Is Healthcare Facing A Silent Epidemic: The Rise Of Cyberattacks?

Durga Chavali[1], Vinod Kumar Dhiman[2], Siri Chandana Katari[3]

[1]Manager, IT Application, Trinity Health, Trinity Information Services, Livonia, USA

[2]Vice President, Information Technology, Deenabandhu Chhotu Ram University of Science & Technology, Sonepat, India

[3]Student, Department of Computer Science and Engineering (IoT), Vasireddy Venkatadri Institute of Technology, Nambur, India

Address for Correspondence: Durga Chavali, durgayc@gmail.com

ABSTRACT: Undesirable consequences, such as the potential harm due to enhanced reliance on electronic platforms, should not be underestimated regardless of the healthcare industry's spectacular growth and the repeatedly applied digital transformation during the COVID-19 pandemic. Healthcare organizations, storing endless documents with very sensitive patient data, have their allure increased among cyber-crooks. The article underlines the fact that hackers find these deficiencies quite appealing, particularly when looking at the slow and unwilling pace of technology adoption and revamping of old systems. Stringent data protection regulations like the Health Insurance Portability and Accountability Act (HIPAA) are catalyzing, cyber-badey organizations into pursuing healthcare systems as their targets for cyber-crime. Healthcare organizations are weakened by the absence of standardized practices for cybersecurity, adoption issues for interoperability, and deficiency in staff training. The article puts the weight on prevention actions as network patching, employee training, and advanced cyber threat detection technologies are vital to protect patient information and provide the high-security standards that correspond the evolving and sophisticated threats.

KEYWORDS: Electronic platforms, Healthcare industry, Data protection regulations, Cyber-crime, COVID-19 pandemic.

INTRODUCTION

The healthcare industry has garnered a lot of attention since the pandemic. Not only the industry has become heavily reliant on technology, it adapted to the new norms the pandemic enforced, such as contactless care, virtual check-ups, and doctor appointments as well as health tracking applications. The healthcare industry has experienced a transformational journey with groundbreaking innovation combined with technology and reshaping the approach to medical treatments, patient care, and disease prevention. There are several components of the healthcare industry such as hospitals, clinics, medical staff, front-line staff, and providers such as insurance and third parties such as record keepers for electronic medical records (EMRs).

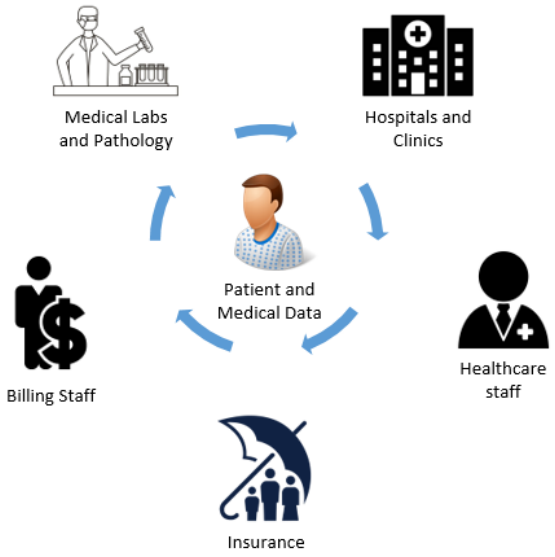


Figure 1. Illustration of different entities that have access to patient and medical data

Healthcare organizations store and process extraordinary amounts of personal and sensitive data of patients in terms of their medical records. This includes full name, email addresses, contact information (phone and physical address), medical history, disease history, social security numbers as well as medications. But why is this data lucrative for hackers? Patient data is gold for hackers in the black market or the Dark Web because it contains a wealth of personal information. The information is also valuable for identity thieves who are looking to create fake identities or conduct targeted phishing attacks. The information could also be utilized by criminals to analyze the type of diseases and health issues people face in a certain region or territory which could then be exploited for various malicious purposes such as bioterrorism or international espionage.

The use of patient data for medical identity theft is not new. Stolen healthcare data can be used to obtain medical services fraudulently. A criminal could use someone else's insurance information to receive expensive medical treatments or prescription medications. Statistically, about 23.9m U.S. residents aged 16 or older have experienced identity theft [3].

