awareness training and evaluation criteria. The second safeguard was to develop physical safeguards to restrict, modify, and control personnel's access to workstations, facilities, and physical devices that contained PHI. The last safeguard was to control access and auditing and ensure the integrity of any hardware, software, or network travel related to PHI and EHR (2022).

Steve Adler (2023), author for the HIPAA Journal, which provides a thorough analysis of the Health Insurance Portability and Accountability Act, discussed how President Barak Obama signed The HITECH Act was signed into law on Feb. 17, 2009, as Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA) stimulus bill. HITECH consists of four components. The first component, called Subtitle A, had two purposes; the first hoped to improve the quality, safety, and efficiency of PHI Access by mandating that healthcare organizations push their PHI and PII to EHR, and the second portion of Subtitle A related to the application and use of health information technology (HIT). Subtitle B focused on the testing of HIT, while Subtitle C focused on grants and funding for loans and grants. The fourth and final component, Subtitle D, had the most significant impact on the healthcare industry because many of its statutes focused on improving HIPAA's Privacy and Security rules (RIS, 2022). The subtitle also established the Breach Notification Rule, which encompassed a series of new regulations related to Business Associate Agreements. Subtitle D also increased criminal penalties for wrongful disclosure of PHI (Adler, 2023).

Prior to HITECH, healthcare organizations were mandated to comply with HIPAA standards; however, because HITECH introduced a new requirement where covered entities and business associates were required to report data breaches and security incidents, HITECH

enabled the Department of Human Services' Office of Civil Rights to enforce penalties for non-compliant organizations (Adler, 2023). HITECH then "persuaded" healthcare providers to adopt (EHR) and achieve privacy and security compliance by increasing penalties for HIPAA and Security rule violations (Adler, 2023). Adopting The Meaningful Use Program (MUP) was an additional challenge. For example, once the legislature passed HITECH, it gave the Department of Health and Human Services (HHS) $25 billion to ensure they met HITECH goals. The HHS used the budget to finance MUP, which used financial incentives to prompt healthcare providers to adopt and certify their organization's EHR. For EHR to qualify as "meaningful," the information had to be used to issue prescriptions or improve the quality of care (Adler, 2023). While the financial incentives were significant and increased as healthcare providers opted to incorporate latest programs, by 2015, Medicare-eligible personnel non-compliant with HITECH EHR standards were penalized by 1%, which increased to 3% by 2017 (Adler, 2023).

HITECH also incorporated new financial penalty levels on non-compliant organizations (Refer to Table 1). The financial penalties depended on the nature of the offense. If hospital organizations were non-compliant for small things, likewise the penalty was small as well. While the maximum financial penalty for noncompliance has increased over the years, the maximum financial penalty as of 2022 was $1,919,173 (Adler, 2023) (see Table 1).

Table 1

Level of Culpability with Violation Type and Penalty Limit

Level of Cupability	Minimum Penalty per Violation Type	Maximum Penalty per Violation Type	Annual Penalty Limit
Lack of Knowledge	$127	$30.133	$30.133
Lack of Oversight	$1,280	$60.97	$121.946
Willful Neglect	12,794	$60.973	$304.865
Willful Neglect not Corrected within 30 days	$60, 972	$1,919.173	$1,919.173

Note. What is the Hitech Act? 2023 Update. HIPAA Journal. (2023, August 11). Tougher Penalties for HIPAA Violations. (https://www.hipaajournal.com/what-is-the-hitech-act/)

The legislature implemented HITECH to transform the healthcare industry, making data transmission more efficient and improving patient care. In hindsight, the U.S. Government accomplished its goal of pushing healthcare organizations to HER adoption. For instance, when the DHS first enforced HITECH upon enactment in February 2009, only 3.2% of organizations incorporated EHR (Adler, 2023). By 2017, 86% of office-based physicians and 96% of non-federal acute care hospitals incorporated EHR. However, the ransomware attacks that occurred from 2016-2023 seem to show that the enforcement of HITECH only enabled ransomware attackers to more easily access vulnerable PHI and PII because the security framework calling for data breach reports was insufficient at significantly protecting patient data despite HIPAA's Privacy and Security rules or HITECH adoption (Langer, 2017; Neprash et al., 2022). Statistics reported by Adler show that the DHS successfully "pushed" 96% of non-federal acute care facilities to adopt EHR but ultimately failed to ensure sufficient security initiatives to prevent ransomware attacks against healthcare organizations (2023).

While holding healthcare organizations liable for non-compliant disclosure of PHI and PII through extensive fines may have improved the organization's internal security, there were no checkpoints in the legislature to ensure patient data was secure from external cyber threats as Azura Stedman (2018) of Utica University discussed in their capstone project. A 2017 Cyber Healthcare & Life Sciences study showed that 47% of providers and health plans had security-related violations or cyber-attacks against their organizations. Jeanne M. Goche (2018), the founder and President/CEO of Solutions in Healthcare Management, reported how hospitals such as the New York and Presbyterian Hospital (NYP) had to pay $3,300,000 to settle for potential violations. However, despite extensive fines and compliance levels, Neprash et al. confirmed there needed to be an objective framework for the government to work with these companies to

ensure the organizations were secure enough to protect themselves against future cyber-attacks (2022). Nevertheless, for whatever reason, the government was intent on preventing cyberattacks by punishing healthcare organizations for violating HIPAA and HITECH (Adler, 2023; Goche, 2018).

The government procedure of fining hospital facilities for HIPAA violations once RaaS organizations published PHI or PII persisted well into the COVID-19 Pandemic and even amplified the consequence of ransomware attacks against healthcare organizations (Minnaar et al., 2021). For example, Grace McDougal (2021), part of the Checkpoint blog's research team, reported how RaaS organizations started initializing a "triple-extortion" threat during the COVID-19 pandemic. In these triple-extortion attempts, the ransomware organizations threatened to publish healthcare organizations' data online, knowing the healthcare organizations would face debilitating governmental fines for violating HITECH and HIPAA standards. Consequently, hospital organizations felt increased pressure to submit ransomware attackers' requests to avoid facing staggering non-compliance fines (Minnaar et al., 2021).

Jason Sewell of Global Engage blog opined how even over time, with its perspective and different technologies in place, seeing ways in which the Internet of Things (IoT) and hospital networks and servers communicate, ensuring the cybersecurity of healthcare systems is excessively evolving and challenging (Sewell, 2021). Thus, in order for HITECH to ensure effectiveness, there should have been more extensive plans in place for government to work along with healthcare organizations to enhance their cybersecurity programs instead of penalizing them for falling victim to aggressive and insidious RaaS organization's cyber-attacks (Minnaar et al., 2021; Reshmi, 2021; Neprash et al., 2022).

