Cybersecurity Challenges in Healthcare

Aaron Jones

Old Dominion University

CYSE601

11/30/2024

Abstract

The purpose of this paper is to focus on cybersecurity challenges relating to HIPAA compliance regulation and the need for better advancing and securing patient information, data, and privacy with the right level of healthcare employees training and cyber solutions and controls executed on the part of all healthcare people, institutions, organizations, and medical governed entities. This research paper determines a professional level of the statement of the problem, related works, methods of searches, and six security incidents during the COVID-19 pandemic, mainly to ensure a more HIPAA-compliant piece of work delivered with professionalism and success factors. The overall research paper concluded and revealed that healthcare employees and organizations face different types of cybersecurity challenges, including phishing attempts, ransomware attacks, insider threats, and a lot more vulnerabilities, necessitating that medical practitioners and cyber professionals join hands together to fight back against these vulnerabilities with stronger measures in practice. There is also a need for healthcare organizations to stay connected through third-party agreements termed the Business Associate Agreements (BAAs) and Multifactor Authentication (MFA) which ensure patient health information (PHI) is secured with the best safety, security, and reliable methods as well as prevents unauthorized access of PHI according to the HIPAA compliance and regulations. All healthcare organizations must become secure HIPAA-compliant professionals and HIPAA compliance regulation followers with due focus, responsibility, undertaking, and diligence. The future work also suggests that Telehealth and Telemedicine technologies, by enabling secure remote consultations and data transmission, can better protect healthcare employees and institutions from all types of cybersecurity challenges while making them more HIPAA compliant, security protected, employee incident responders, and quick protection assurance with higher due healthcare obligations and successful outcomes.

Introduction

There is a growing concern for dealing with cybersecurity challenges while maintaining HIPAA compliance. It has become quite difficult for healthcare organizations to ensure that patient information is secure, and security rules are followed strictly. There is a significant need to provide employee awareness and training for maintaining security and HIPAA compliance to the strictest level possible. An important question arises how healthcare employees and cyber security professionals can collaboratively maintain the right balance between HIPAA compliance and healthcare technologies to protect patients' data security and privacy? The purpose of this paper is to focus on cybersecurity challenges while maintaining HIPAA compliance, ensuring that patient information, data, and privacy are secure, and security rules are followed together with the right training and awareness are provided to all healthcare employees and cybersecurity professionals, exclusively to maintain security and HIPAA compliance strictly, and diligently.

Statement of Problem

There is now a great lack of security awareness among healthcare workers related to cybersecurity threats and cyber risks. A major strategic action needed to avoid such attacks or breaches is to provide adequate staff communication and training. Healthcare organizations lack policies and reinforcement to secure the behaviors of medical employees to respond quickly and efficiently against such cybersecurity threats (Mia et al., 2022). The vulnerability among healthcare workers related to suffering cyber risks occurs due to the lack of pandemic-focused strict and secure procedures, guidance, documentation, campaigns, and training.

The above sensitive scenario necessitates worldwide healthcare organizations to ensure strong focused coordination for an immediate incident response. The healthcare sector needs to tend to a timeline between detecting the breach and the attack that occurred to reach

the final incident-responsive outcome. The contemporary healthcare cyber defense system has been reactivated and processed to detect all malicious attacks. However, the lack of coordinated incident response has led to the failure of the counteractive response, resulting in malware threats rising over time.

In general, cybersecurity needs to be a team-focused effort from the front-level workforce to the board management officials, thus accounting for cyber risks to the minimum level possible. The research suggests that the healthcare sector faces three different types of cybersecurity threats, such as ransomware attacks, phishing attempts, and insider threats:

A. Ransomware Attacks:

The first threat is ransomware attacks which include the threats that continue disrupting healthcare services, patient records, and networks. An example is the ransomware of the WannaCry attack of UK healthcare system that corrupted the networks and communication systems to a serious level of disruption and then caused failure of the overall healthcare work and performance level.

B. Phishing Attempts:

The second threat is phishing attempts which include errors, mistakes, and viruses in emails and messages. Healthcare employees and workers are often confronted with phishing attempts due to getting bombarded with virus-involved messages and emails, thus putting the entire healthcare network at risk of vulnerability.