Healthcare organizations often struggle with maintaining up-to-date infrastructure due to budget constraints, regulatory compliance challenges, and the critical nature of healthcare services. Hackers very well know that till today majority of the healthcare organizations lean on outdated infrastructure which includes end-of-life hardware, operating systems, and network equipment that are more susceptible to security vulnerabilities. It becomes a cakewalk for hackers to intrude on such legacy systems, specifically when vendor support has ceased as well. Additionally, the rapid evolution of technology also makes it challenging for healthcare organizations to keep pace with the latest security solutions and often contributes to the discouragement these organizations have towards completely overhauling their technology environment, majorly because of backward compatibility issues.

Stringent data protection regulations also make healthcare organizations very attractive targets for hackers seeking to exploit potential weaknesses in technical systems. Non-compliance with data protection regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, can result in substantial fines. The fear of regulatory penalties may drive some organizations to prioritize paying a ransom to avoid legal as well as reputational consequences, creating an additional incentive for hackers.

1.DATA BREACH AND HEALTHCARE ORGANIZATION'S PREPAREDNESS

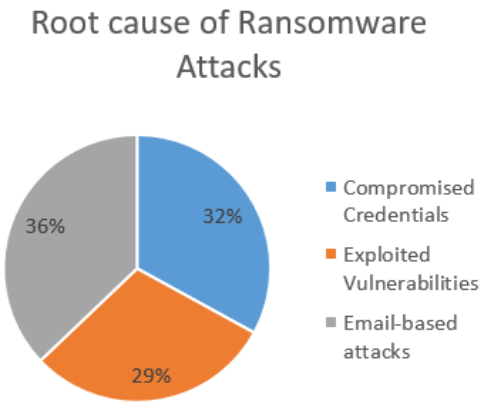
According to a report published in HealthITSecurity [1], data breaches have impacted around 112M individuals in 2023. The growing reliance of healthcare on technology is driven by various factors that aim to improve patient health, streamline operational processes such as insurance as well as enhance efficiencies in providing healthcare services. However, this growing reliance on technology has also resulted in increased exposure of medical records and healthcare data to hackers. According to a report in the HIPAA journal, healthcare providers are the worst hit when it comes to data breaches [4]. A recent cyberattack on a Texas-based healthcare provider impacted around 3.9M patients, where their protected health information (PHI) and medical information such as full names, date of birth, address, medical record number, hospital account number, admission diagnosis, and date(s) and time(s) of service, as well as social security number and diagnostic testing result and medication, were compromised. Class Action Lawsuits were filed against which alleged that "defendants failed to implement reasonable and adequate security measures which left their sensitive data vulnerable to cyberattacks." [2]

Data breaches have been a nightmare for most healthcare providers. It has been historically observed, that although healthcare has drastically adopted technology, it never upgraded it. For instance, many healthcare organizations lack standardized cybersecurity practices and protocols, which leads to inconsistencies throughout the organization. Challenges in interoperability are another struggle healthcare faces, which hinders the seamless exchange of patient information across different systems and healthcare providers. Incompatible health records, caused by interoperability issues, can lead to medical errors, delayed treatments, and compromised patient care. The fragmented nature of health data systems poses challenges in implementing unified security protocols. This results in security vulnerabilities which are usually overlooked, simply because security measures cannot be consistently implemented.

Often it is also seen that healthcare organizations fail to train their staff adequately on security protocols and awareness required to handle PHI data. Insider threats, whether intentional or unintentional, pose a significant security challenge. Healthcare staff including employees or contractors or even healthcare professionals can inadvertently expose sensitive information through actions like sharing passwords, falling victim to phishing attacks, or mishandling data. Such incidents result in unauthorized access to patient data, data breaches, and compromises in the integrity of healthcare systems. Human errors, such as accidental exposure of patient records, can have serious consequences for data security. In 2021, a major U.S pharmaceutical company sued a long-term employee for uploading 12,000 files without permission to a personal account from the company issues laptop before joining a competitor firm [5]. A report from Varonis in 2021 on data risk for healthcare reveals that on average a healthcare worker has access to 31,000 sensitive files on their first day of work [6]

2.THE RANSOMWARE ATTACKS

Another growing concern is ransomware attacks, where malicious actors exploit existing vulnerabilities in the healthcare infrastructure to encrypt sensitive patient data. Such attacks not only disrupt critical healthcare services but also jeopardize patient safety. In 2020, the University of Vermont Health Network fell victim to a ransomware attack, forcing the healthcare system to divert resources from patient care to address the cyber threat. Patient appointments were canceled, and essential services were compromised, highlighting the real-world implications of these attacks on patient well-being. According to a report published by Sophos on The State Of Ransomware Attacks in Healthcare 2023, compromised credentials were the number one root cause of ransomware attacks. Hackers access an organization's network by exploiting weak or stolen credentials. Once inside the network, they can move laterally, escalate privileges, and deploy ransomware to encrypt critical data and demand payment for its release. This is followed by exploiting vulnerabilities in the network and legacy infrastructure as well as applications. And lastly, email-based attacks which include phishing, are the most common type of email attack. Hackers send emails to potential victims that may appear legitimate and often contain links or attachments, which once clicked lead to either fake login pages designed to capture usernames and passwords or download malware to the victim's system, which then gains access to the organizational network.