The Healthcare Sector Struggles in Establishing Strong Cybersecurity Postures

Broad Attack Surface

Cybersecurity posture describes an establishment's ability to protect their information, networks, and servers from threats, according to Frank Cremer (2022) of the University of Limerick in Ireland and others. Healthcare practitioners do not fully implement cybersecurity practices to improve their security posture because of the broad attack surface (Tin et al., 2023). An *attack surface* is a term used to describe the number of weak spots where an unauthorized user could access or exfiltrate data in a computer or network system, as Sarah Moshtari (2022) and others from the Rochester Institute of Technology defined. Cybercriminals' use of technology increases at exponential rates almost daily. Furthermore, the attack surface and domains are changing, as well. For example, Tin et al. maintained that while cybersecurity professionals up until recently had merely focused on ransomware attacks and various other types of cyber-attacks, there are new types of cyber incidents beyond ransomware attacks that healthcare organizations should be aware of and guard against (2023). For example, cybercriminals are utilizing unmanned aerial vehicles (UAV) as a new attack method, according to researcher Sibi Sethuraman (2019) of Vellore Institute of Technology and other researchers pointed out. Healthcare organizations are increasingly moving toward wireless systems to develop a mobile approach to EHR. Wireless technology in the medical field is the technology behind the wearable Internet of Things (WIoT) and has multiple benefits. For example, physicians can now receive rapid and comprehensive medical data from remote monitoring devices connected to their patients. Wireless technology also has the potential to enhance patients' treatment of chronic conditions. Although WIoT devices are marvelous, the technologies are susceptible to cyberattacks via UAVs. For example, a UAV may hover over

medical centers or clinics and conduct malicious cyber-attacks. When cybercriminals develop UAVs intending to cause cyber-attacks, it can pose a serious risk to healthcare organizations because these UAVs can evade any physical security protocols to perform the attack (2019). Cybercriminals are not just inventing new devices to commit their cyber-attacks but also refining ransomware technology, as Minnaar et al., Neprash et al., Tin et al., and Reshmi et al. pointed out (2021, 2023, 2021).

For example, during the COVID-19 pandemic, cybersecurity personnel discovered a new type of destructive ransomware. As mentioned in this paper, during Covid-19, hospital information security staff dealt with the double-extortion ransomware attack, where cybercriminals would threaten to publish a hospital organization's PHI or PII if the facility failed to pay the required ransom (Minnaar et al., 2021). Another type of aggressive ransomware attack originated during the COVID-19 pandemic. This attack showed the downsides of having a broad attack surface because this ransomware attack did not require a user to activate the attack. Instead, this new ransomware oozed through a computer's operating system and lodged into the target's Random Access Memory (RAM) (Minnaar et al., 2021). Thus, it is difficult for healthcare organizations to anticipate the movements of a cyber-attack and protect against a wide range of attack surfaces. Consequently, it is difficult for healthcare practitioners to implement adequate cybersecurity initiatives to protect PHI or PII (Moshtari et al., 2022).

Limited Funds and Resources

Menaka Muthuppalaniappan (2021) and other researchers at the London School of Hygiene and Tropical Medicine opined that healthcare managers and facilities lack resources to protect against cyber-attacks. Part of the need for more resources stems from the cost and long-term impact of ransomware attacks and cyber incidents. Evolving new Cybersecurity techniques,

such as the new blockchain-enabled security frameworks used to detect and defend against ransomware attacks against IoT devices, are expensive for hospitals to develop and implement, according to Mohammad Wazid (2023) and other researchers from the Department of Computer Science and Engineering at the Manipal Institute of Technology in Manipal, India. According to a Cost of a Data Breach 2022 study conducted by the International Business Machines Corporation (IBM), healthcare organizations had the highest number of breaches related to financial damages of all industries for up to 12 years, with the average cyberattacks amounting to 10.1 million dollars per data breach alone (Tin et al., 2023).

Tin et al. discussed how a lack of financial resources in hospital settings leads to decreased cybersecurity awareness among medical professionals. The research conducted by Tin and others suggested that when hospitals do not allocate the funds necessary to train medical staff, they are at an increased risk of cyber incidents. Additionally, medical staff, including physicians in the emergency department, were the most critical personnel to train because they acted as gatekeepers of PHI and PII. Tin's research further showed that when hospital management allocated resources to train emergency medical staff in how to identify cyber-attacks, phishing emails containing ransomware links, and other modes of cyber-attacks, hospitals were able to mitigate cyber incidents sooner than those organizations who did not correctly fund training awareness programs to emergency personnel (2023). Ideally, the training focus would not extend to emergency physicians but to cybersecurity professionals, emergency department police officers, paramedics, nurses, information security personnel, and administrators (Muthuppalaniappan et al., 2020). It would also be fruitful for hospital administrators to establish a security culture equipped with a fully staffed cybersecurity team to ensure a thorough audit of all individuals accessing HRS (2020).

Unwise Administrative Decisions

Another factor contributing to low cybersecurity posture for smaller healthcare practitioners is administrative decisions, as Mohammad Jalali (2018) of the Massachusetts Institute of Technology in Cambridge, MA, and others discussed. Jalali et al. explained that healthcare organizations are decidedly complex, and healthcare administrators might need technological literacy to make competent decisions regarding cybersecurity. For example, multiple interconnected devices and technology affect the efficiency and effectiveness of medical care. For healthcare administrative teams, it is challenging to attain technological literacy to manage all the devices, especially as individual clinicians procure their technology for their private offices. Even though private care physicians own the computer systems, larger hospital organizations oversee these private healthcare workers. Thus, when these smaller practitioners fall victim to cyberattacks, the larger hospital organizations are liable for these attacks. Consequently, Healthcare administrators need more information and training to develop the foresight and scope to make decisions that positively impact their organization's security posture.

Another way the decisions of healthcare administrators contribute to low cybersecurity posture for healthcare practitioners is through internal politics within the organization. While healthcare organizations function like other companies where there is a solid and functional IT department, Finance Department, and Accounting Departments, there are also specialized medical departments that create a lot of pressure on healthcare practitioner's administrative departments to allocate funds or other resources that might not pertain to developing a strong cybersecurity posture. Regulatory decisions are also part of the healthcare politics that could impact how hospital administrators decide whether or not they want to allocate resources to build

a robust cyber policy. While the broad attack surface, limited funds, resources, and poor administrative decisions may be reasons why healthcare organizations have a poorly developed cybersecurity posture, researchers are at odds when it comes to determining the cause (Tin et al., 2023); Muthuppalaniappan et al., 2020; Jalali et al., 2018). For example, some researchers suggest that weak cybersecurity posture in healthcare organizations stems from deep-seated societal, political, and cultural defects and calls for a significant upheaval of current health organizational procedures (Farringer, 2019). Other researchers believe the cybersecurity risks stem from vulnerabilities from third-party vendors whom hospitals contract to secure hospital networks (Kiser et al., 2021).