C. Insider Threats:

The third threat is insider threats which include the rights and access of the healthcare networks, systems, and technologies getting compromised. The risk factors of insider threats

generally include removing protected health information (PHI) and related confidential information, thus bringing the integrity and privacy of the concerned healthcare organization to great risk and vulnerability (Tekinerdogan et al., 2022). The resulting outcome of insider threats is compromised system integrity, improper disclosure of PHI, employee negligence, data theft, and unauthorized access to patient data and information.

Related Works

The related research work conducted by Adegoke et al. (2022) revealed that cybersecurity challenges have been drastically confronted by healthcare workers concerning HIPAA compliance and patient security, safety, and protection. Many years ago, the HIPAA Act of 1996 was updated with a major change initiated in 2013 related to the Omnibus Ruling Act. Several issues have occurred following such a change among the healthcare practices of medical professionals, thus necessitating the technologies be advanced with the updated HIPAA regulations. This strategic action will strongly help healthcare workers and medical practitioners to comply with and maintain HIPAA regulations with the right security, safety, and protection of patient health information, data, and privacy.

In December 2020, another great related work was initiated to maintain HIPAA compliance and subsequent regulation, such as the issuance of a Notice of Proposed Rulemaking Authority by the Office for Civil Rights (OCR). This notice outlined newly proposed changes to HIPAA compliance, facilitating healthcare workers to secure patient information, privacy, and data more securely, strongly, and perfectly. This work modified the old HIPAA regulations and then made the newer healthcare technologies be practiced and implemented to resolve all cybersecurity problematic situations successfully.

Other related winning work was initiated by the Department of Health and Human Services, revealing the first-ever healthcare provisionary suggestion board to submit the

notice of proposed HIPAA-related cybersecurity threats, sufferings, and risk factors (Elkourdi et al., 2024). This systematic board was ruled and governed with a 60-day comment period where all issues of cybersecurity threats were resolved in connection with the suggestions and feedback received from diversified healthcare organizations, stakeholders, and entities. The final rule-making decision was initiated on the part of the successfully contributing healthcare organizations, thus making the medical policies and healthcare systems run with proper HIPAA compliance and protected patient information, data, and privacy secured and reserved.

Methods

A. Information Sources:

The methods of this research paper exclusively involved conducting research from four major medical, healthcare, and scientific journals, such as ScienceDirect, ResearchGate, PubMed, and The HIPAA Journal.

B. Search Methods:

The search formula used included the key terms “HIPAA compliance, patient information, patient security, patient data, cybersecurity threats, and healthcare security”. Several scholarly articles, news, and reports were reviewed, but only the most related sources were utilized to collect data and information.

C. Timeline of Sources:

The research sources timeline included from 2020 to 2024 to ensure the receipt of the most accurate, updated, and demanding information be added to this research paper,

particularly 5 years old. The sources included updated healthcare trends, facts, and information from the most realistic sources necessary to be reviewed for updated reference.

D. Checklist, Protocol, and Registration:

This research paper was initially completed with a review of course competition requirements, clinical protocols, and registration. Meaning, that the work was concluded with the help of the research paper completed to review the identified HIPAA compliance regulations and patient information security. This strategic action effectively helped in identifying and handling the latest healthcare risks and following modern cybersecurity threats and challenges together with its proposed solutions, strategic safety performances, and reliable medical compliance outcomes.

E. Selection of Sources of Evidence:

The selection of sources of evidence was gathered from the EndNote Library and Purdue which serve as the best referencing and citing management tools. These specific tools helped the research paper reach its top priority concerning the sources cited with a good outlook while not leaving any chance for confusion. The healthcare sources related to HIPAA compliance and patient information security were accessed using these tools.