Such attacks call out the need for the healthcare industry to implement robust cybersecurity measures, including regular security audits, employee training programs, and the use of advanced threat detection technologies. Since staff and employees play a crucial role in cybersecurity, healthcare organizations need to invest in ongoing security awareness training to educate staff about the latest threats, phishing attacks, and best practices for maintaining a secure working environment. Data encryption is also important as an added layer of security for data at rest and in transit, making it more challenging for hackers to use the data maliciously. Developing and regularly testing incident response plans can help mitigate the impact of cybersecurity attacks and take swift action against any such incident.

3.MITIGATION STRATEGIES FOR CYBERSECURITY THREATS WITH THE LATEST TECHNICAL ADVANCEMENTS

A. AI-Enabled Threat Intelligence

AI is on the cusp of the next five years while evolving into the core of the entire threat intelligence process, bringing a completely new paradigm in tackling cyber risks. With an autonomous threat detection and response module, AI is designed to perform data collection, processing, and synthesis. Therefore, the industry finds itself riding a high-speed, completely machine-driven operation. Analysts will have a tremendous reduction in tasks to carry out as AI creates a more relevant position for them to deal with complex problems that only humans can handle. AI integration in threat analysis would bring substantial productivity improvement. It will, in turn, lead to more time being spent on strategic planning, proactive threat hunting, and result-oriented control mechanisms. AI's role in the shift from reactive to proactive cybersecurity will enable organizations to keep up with the level of growing fast-paced cyber threats. In addition, AI-driven systems will also play a major role in the future responsibilities of Level 1 SOC teams, handling the usual tasks and analysts himself/herself concentrating on critical activities such as analysing complex threats and coordinating incident responses. This morphology can be realized by using AI tools such as automated threat detection, behavior analytics, natural language processing, assistance in threat hunting, the sharing of rapid threat intelligence, predictive analytics, and response and mitigation that are automated.

Although AI is a powerful tool in threat intelligence, its prospects should be addressed with concern about the balance between its promises and the ethical, privacy, and accuracy issues. Adopting AI is decisive to transform the field, rebuild jobs, boost efficiency, and further consolidate collective cybersecurity infrastructure, which in turn builds a proactive-based posture for a continuously changing cyber threat environment. The future of the threat intelligence industry is in the combination of AI capabilities and it allows to seek a transformative but needed reaction to the cybersecurity environment changes.

B. Quantum computing cryptography

While the emergence of quantum computing breeds a novel range of obstacles and revolutionary possibilities, the conventional cryptography techniques that were grounded on the use of secure communication are now under attack from the classical quantum computing. Quantum computing (QC)—the method of exploiting quantum mechanics principles analogously—presents a serious risk to the authority of algorithms currently deployed including RSA, ECC, AES, Blowfish, and Diffie-Hellman. Mathematical operations that are very problematic as regards the conventional encryption method such as RSA and ECC essentially depend on the difficulty of factoring large numbers. Moreover, quantum algorithms, particularly Shor's algorithm, rather race to upset these pillars by the extremely swift execution of such calculations. Even though AES and Blowfish have shown their ability to withstand classical computing royal, they have become vulnerable to Grover's method, so their security may even not be guaranteed.

Confronting the emergence of post-quantum cryptography, the concept of post-quantum cryptography has got much attention. These quantum-resistant algorithms will have to be engineered and accepted by all parties to withstand their vulnerability to quantum computers. QKD (Quantum Key Distribution) which is a solution that relies on quantum mechanics, appears as a promising measure to cope with security challenges in key exchange processes. Shifting to post-quantum cryptography is a critical issue for the protection of information confidentiality, availability, and integrity by preserving these five values. It is about a complete appreciation of recent critical cryptographic algorithms

and their performance in the quantum realm. While the quantum computing era unravels itself, cybersecurity specialists should face this shift affirmatively, closely studying and implementing new techniques to have long-term and robust cybersecurity. A timely and responsive strategy of cyber security is a postulate need of the present quantum computing, that keeps the cat-and-mouse gameplay going on with persisting danger.