On the other hand, other perspectives suggest that moving to remote during the COVID-19 pandemic caused the rise in ransomware attacks from the latter end of 2019 through 2021 (Granholm et al., 2022). Furthermore, other researchers opined that organizations may not fully develop a cybersecurity posture because hospital staff and leadership fail to consider the importance of cybersecurity (Jalali et al., 2018). Other perspectives such as Cremer et al., opined that it is the level of data availability that leads PHI and PII susceptible for ransomware attacks and called for stricter policies to enforce authorization privileges. While there are diverse discussions as to the cause of ransomware attacks, studies conducted before Covid-19, showed only 70% of Hospital boards within the United States included cybersecurity in their risk management surveillance plans. In comparison, only 37% of hospital organizations conducted annual incident response audits (2018). A 2022 study conducted by the HIMSS revealed that up to 61% of healthcare organizations report a lack of professional cybersecurity staff. For the Cybersecurity Report, HIMMS surveyed 159 healthcare cybersecurity professionals that were in some way responsibility for day-to-today cybersecurity operations or oversight. In the survey,

the professionals determined there were multiple barriers to achieving more robust cybersecurity (see Table 2).

Table 2

Barriers to Achieving Robust Cybersecurity

Barriers	Percent
Lack of cybersecurity staff (inadequate numbers)	61.01%
Lack of budget	50.31%
Lack of data inventory (knowing what kind of data we have & where)	44.65%
Lack of data classification (e.g., PHI, PII, IP, etc.)	38.36%
Lack of certain specialized skills for cybersecurity staff	37.74%
Lack of cooperation by people within the organization	31.45%
Policies and procedures do not reflect current practices	30.82%
Lack of awareness about policies and procedures	29.56%
Lack of executive buy-in	22.64%
Lack of interdisciplinary teams	21.38%
Lack of leadership	15.09%
Policies and procedures are difficult to understand	13.84%
Other	2.52%
None – no barriers are present	10.69%

Note. Table Adapted From *2022 HIMSS Healthcare Cybersecurity Survey.* p.13. Copyright 2023 by the Healthcare Information and Management Systems Society

A Proofpoint (2022) study also emphasized how only 57% Healthcare boardrooms have regular CISOs on their administrative teams, compared with 73% in other organizations, with only 23% of administrative boards meeting regularly with CISO's to review cybersecurity reports. Thus, there seemed to be an abundance of systematic challenges that cause the healthcare sector to fail in their ability to develop a strong cybersecurity posture (Neprash et al., 2022; Tin et al., 2022).

Discussion of the Findings

The purpose of this research was to evaluate ransomware events in the medical industry to develop a three-step strategy to prevent successful attacks that expose patient data. The purpose of the research question will be established after examining the literature to get an accurate idea of the cybersecurity issues facing the healthcare sector. How did HIPPA and

HITECH impact the growth of Ransomware across the healthcare sector over the past decade? What safeguards were incorporated into the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 to protect patient data? What are three reasons healthcare practitioners do not fully implement cybersecurity best practices despite awareness of risk to patient data?

The Growth of Ransomware in the Healthcare Sector from 2016-2021

Healthcare organizations oversee massive amounts of information daily. As Tanriverdi emphasized, Healthcare organizations must manage financial issues, coordinate patient care, balance the demands of health insurance companies, and ensure that information is available to multidiscipline healthcare professionals. Consequently, to provide available and confidential information, the U.S. Government instated HIPAA's privacy and security rules to protect patient information, as Adler maintained. In 2009, with the advancements in technology and 3.2% of healthcare organizations already pushing patient data to EHS, the U.S. government added rules to HIPAA, including a new law, the HITECH Act, mandating that non-federal organizations drive patient information to EHR. However, as Minnaar and Neprash concluded, when the legislature passed the HITECH Act in 2009, the law left much to be desired regarding practical ways to ensure PHI remained secure from vulnerabilities. As Granholm discovered, the amount and variety of sellable information harvested from PHI and PII in EHR and the weakly secured electronic health systems (EHS) made the healthcare sector a prime target for cybercriminals.

Soon, As Witt, Neprash, and Minnaar discussed, cybercriminals discovered they could carry out ransomware attacks, and healthcare organizations were more eager than other organizations to pay the ransom to restore their systems quickly. It was initially surprising to learn from Witt’s research that Healthcare organizations were more eager than other industry

leaders to deliver the cybercriminal's ransom request. However, as Tin observed, the risk of suffering reputational damage, and disruption in patient care, combined with facing fines for non-compliance if cybercriminals happened to publish confidential information, are strong motivations for any healthcare organization to succumb to ransomware threats.

Additionally, it seems logical to understand from Minnaar and Neprash's discoveries why cybercriminals increased the frequency and depth of ransomware attacks. Healthcare organizations often need to update their devices that are unpatched and insecure. Another concern is how users of those devices often had varying levels of technology expertise, and ransomware could easily slip past unskilled hospital personnel using insecure devices. Witt explained how toward the end of the pandemic, cybercriminals used software in their ransomware attacks to manipulate healthcare organizations even further by threatening to post PHI and PII on public websites, knowing hospitals would be eager to pay off ransom instead of face penalties enforced by the government for allowing unauthorized exposure to confidential information.

It is crucial to understand why healthcare organizations comply with ransomware attackers' threats and why cybercriminals attack healthcare organizations are the symptom of a deeper problem that healthcare organizations face. In fact, as Bohn maintained, the rise in ransomware attacks from 2016-2021 seems to speak of the institutional failure of the HITECH Act and the fundamental lack of concern by the government for the actual security of patient data. Moreover, HITECH's highhanded way of incentivizing healthcare organizations to jump to EHR without ensuring these institutions were securing these EHS systems makes it seem like the government was more concerned with rewarding bureaucracies and corporations responsible for developing EHS. For instance, organizations were penalized if hospitals did not jump to EHS or

if cybercriminals successfully managed to expose patient data to the public. Thus, the legislature's word choice and construction of the HITECH act seemed to indicate high levels of cyber illiteracy, as if the founders needed to adequately understand the complexity of issues that make it difficult for the healthcare sector to embrace cybersecurity.

Another surprising theme from Minnaar's findings included how aggressive and inhumane organized cybercriminals deploying RaaS, such as the Maze group, can be. For example, during COVID-19, when there were shortages of hospital staff, heavy inpatient numbers, and few professional staff to balance the number of patients, cybercriminals not only continued to increase their vicious attacks against the healthcare sector but made a promise to stop the attacks, that they did not intend to keep. Instead, by late 2020, health records exposed through ransomware attacks increased month by month. Then finally, the U.S. government acted to declare a national emergency because of the aggressive and frequent ransomware attacks against the healthcare industry. Cybersecurity professionals, government officials, and healthcare organization CEOs need to understand the brutality and inhumanity of these cybercriminals, or these criminal entities will continue to increase ransomware attacks.