Results and Discussion

Leading research was conducted from online sources relating to 6 healthcare organizations. It revealed that cybersecurity attacks were misleading and disseminating confidential data to the public via different online platforms. These hackers and cyber

attackers used significant and prominent methods to make the databases and systems of 6 healthcare organizations vulnerable. Most of these attacks were made during the COVID-19 pandemic, particularly involving the cyber threats and risks of malware, distributed denial-of-service attacks, ransomware, and phishing. A brief overview of such cybersecurity challenges and subsequent attacks against 6 healthcare organizations is as follows:

A. Examples of 6 Security Incidents during the COVID-19 Pandemic:

Security Incidents	Type of Attack	Impact and Risk
Brno University Hospital	Ransom ware	Postponements of appointment, surgeries, treatments, intervention, and healthcare facilitative programs
U.S. Health Care Supply Chains	Malware	Disruption of medical facilities and healthcare services
Hospitals in Romania	Ransom ware and phishing	Exfiltration and disruption of healthcare services, networks, and systems
Gilead Sciences, Inc	Phishing	Exfiltration and impersonation of patient's data, information, and privacy

World Health Organization	Phishing and ransom ware	Act of misinformation and defacement
US Department of Health and Human Services	Distributed denial of service	Pandemic responses were dismissed relating to COVID-19 sensitive treatments, scenarios, and interventions

B. Patient Information Breaches and Third-Party Risks:

Throughout the HIPAA compliance consideration, the third-party risk has inadvertently caused a vulnerable risk and patient information breach drastically. Consequently, all HIPAA-covered healthcare organizations are necessitated to ensure entering a third-party agreement termed as Business Associated Agreements (BAAs). This agreement ensures that all patient information, data, and privacy are secured using the utmost safety PHI system while necessitating the strictest level of HIPAA compliance over its regulations. However, it has still been diversely observed that many HIPAA-covered entities are vulnerable and face third-party risks from cybersecurity attacks and challenges.

Some 7 out of 10 huge healthcare data-related breaches occurred through the Optimal Character Recognition (OCR) technology which is significantly utilized in medical services for streamlining patient-related record keeping and patient security of information and care. The Healthcare document automation with Optimal Character Recognition (OCR) technology was affected by cybersecurity attacks, necessitating these healthcare organizations to secure their online platforms and healthcare systems with some digital cyber-secured technologies under HIPAA-compliant regulations (Hom et al., 2022). An example may include the breach

of third-party mail cyber risks caused to 35 healthcare organizations, particularly impacting 2.6 million individuals throughout the channels of cyber risk threats.

More multiple healthcare entities have reported about the cyber risks and threats confronted at their forefront medical services. An example may include the Meta Pixel case which serves as the most cautious storytelling relating to third-party attacks. These affected organizations have been utilizing the Meta Pixel tracker throughout their healthcare systems, networks, and websites to secure their patient data, information, and privacy more strongly. An example of a social media platform causing third-party cybersecurity attacks included Facebook processing patient information and data on the background search. However, Facebook refused such an allegation about the collection of patient data and thus turned into a malicious and suspected online platform to be used for a protected patient data source, system, network, and channel.

The above scenario revealed that HIPAA compliance and cyber risks are exclusively related to patient information, data, and privacy breaches. Many global hospitals are at a vulnerable stage of cybersecurity challenges, necessitating them to use the Meta Pixel and the Business Associate Agreements (BAAs) for a more protected source to fight against all types of cyber risks and threats (Alder, 2024). These two channels and methods can help all healthcare organizations save their networks and systems from getting tracked and user activities facing spoiled. It allows all healthcare organizations to comply strictly with HIPAA-compliant technology and PHI-facilitated systems for great facilitated resources to fight against cybersecurity attacks, risks, challenges, and vulnerabilities.

C. HIPAA Compliance Training for Employees' Education/Awareness to Maintain Security:

i) *Security Training:*

All healthcare organizations must continue conducting frequent online training modules to realize the warning signs of compromised information security, infected linked messages, risk of suspicious emails, and recognition of identity theft. Medical services should be empowered with employees' strong lines of defensive training to deter all types of cybersecurity challenges, attacks, and risks. It may specifically include developing a culture of cyber vigilance and cyber alert training, thus saving all healthcare data, information, and privacy according to the HIPAA compliance regulation, act, and mandate successfully.