C. Continuous Monitoring and Anomaly Detection

Since healthcare organizations handle vast amounts of sensitive data, continuous monitoring becomes a real-time approach in proactively defending against cyberattacks on healthcare institutions. It provides constant assessment and analysis of network activities, such as more than usual traffic on a network device, unavailability of data and services as well as unauthorized access. Continuous monitoring enables organizations to identify, analyze, detect, contain, and respond to potential threats as they surface. Real-time threat detection of these threats is required to mitigate and minimize the risks associated with them. By identifying anomalies in time and responding promptly, healthcare organizations can reduce the impact of security incidents if not eliminate them. Early detection through monitoring can significantly limit the damage.

Several security incidents have been brought to light where hackers were able to breach the network using compromised usernames and passwords to access servers and maintained undetected access for several days. Such activities could be prevented and actioned upon in time leveraging robust 24x7 monitoring in place. Lacking continuous monitoring to detect such incidents not only results in sensitive data leaks but also uncovers an organization's non-compliance with cybersecurity regulations as discussed in the next section. Such non-compliance results in organizations being heavily fined and penalized for not having adequate security controls in place to protect data.

REGULATORY COMPLIANCE

Any organization in the United States that stores or processes Protected Health Information (PHI), needs to comply with the Health Insurance Portability and Accountability Act (HIPAA). HIPAA could also be applied internationally when a covered entity or healthcare business shares the PHI with any overseas business or third party. One of the reasons healthcare organizations need to comply with regulations is to protect patient data, due to the sensitivity around it. HIPAA is a US federal law that requires appropriate cybersecurity controls and standards to be set up by organizations dealing with Protected Health Information (PHI). PHI may include information such as medical records, medical history, medicine information, name, number, and email. The overall objective of HIPAA is to secure patient's sensitive information from being disclosed.

A covered entity is any entity or organization that engages in electronic transactions of health information. This includes (1) Health Plan, (2) Healthcare Clearinghouse, and (3) healthcare providers. HIPAA also includes two rules (1) Privacy Rule which is intended to protect sensitive patient information, and (2) Security Rule which specifies the security controls to be in place to protect patient information.

Non-compliance of healthcare organizations with HIPAA can lead to serious financial and legal consequences. Many incidents, such as the one discussed in the above sections have been uncovered where data breaches and cyber-attacks have resulted from hacking into any third party application that is being used by healthcare providers or exploiting any

vulnerability within the healthcare providers network. In some cases, the attack has gone undetected for days, resulting in a vast amount of sensitive data being leaked out. Organizations have paid penalties as high as $1.3m for such non-compliance

CONCLUSION

In this article, we briefly discussed why healthcare is one of the most targeted industries by hackers, and existing privacy and security issues within healthcare, as well as regulations that healthcare organizations need to follow.

As the healthcare sector is experiencing a shift from traditional infrastructure to technology-driven transformation, the security challenges that come along with it cannot be overlooked. Additionally, the pandemic forced the healthcare industry to adopt the new "technology-enabled" norms of working. As healthcare organizations navigated evolving with technology, data security which includes primarily patient data became the priority to protect. Healthcare data is also required to be stored, processed, and used for ethical research purposes to benefit society, where the primary purpose of protecting this data is to protect the interests of the individuals involved. With rapid developments in AI, it is not only the technology that would become increasingly complex, it is also the attack complexity that would need to be comprehended and mitigated. At a time when we have been forced to leave traditional ways of working and adopt technology, we cannot afford to underestimate its downward impacts. Hence, healthcare providers need to invest and implement data security measures such as encryption technologies, access control mechanisms, and continuous monitoring to mitigate and minimize the risks of data breaches, ransomware attacks, and non-compliance.

REFERENCES

[1]. https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches
[2]. https://www.hipaajournal.com/pja-data-breach/
[3]. https://bjs.ojp.gov/press-release/victims-identity-theft-2021
[4]. https://www.hipaajournal.com/security-breaches-in-healthcare/#:~:text=There%20was%20a%2010.4%25%20increase,or%20disclosed%20across%20those%20incidents.
[5]. https://www.reuters.com/business/healthcare-pharmaceuticals/pfizer-sues-departing-employee-it-says-stole-covid-19-vaccine-secrets-2021-11-24/
[6]. https://info.varonis.com/hubfs/Files/docs/research_reports/2021-Healthcare-Data-Risk-Report.pdf