Moreover, hospital staff and cyber personnel must understand the callous nature of cyber criminals that commit ransomware attacks. Witt's article explained that when CEOs and other cybersecurity experts underestimate cybercriminals' malicious intentions, their organizations are at an increased risk of falling victim to successful ransomware attacks. For example, hospital CEOs and even Abrams underestimated the dangerous nature of these cybercriminals and RaaS organization groups. For instance, when cybercriminals attacked hospital organizations using ransomware before COVID-19, healthcare administrators, and leadership assumed they were not the target of these dangerous ransomware attacks. Astonishingly, it was not until hospitals

received more frequent ransomware attacks that the healthcare industry realized they were the target of these destructive ransomware attacks. Abrams made the mistake of reaching out to RaaS organization leaders in an attempt to make them promise to stop their ransomware attacks against hospitals. It was surprising that Abrams believed he could trust cyber criminals' promises. Thus, as Minnaar pointed out, it seems that if the CEOs from the healthcare sector before COVID-19 understood that ransomware attackers were after the data from their organizations, perhaps they would have allocated more resources to defend against ransomware attacks. Abram's experience shows that cybercriminals do not care if they interrupt patient care, and they do not care if their ransomware attacks are potentially destroying human life.

Still, the evidence of the cybercriminals extending their promise to cease ransomware attacks against healthcare organizations and continue and increase their attacks against hospital organizations illustrates that these cybercriminals are unwilling to cooperate and cannot be trusted. Thus, the increase in ransomware attacks seems to indicate a deep intrinsic problem that the legislature developing the language and laws in HITECH could not have possibly foreseen, although Yaraghi disagreed. Yaraghi maintained that organizations were more susceptible to ransomware attacks when they failed to follow through on HITECH mandates. Yaraghi continued to explain that HITECH reduced ransomware attacks and successfully prevented 180 Data breaches. Yaraghi's study showed that the 2013 adjustments created sufficient provisions for maximum privacy protection. It was interesting to observe that although HIPAA set grounds for a secure environment, Yaraghi's data showed that healthcare organizations and information security teams could not ensure hospital staff followed security protocols as they collected, edited, viewed, and archived patient data.

Surprisingly, Kim and Yaraghi applauded HITECH for increasing the availability of PHI and PII data. However, Kim's data also showed that such availability increased the exposure rate of unauthorized users accessing healthcare data. However, Minnaar, Neprash, and Bohn discussed that by forcing hospital organizations to push their patient data onto EHR or suffer heavy penalizing fines for non-compliance, it seemed as if the government was more anxious to ensure healthcare sectors were using these systems instead of verifying that these systems kept EHR secure.

What Safeguards did the Legislature Place in HITECH to Protect Patient Data?

What is important to understand from the information gathered from the RSI Security blog article is that it is only possible to understand the HITECH law by first understanding the Security and Privacy Rule in HIPAA. The RSI blog emphasized how the new Privacy and Security Rules initiated by the legislature in 2004 and 2005 laid the foundation for cybersecurity. HIPAA's privacy rule defines PHI and individuals and entities authorized to use and handle patient data. The Privacy Rule in HIPAA also created boundaries by restricting access to PHI only to individuals authorized to use or disclose patient information based on least privilege. The RSI Security blog emphasized that the goal of the Privacy Act was to limit access to data and make the data as anonymous as possible, even to authorized entities.

RSI security blog next clarified HIPAA'S security rule and its goal in attempting to implement risk analysis and management of patient data. Thus, the Security Rule encouraged PHI's confidentiality, integrity, and availability. The Security Rule accomplished this goal through a series of standards and frameworks designed to help Healthcare Organizations and other Industries authorized to protect patient data. Researchers, such as Adler, maintained that such initiatives punctuated through the changes in HIPAA reflect the government's anxiousness

to protect patient information. However, as Minnaar, Neprash, Langer, and others discussed, the legislation in HITECH seemed to undermine all efforts to protect patient data.

Adler explained in the research the rulings in the HITECH Act. First, HITECH was separated into a series of subtitles—the first Subtitle called on all non-federal healthcare organizations to push hard copies of patient data onto EHS. Adler discussed how the first component attempted to increase the availability of patient data and to define the application and use of HIT. Here, Neprash, Adler, Bohn, and Langer emphasized that while the provision increased patient data availability to electronic systems, the legislation failed to establish frameworks or standards to ensure the systems were protected. Additionally, instead of defining secure or insecure EHR and environments in the next two subtitles, which would seem to be the most rational approach, the legislature chose to move forward to discuss funding. For example, Adler discussed how the second and third subtitles clarified which entities were eligible to receive grants and funding to push hard copies of patient data to EHS. Finally, in the fourth Subtitle, the legislation attempted to establish a cybersecurity protocol by instituting a breach reporting provision. However, as Neprash and Minnaar maintained, the provision was insufficient to protect patient data. According to Adler, the final Subtitle established the Breach Notification Rule, which encompassed a series of new regulations and business associate agreements for those entities connected in any way to protect patient data and increased criminal penalties for wrongful disclosure of PHI. Adler maintained that although the government-mandated healthcare organizations comply with HIPAA standards, HITECH was unique in that it established the reporting of data breaches and security incidents,

Adler discussed that if healthcare organizations failed to move their hard copies of data to electronic systems or if healthcare faculties experienced a data breach incident, the DHHS forced

healthcare organizations to comply through heavy fees and financial incentives. Another challenge presented itself through the Meaningful Use Program (MUP). Langer's research suggested that the MUP was merely a symptom of massive government overreach because the MUP gave the Department of Health and Human Services (HHS) $25 billion to ensure they met HITECH goals. While it is not uncommon for the U.S. Government to allocate a spending stipend due to new laws, Langer believed the DHS was wrong to use financial incentives to prompt healthcare providers to adopt EHR or face severe financial penalties.

According to Langer, such external pressure from the government ensured that non-federal entities quickly moved their hard copies of patient data without ensuring the EHR systems were secure. By 2017, Adler discovered that 86% of office-based physicians and 96% of non-federal acute care hospitals incorporated EHR, and 96% % of non-federal acute care hospitals incorporated EHR by 2017. Langer complained that patient data was less secure than ever, and predicted cybercriminals would take advantage of the insecure EHR through ransomware attacks. Interestingly enough, the literature established by critics of HITECH and those who sustained HITECH, such as Neprash, Minnaar, Bohn, and Yaraghi, that the availability of patient information established by HIPAA contributed to the growth in ransomware attacks during the 2016-2022 time period. Surprisingly, not all the literature criticized the HITECH law for the increasing availability of patient data on insecure EHR systems.