All healthcare organizations are required to facilitate and educate their employees with the right HIPAA compliance training exclusively to maintain security against all types of cybersecurity challenges. The employee's training can help all medical services be implemented without disruption, infection, and chaos. All persons and institutions with PHI are needed under the regulation to educate them with the right HIPAA compliance training. This strategic action can help these healthcare organizations to ensure the confidentiality of PHI and security of patient data and privacy at the strictest level possible via the sensitive patient information reporting system.

HIPAA security training and awareness is the right way to avoid violations within healthcare organizations relating to patient health information breaches (Gajwani et al., 2023). All employees and institutions need basic cybersecurity awareness resources to fight against all cybersecurity challenges, risks, and threats. Examples include employees fighting against potential patient information breaches, observing physical security measures, creating strong passwords, identifying scams, and avoiding phishing by not clicking on the unaware or insecure web links sent in emails and online web messages.

ii) *Security Risk Assessment:*

The best way to fight against all cybersecurity challenges is to conduct a security risk assessment to protect patient information, data, and privacy. The first action in a security risk assessment is to cautiously analyze the medical infrastructure to ascertain all possible cyber risks. It will particularly include analyzing healthcare systems' weaknesses, and sensitive software application usage, and examining network configuration with the strong passwords and systems. The healthcare or medical software needs to avoid inappropriate access, entrance, and usage from third-party people or organizations. This strategic action is the most demanding regulation under HIPAA compliance because it does not mandate signing with third-party providers, sharing patient data management systems, or linking patient data networks with any third institution.

iii) *Security-Focused Encryption and Data Protection Strategies:*

There exists a spectrum of ways where healthcare providers can ensure the protection of patient data, information, and privacy to the greatest level possible. This action may include implementing end-to-end encryption, regularly updating encryption keys, and installing strong encryption switches. Such careful reactions on the part of healthcare employees ensure perfect HIPAA compliance and avoid cybersecurity challenges by communicating the right information sufficiently needed for any medical purpose with the greatest protection measures.

iv) *Security-Related Authentication and Access Control:*

Another HIPAA compliance-protected measure is the authentication and access control where unauthorized access to patient data is avoided by protecting the medical systems, healthcare networks, and PHI platforms. It serves as a highly efficient line of

defense against all cybersecurity challenges, such as implementing authentic methods and applying secure access control measures where needed. Another effective method is Multifactor Authentication (MFA) which prevents unauthorized access of PHI and patient privacy and data to the secure level possible. It diminishes cybersecurity risks and threats with the strong protection of exclusively authorized data and information to the right people with uncompromised login credentials. It significantly means that the overall system, network, and platform are secured using a strong encryption method to fight against all types of cyber risks and crimes at the forefront of a giant and reliable cyber technology.

D. Cyber and Healthcare Employees Training Related to Cybersecurity Solutions/Controls:

i) *Apply Endpoint Device Management Tools:*

An effective solution and control for cyber and healthcare employees concerning cybersecurity challenges is to apply end-point device management tools. It may include protecting the healthcare systems against cyber-attacks by applying defensive firewalls, antivirus, and perimeter device systems. It may also include restricting the technology and device usage from healthcare employees with strict security regulations, including HIPAA-compliant laws. It may adapt to secure IoT medical devices to ensure security management with the NIST approach.

ii) *Secure the Remote Work Environment:*

A better way for cyber and healthcare employees to secure healthcare systems, networks, and platforms is to secure a remote work environment that could fight against all

cybersecurity challenges. An effective way is to apply multifactor authentication and a chaotic map-based authentication that could serve as a security-focused framework to remotely work out points of care. The next step is to comply with the NHS attack's surfaced reduction rules by remotely monitoring a perimeter security solution. It may specifically include protecting the healthcare system through the NHS Secure Boundary for enabling secured access controls. The healthcare data needs to be accessed and transmitted through a secure system with encryption rules and strong data protection mechanisms.

iii) *Apply Technical Controls:*

The cyber and healthcare employees should then apply efficient technical controls by isolating the network traffic through the network segmentation process. They should also apply security means of authorization, authentication, and encryption through general technical control systems. They should apply homomorphic encryption that guarantees stronger privacy/security outcomes by applying sensitive medical information and encrypted data analysis. They should afterward facilitate health care interoperability via the blockchain technological system to ensure protected patient information across network systems, thus addressing the data sharing and storage to be secured with effective cryptographic security solutions and control.