Researchers like Stedman criticized HITECH security provision for failing to ensure procedures were in place to ensure patient data was safe from external cyber threats. Moreover, by 2017, 47% of providers or healthcare entities suffered security-related violations or cyber-

attacks against their organizations. Goche explained through her research that the government forced non-federal hospitals to pay $ 3,300,000 to settle for HIPAA and HITECH violations.

In addition to heavy fines, Chernyshev discovered that hospital organizations face a staggering amount of internal pressure following large-scale ransomware attacks. For example, during ransomware attacks, healthcare providers cannot access PHI, and thus providers face staggering mental health crises, physicians postpone lifesaving procedures, and patient mortality rates climb. In addition to disruptions in patient care, Minnaar explained how during the COVID-19 pandemic, cybercriminals used HITECH "safeguards" to their advantage during their healthcare ransomware attacks. For example, cybercriminals threatened to publish patient information online if healthcare organizations failed to pay the ransom. Thus, Minnaar opined that cybercriminals use the HITECH provision intended to safeguard patient data as a weapon during ransomware attacks.

On the other hand, Sewell maintained that the founders responsible for HITECH could not have predicted the security issues from advanced technology. Some researchers, such as Langer, believed the government, through HITECH, forced non-federal healthcare organizations to upload patient data to EHR before these entities could establish a secure system and felt the penalties were unjust and prevented the healthcare industry from adequately building a strong cybersecurity posture. Unsurprisingly, there are differences in opinions regarding the government's role in HITECH. For example, Neprash maintained that it was the government's fault for failing to establish a framework in the HITECH Act where healthcare entities could audit for external cyber threats and protect their organization.

In contrast, Langer maintained that private healthcare organizations should be responsible for ensuring their organization's EHR has adequate security through frameworks and standards

established through internal security audits. Nevertheless, it is vital as researchers to understand that the most critical facet in healthcare information technology, as Sewell maintained, is ensuring healthcare information and EHR are secure from cybercriminals despite challenges from private organizations or the government. Therefore, the best course of action shared by Sewell seems to understand how the legislature could improve HITECH's safeguards, if government officials truly understood the limitations faced by hospital organizations.

The Healthcare Sector Struggles in Establishing Strong Cybersecurity Postures

The research Jalali uncovered showed how there are so many categories of data and so many avenues of availability of data in healthcare organizations that the industry struggles to protect. Tin not only acknowledged the issue of securing patient data, but also emphasized that different data sharing technologies also contributed to healthcare organizations having insecure data sharing environments. Thus, Tin urged how healthcare organizations have a broad attack surface that makes it difficult to protect patient data. A broad attack surface means there are multiple avenues of weak spots in a system where cybercriminals or unauthorized users could access and exfiltrate data as Moshtari suggested.

Another area of weakness Tin addresses is that hospitals often use third party vendors to secure patient data and that by using third-party vendors, hospitals introduce a considerable number of vulnerabilities that put their systems at risk for cyber-attacks. A final attack surface Tin mentioned arises when cybercriminals exploit outdated and unpatched systems in healthcare organizations with modern technology. The research Sethuraman discovered maintained that cybercriminals are not only using advanced software to create ransomware, but they are using drones and other technologies to steal patient data. Console discussed how the increased amount

of ransomware attacks after COVID-19 shows that cybercriminals are continuing to exploit the healthcare industry and their techniques will continue to evolve.

Unfortunately, Console emphasized how the constant rise in ransomware attacks against hospital organizations indicates that patient information will continue to be a sellable commodity on the black market. Wazid warned that to meet the demands of such rigorous ransomware attacks, healthcare organizations need to secure cybersecurity professionals who understand the attack surface and how to defend healthcare systems against aggressive ransomware attacks. However, a hospital organization can only build a strong cybersecurity team with proper funds and resources. Wazid also emphasized how the decision to build a cybersecurity team adept at protecting patient data depends on the decision of the hospital's administrative body. Thus, as Minnaar and Neprash maintained, that to fully address the lack of healthcare practitioners failing to establish cybersecurity best practices, it is essential to sift through the research to determine an ultimate solution.

The findings from researchers such as Neprash, Wazid, and Granholm are unique in that it shows multiple perspectives, data, and literature trying to establish why healthcare professionals lack critical cybersecurity. For some researchers, like Tin and Jalali, their data showed that healthcare organizations have a vast amount of patient data available for sharing and described how data sharing technologies contributed to successful ransomware attacks. Other researchers, such as Muthuppalaniappan, Neprash, Console, and Minnaar opined that many hospital organizations allocated limited funds and resources to cybersecurity initiatives, making it challenging to for the hospital's cyber analysts to develop and integrate a robust cybersecurity program fully. Finally, other researchers, like Farringer, Tin, Cremer, Granholm, and Kiser opined that hospital organizations made unwise administrative decisions that led to increased

cybercriminal activities and ransomware attacks. Minnaar also stressed how the varying opinions from the researchers and even the lack of unity when determining why patient data remains unprotected seem to reflect the overall confusing and disunified approach and perspective from those entities responsible for protecting patient data.

Astonishingly, the research presented by Zimba highlighting healthcare organizations having a broad attack surface, limited funds and resources, and unwise administrative decisions impact the protection of patient data, seems to oversimplify those issues surrounding cybersecurity. Rather, those three components seem to be categorizations of the exact problems facing healthcare organizations daily. For example, the HIMSS study establishing more reasons healthcare organizations have challenges adopting best cybersecurity practices does not seem to be additional reasons. Instead, the issues exemplify more detailed explanations for how having a broad attack surface, limited funds and resources, and unwise administrative decisions prevent healthcare industries from developing adequate cybersecurity programs. For example, in the HIMSS study in Table 1, 61% of the 159 participating healthcare organizations attributed inadequate cybersecurity staff as a leading barrier to achieving a solid cybersecurity program.

While initially, it may seem that having few cybersecurity professionals in healthcare organizations is irrelated to broad attack surfaces, limited funds, and resources, or unwise administrative decisions on the part of hospital industries, further analysis of the conclusions from the HIMSS study seems to show that these barriers are consequences of hospital industries having broad attack surfaces, limited funds and resources, or unwise administrative decisions. For instance, as maintained by Tin, Jalali, Muthuppalaniappan Wazid, and Cremer if healthcare industries lack cybersecurity staff, the reason for the lack of staff could be that there are too many vulnerable avenues in the healthcare sector for cybersecurity staff to safeguard

appropriately, or hospital organizations could fail to allocate a sufficient budget to the hiring and retention of cybersecurity staff, or unwise administrative decisions could impact the number of cybersecurity staff hired to secure patient information.

Accordingly, the research seemed to show that every barrier to achieving robust cybersecurity could fall under Broad Attack Surface, Limited Funds and Resources, or Unwise Administrative Decisions (see Table 3).

Table 3

Problems Preventing Healthcare Industry from Implementing Cybersecurity Best Practices

Barriers to Achieving Robust Cybersecurity	Broad Attack Surface	Limited Funds and Resources	Unwise Administrative Decsions
Lack of Cybersecurity Staff	✓	✓	✓
Lack of Budget		✓	✓
Lack of data inventory	✓		✓
Lack of data classification	✓	✓	✓
Lack of certain specialized skills for cybersecurity staff	✓	✓	✓
Lack of cooperation by people within the organization			✓
Policies and procedures do not reflect current practicies		✓	✓
Lack of awareness of about policies and procedures		✓	✓
Lack of executive buy-in			✓
Lack of interdesciplinary teams		✓	✓
Lack of leadership		✓	✓
Policies and procedures are difficult to understand	✓	✓	✓
Other			
None - No Barriers are Present			

Thus, as Minnaar and Neprash emphasized from a cybersecurity perspective, it is essential to ensure that healthcare organizations, including information security staff, healthcare providers, nurses, police officers, and EMTs, are aware of cybersecurity best practice initiatives and receive adequate training to ensure healthcare organizations protect patient data.

In trying to understand the data from the study conducted by HIMSS showing the barriers healthcare industries face that prevent them from having robust cybersecurity, it was surprising to learn that 44% of healthcare practitioners and administrators need help understanding the kind of data their hospitals contain. Another startling revelation was that 44% of the 159 healthcare industries that responded to the required survey needed help understanding where healthcare organizations stored the information. It was also shocking that 38% of the healthcare community

also had trouble when it came to defining or classifying PHI and PII. The data shows that in addition to receiving training, it is clear from the findings in the HIMSS study that hospital organizations must focus on ensuring every staff member has basic cybersecurity literacy. If healthcare staff are unaware of the type of data being exchanged or accessed, hospital organizations can't expect these staff members to secure patient data. It would then be best practice for health information and cybersecurity professionals to ensure that their organizations align their information security strategies and procedures with industry-approved standards and frameworks. It seems from the literature that the complexity of the interconnectedness of EHR means healthcare providers and staff must actively protect PHI from cyber threats as cybersecurity professionals. It is also important that healthcare organizations must train their healthcare professionals and staff members to understand cyber warfare's severe impact on healthcare facilities and strive for organizational awareness to prevent future data breaches.

Another concerning finding from the research worth discussing is the need for cybersecurity awareness in healthcare administrative leadership, as stressed by Wazid and Kiser. The literature from Cremer showed that before COVID-19, only 70% of hospital boards included cybersecurity protocols in their risk management surveillance programs, and only 37% of hospitals even conducted an annual incident response audit. The literature indicates some severe managerial deficiencies when developing a cybersecurity plan. For example, in the HIMSS study, it showed that that hospital boardrooms must consult with cybersecurity professionals regularly, and only 57% of healthcare organizations have CISOs on their administrative teams. That is an astonishing number compared to 73% of non-healthcare organizations reporting using CISO consult with their administrative teams. Therefore, as Minnaar and Neprash emphasized, when it comes down to establishing a probable cause for why healthcare practitioner’s struggle

with creating a strong cybersecurity posture, it is imperative that researchers examine individual healthcare organizations and strive to implement best practices on a case-by-case basis. A three-step strategy to enhance the security posture of healthcare administrators seems to be for hospital administrators and CEOs to increase their hospital's cybersecurity budget, include CISO personnel on hospital boards and decision-making panels, and conduct quarterly cybersecurity awareness training for every hospital staff member. Individual healthcare organizations should build off the three-step approach to meet the cybersecurity needs of their corporation.

Limitations of the Research

Limitations encountered during the research include scope limitations. For example, the research could not adequately cover how healthcare organizations managed their EHR systems before HITECH or discuss the type and frequency of ransomware attacks before implementing HITECH. This research emphasized that although healthcare organizations may face similar issues when developing a cybersecurity program, hospital industries must examine their cybersecurity postures and develop initiatives to help them build strong cybersecurity policies. The research also showed that the government initiated other laws to respond to the rise in ransomware attacks against the healthcare industry. This research paper did not pursue those laws or how those laws impacted healthcare organizations following HITECH.

Future Research Recommendations

How did Healthcare Organizations Move Their Paper Data to Electronic Health Records?

Understanding how healthcare organizations moved their paper data to EHR would be exciting and helpful. The research should have stated if hospital organizations used government authorized EHR to contain patient data or if private hospitals were responsible for securing their EHR portal sites. By understanding the background specifications for the EHR, one would

understand the vulnerabilities inherent in the EHR system. Perhaps understanding the software in EHR would help narrow down the types of patches needed to prevent future ransomware attacks.

How do CISO Consultants Improve Cybersecurity in the Medical Industry?

The studies from the research indicated that 73% of organizations outside of healthcare industries utilize CISO consultants in their administrative teams/boardrooms. Of the Healthcare Industries surveyed, only 57% of users had CISO Consultants to impact leadership decisions. As a researcher, it would be fulfilling to examine how CISO consultants' function in other industries and compare their approach with how CISO consultants operate in medical industries.

How has the U.S. Government Worked with Healthcare Organizations to Prevent Cyber Attacks?

In the years after HITECH, it was clear from the research that the government did try to respond to the rise in ransomware attacks following HITECH. For example, before COVID-19, the U.S. Government instated the Cybersecurity and Infrastructure Security Agency (CISA) Law in 2015 to help organizations reduce cyber risk. On the other hand, during COVID-19, the U.S. Government declared a state of emergency and initiated an advisory and standards to address the rise in ransomware attacks during the pandemic. Thus, examining how the U.S. government has worked with healthcare industries to crack down on ransomware attacks would be eye-opening.

Conclusion

This research aimed to evaluate ransomware attacks in the healthcare industry and determine three reasons why healthcare organizations suffer more severe ransomware attacks than other industries. The research first examined the growth of successful ransomware attacks on the U.S. healthcare industry. Next, the research attempted to examine HIPAA and HITECH Legislation to determine how HIPAA and HITECH contributed to the growth of ransomware

attacks. Finally, the research narrowed down three issues challenging the U.S. healthcare industry's cybersecurity posture.