Conclusion and Future Work

To conclude this research paper, it can be claimed that around 20 years ago, it was the greatest challenge for healthcare professionals to maintain HIPAA compliance using cybersecurity technology. However, growing progress has been achieved by cybersecurity

technology to secure patient information and privacy data with convenience. The patient's data, security, and privacy are now exclusively protected using the Health Insurance Portability and Accountability Act (HIPPA) which was enacted 30 years ago and has been revised from different time intervals in the forefront of cybersecurity challenges, threats, and risks. Concerning this research paper's overall discussion, it revealed that today's climatic condition causes newer cybersecurity challenges to remain HIPAA compliant. Therefore, Telehealth technology is the only source to use electronic communication and information technology-focused solutions for delivering medical services, diagnosis, treatments, and intervention. Telehealth is the best method for healthcare employees to rapidly increase the safety and security of their healthcare data, information, systems, networks, and websites. It is the only reason that Telehealth technology was excessively used by over 11,718 health institutions between March and April 2020.

As a reference for future work, staying HIPAA compliant today and beyond is an important requirement for all healthcare professionals and institutions. The Notification for Enforcement Discretion relating to Telehealth technology is believed to secure the entire healthcare system and security with strong protective measures. The Office for Civil Rights (OCR) and Telehealth Remote Communications collectively recommend Telehealth secure healthcare's systematic performance, actions, and outcomes while not leaving any chance for compliance. Proper compliance with Telehealth technology can lead to better follow-up with HIPAA security and privacy, thus avoiding breaches of patient information leakage and data privacy from getting ruined in darkness. It can be finally concluded about the future work of healthcare employees and institutions that Telemedicine continues advancing quickly, leading to achieving better patient security control over their privacy, data, and information. Though healthcare business associates face rising pressure, they can still get full control over all cybersecurity challenges with the knack of healthcare information exchange as and where

needed from time to time securely. It all clarifies that HIPAA compliance training remains at the forefront of all healthcare employees and cyber professionals, thus necessitating healthcare employees' training, education, and awareness as have been recommended in this research paper thoroughly.

References

A. Adegoke, N. Achen, F. J. Jordan, and N. J. Jenifer, "Cyber security as a threat to health care," *Journal of ResearchGate and Journal of Technology and Systems,* vol. 4, no. 1, pp.32-64, 2022.

A. Gajwani, A. Shah, R. Patil, D. Gucer, and N. Osier, "Training undergraduate students in HIPAA compliance," *Journal of PubMed,* vol. 30, no. 7, pp. 530-541, 2023.

B. Tekinerdogan, T. Alskaif, A. Boddy, and N. Shone, "Securing electronic health records against insider-threats: A supervised machine learning approach," *Journal of ScienceDirect and Journal of Smart Health,* vol. 26, 2022.

F. Elkourdi, C. Wei, L. Xiao, Z. Yu, and O. Asan, "Exploring current practices and challenges of HIPAA compliance in software engineering: Scoping review," *Journal of ResearchGate and IEEE Open Journal of Systems Engineering,* vol. 99, pp. 1-10, 2024.

J. Hom, J. Nikowitz, R. Ottesen, and J. C. Niland, "Facilitating clinical research through automation: Combining optical character recognition with natural language processing," *Journal of PubMed and Journal of Clinical Trials,* vol. 19, no. 5, pp. 504-511, 2022.

R. Mia, H. Shahriar, M. Valero, N. Sakib, B. Saha, A. Barek, J. H. Faruk, B. Goodman, R. A. Khan, and S. I. Ahamed, "A comparative study on HIPAA technical safeguards assessment of android mhealth applications," *Journal of ScienceDirect and Journal of Smart Health,* vol. 26, 2022.

S. Alder, "One-third of healthcare websites still use meta pixel tracking code," *The HIPAA Journal,* 2024.