A major finding of this research was that the HITECH Act did nothing to prevent ransomware attackers from targeting the healthcare industry. Some researchers also opined that HITECH created an unsafe cybersecurity environment that cybercriminals could exploit to access patient data. Patient data remains a marketable commodity on the black market, ranging between $250 and $1000. Thus, when healthcare industries suffer a ransomware attack, it could cause the corporation around $740 000 to remediate the problem. The research indicated that hospital organizations were under extreme pressure when cybercriminals attacked the EHR during COVID-19. For example, hospital organizations were responsible for providing and ensuring their patients receive the maximum level of care and reassurance that their private health information remained safe from unauthorized access. When cybercriminals used ransomware attacks against hospitals, the attack disrupted patient care. There were many instances in the literature where hospitals would delay procedures or transfer their patients to other facilities because successful ransomware attacks disrupted the hospital system. Therefore, protecting patient data and ensuring patient care made healthcare administrators and CEOs quick to meet cybercriminals' demands. The literature followed the critical nature of ransomware attacks on hospital organizations and attempted to alert healthcare researchers, healthcare information security professionals, healthcare providers, and other healthcare staff members to the dangers of ransomware attacks and unsafe cybersecurity practices.

The growth of ransomware attacks before and after the COVID-19 pandemic further emphasized cybersecurity's critical role in protecting patient health information. As of 2022, successful ransomware attacks against hospital organizations continue to climb. Despite the

cybersecurity initiatives in HIPAA, HITECH, and other legislation, hospital organizations needed help developing a strong cybersecurity posture that protects patient data against successful ransomware attacks.

The literature also highlighted the importance of healthcare cybersecurity researchers examining the security and privacy rules instated by HIPAA in 2004 and 2005 in correlation to HITECH. For example, HIPAA's Security and Privacy rules encouraged healthcare organizations to establish best practices in cybersecurity and reduce risk. Thus, when the U.S. government passed and enforced HITECH's Subtitle D, there seemed to be an assumption that reporting cyber incidents would be enough to discourage cybercriminals from targeting healthcare institutions. However, the research showed that despite HITECH, the growth of ransomware attacks against healthcare organizations continued to rise, and it was clear that Subtitle D in HITECH failed to protect patient data from successful ransomware attacks.

It was not HITECH's failure alone that caused the rise in ransomware attacks. Research showed that Healthcare Organizations across the U.S. continue to have challenges adopting best cybersecurity practices. The number of vulnerabilities, limited funds and resources, and unwise administrative decisions from healthcare leaders all contribute to a weak cybersecurity posture in the healthcare industry. Thus, private Healthcare industries can improve their cybersecurity postures by allocating more resources to obtain cybersecurity professionals and CISO consultants who could help organizations develop a strategic initiative to improve the cybersecurity awareness of all healthcare staff.

References

The 2022 board perspective - board of Directors Cybersecurity Views: Proofpoint us. Proofpoint. (2023, June 30). https://www.proofpoint.com/us/resources/white-papers/board-perspective-report

2022 HIMSS Healthcare Cybersecurity Survey. (2023) Healthcare Information and Management Systems Society. https://www.himss.org/sites/hde/files/media/file/2023/04/03/2022-himss-cybersecurity-survey.pdf

2023 Threat Labz state of Ransomware. Zscaler. (n.d.). https://info.zscaler.com/resources-industry-reports-2023-threatlabz-ransomware-report?_bt=650277908305&_bk=enterprise+ransomware+prevention&_bm=b&_bn=g&_bg=155185563548&utm_source=google&utm_medium=cpc&utm_campaign=google-ads-na&gclid=EAIaIQobChMIg9G207WZgAMVsh-tBh3gIAawEAAYAiAAEgKXK_D_BwE

Adler, S. (2023, June 22). What is the Hitech Act? 2023 update. HIPAA Journal. https://www.hipaajournal.com/what-is-the-hitech-act/

Bohn, L., Schiereck, D. (2022). Regulation of data breach publication: The case of US healthcare and the HITECH act. Journal of Economics and Finance, 47(2), 386–399. https://doi.org/10.1007/s12197-022-09607-6

Chen, Z., Jardine, E., Fan Liu, X., & Zhu, J. J. (2022). Seeking anonymity on the internet: The knowledge accumulation process and global usage of the Tor Network. New Media and Society. https://doi.org/10.1177/14614448211072201

Chernyshev, M., Zeadally, S., & Baig, Z. (2019). *Healthcare data breaches: Implications for digital forensic readiness*. Journal of medical systems. https://pubmed.ncbi.nlm.nih.gov/30488291/

Console, R. (2023, April 11). Common spirit health notifies 623,774 individuals of data breach following 2022 ransomware attack. JD Supra. https://www.jdsupra.com/legalnews/commonspirit-health-notifies-623-774-7650462/

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Dameff, C., Farah, J., Killeen, J., & Chan, T. (2020). Cyber disaster medicine: A new frontier for emergency medicine. Annals of Emergency Medicine, 75(5), 642–647. https://doi.org/10.1016/j.annemergmed.2019.11.011

Dey, N., Ashour, A. S., Shi, F., Fong, S. J., & Tavares, J. M. R. S. (n.d.). *Medical cyber-physical systems: A survey*. Journal of medical systems. https://pubmed.ncbi.nlm.nih.gov/29525900/

Farringer, D. R. (2019). Maybe if we turn it off and then turn it back on again? exploring health care reform as a means to curb cyber-attacks. *Journal of Law, Medicine & Ethics*, *47*(S4), 91–102. https://doi.org/10.1177/1073110519898046

Goche, J. M. (2016, September 13). How Cyber Attacks Complicate HIPAA Compliance. Retrieved from http://health-information.advanceweb.com/Features/Articles/How-CyberAttacks-Complicate-HIPAA-Compliance.aspx.

Granholm, F., Tin, D., & Ciottone, G. R. (2022). Not war, not terrorism, the impact of hybrid warfare on emergency medicine. The American Journal of Emergency Medicine, 62, 96–100. https://doi.org/10.1016/j.ajem.2022.10.021

Half of ransomware attacks have disrupted healthcare delivery, JAMA report finds. Healthcare IT News. (2023, January 10). https://www.healthcareitnews.com/news/half-ransomware-

attacks-have-disrupted-healthcare-delivery-jama-report-finds#:~:text=%22In%20terms%20of%20the%20impact,global%20average%20of%2053%25.%22&text=%22This%20cohort%20study%20of%20ransomware,said%20in%20the%20study%20report.

Health and Human Services. (2009). HIPAA administrative simplification: Enforcement. *Federal Register, 74*(209). https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf

Kim, H., & Lee, J. (2020). The impact of health IT on hospital productivity after the enactment of Hitech Act. *Applied Economics Letters*, *27*(9), 719–724. https://doi.org/10.1080/13504851.2019.1644433

Kiser, S., & Maniam, B. (2021). Ransomware: Healthcare Industry at Risk. *Journal of Business and Accounting*, *14*(1).

Lacobucci, G. (2017). Patient data were shared with google on an "inappropriate legal basis," says NHS Data Guardian. *BMJ*. https://doi.org/10.1136/bmj.j2439

Langer, S. G. (2017, January 13). *Cyber-security Issues in Healthcare Information Technology*. Mayo Clinic. https://mayoclinic.pure.elsevier.com/en/publications/cyber-security-issues-in-healthcare-information-technology

LI, H., Yoo, S., & Kettenger, W. (2019, December 15). The Changing Tides of Investments and Strategies and Their Impacts on Security Breaches. Aisel. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1257&context=icis2019

McDougal, G. (2021, June 12). The new ransomware threat: Triple extortion. Check Point Blog. https://blog.checkpoint.com/security/the-new-ransomware-threat-triple-extortion/

Meland, P. H., Bayoumy, Y. F., & Sindre, G. (2020). The ransomware-as-a-service economy within the darknet. Computers & Security, 92. https://doi.org/10.1016/j.cose.2020.101762

Minnaar, A., & Herbig, F. J. (n.d.). Cyberattacks and the Cybercrime Threat of Ransomware to Hospitals and Healthcare Services During the COVID-19 Pandemic. https://journals.co.za/doi/10.10520/ejc-crim_v34_n3_a10

Modi, S., & Feldman, S. S. (2022, September 9). *The value of electronic health records since the Health Information Technology for Economic and Clinical Health Act: Systematic Review*. JMIR Medical Informatics. https://medinform.jmir.org/2022/9/e37283

Moshtari, S., Okutan, A., Mirakhorli, M. (2022). A grounded theory-based approach to characterize software attack surfaces. Proceedings of the 44th International Conference on Software Engineering. https://doi.org/10.1145/3510003.3510210

Muthuppalaniappan, M., Stevenson, K. (2020). Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to Global Health. International Journal for Quality in Health Care, 33(1). https://doi.org/10.1093/intqhc/mzaa117

Murdoch, B. (2021). Privacy and artificial intelligence: Challenges for Protecting health information in a new era. *BMC Medical Ethics*, *22*(1). https://doi.org/10.1186/s12910-021-00687-3

Nadrag, P. (2021, January 26). Industry voices-forget credit card numbers. Medical records are the hottest items on the dark web. Fierce Healthcare. https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in ransomware attacks on US hospitals,

clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum*, *3*(12). https://doi.org/10.1001/jamahealthforum.2022.4873

Pant, K., Bhatia, M., & Pant, R. (2022, September 20). *Integrated Care with Digital Health Innovation: Pressing Challenges*. Journal of Integrated Care. https://doi.org/10.1108/JICA-01-2022-0008

Ponemon Institute. (2021). Cyber Insecurity In Healthcare: The Cost and Impact on Patient Safety and Care.

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks - A systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013. https://doi.org/10.1016/j.jjimei.2021.100013

RSI Security. (2022, June 30). Major components of the HITECH Act: What you should know. RSI Security. https://blog.rsisecurity.com/major-components-of-the-hitech-act-what-you-should-know/

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare data breaches: Insights and implications. Healthcare, 8(2), 133. https://doi.org/10.3390/healthcare8020133

Sewell, J. (2020, January 29). Why is healthcare so vulnerable to cybercrime? Global Engage. https://www.global-engage.com/life-science/why-is-healthcare-so-vulnerable-to-cybercrime/

Shah, S. M., & Khan, R. A. (2020.). *Secondary Use of Electronic Health Record: Opportunities and Challenges*. doi.org. https://doi.org/10.1109/ACCESS.2020.3011099

Stedman, A. (2018). Healthcare is under attack: Investigating the importance of cybersecurity to protect patients and organizations (Order No. 10810058). Available from Dissertations &

Theses @ Utica College. (2042846930). Retrieved from http://ezproxy.utica.edu/login?url=https://www.proquest.com/dissertations-theses/healthcare-is-under-attack-investigating/docview/2042846930/se-2

Sethuraman, S. C., Vijayakumar, V., Walczak, S. (2019). Cyber-attacks on healthcare devices using unmanned aerial vehicles. Journal of Medical Systems, 44(1). https://doi.org/10.1007/s10916-019-1489-9

Tin, D., Hata, R., Granholm, F., Ciottone, R. G., Staynings, R., & Ciottone, G. R. (2023). Cyberthreats: A Primer for Healthcare Professionals. The American Journal of Emergency Medicine, 68, 179–185. https://doi.org/10.1016/j.ajem.2023.04.001

Tuttle, H. (2020). *Risk Management Magazine - Prescription for Disaster*. Magazine. https://web-p-ebscohost-com.ezproxy.utica.edu/ehost/pdfviewer/pdfviewer?vid=2&sid=a88efba2-fc7a-4c3d-9912-b150e76b93a7%40redis

Wazid, M., Kumar Das, A., Shetty, S. (2023). BSFR-SH: Blockchain-enabled security framework against ransomware attacks for Smart Healthcare. IEEE Transactions on Consumer Electronics, 69(1), 18–28. https://doi.org/10.1109/tce.2022.3208795

What is an electronic health record (EHR)? What is an electronic health record (EHR)? | HealthIT.gov. (2019, September 10). https://www.healthit.gov/faq/what-electronic-health-record-ehr

Witt, R. (2023, March 14). *Why healthcare boards lag other industries in preparing for cyberattacks*. Dark Reading. https://www.darkreading.com/attacks-breaches/why-healthcare-boards-lag-other-industries-in-preparing-for-cyberattacks

Xu, Z., He, D., Vijayakumar, P., Choo, K.-K. R., & Li, L. (n.d.). Efficient NTRU lattice-based certificateless signature scheme for medical cyber-physical systems. Journal of medical systems. https://pubmed.ncbi.nlm.nih.gov/32189085/

Yang, A., Kwon, Y. J., & Lee, S.-Y. T. (2020). The impact of information sharing legislation on the cybersecurity industry. Industrial Management & Data Systems, 120(9), 1777–1794. https://doi.org/10.1108/imds-10-2019-0536

Yaraghi, N., Gopal, R. D. (2018). The Role of HIPAA OMNIBUS rules in Reducing the Frequency of Medical Data Breaches: Insights from an empirical study. The Milbank Quarterly, 96(1), 144–166. https://doi.org/10.1111/1468-0009.12314

Yu, Z., Kaplan, Z., Yan, Q., & Zhang, N. (2021). Security and privacy in the emerging Cyber-Physical World: A survey. *IEEE Communications Surveys & Tutorials*, *23*(3), 1879–1919. https://doi.org/10.1109/comst.2021.3081450

Zhu, S., Saravanan, V., & Muthu, B. (2020, December 3). *Achieving Data Security and privacy across healthcare applications using cyber security mechanisms*. The Electronic Library. https://doi.org/10.1108/EL-07-2020-0219

Zimba, A., & Chishimba, M. (2019). On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems. *European Journal for Security Research*, *4*(1), 3–31. https://doi.org/10.1007/s41125-019-00039-8