International Journal of Core Engineering & Management
Volume-7, Issue-08, 2023 ISSN No: 2348-9510

DATA PRIVACY, DATA SECURITY, AND CYBERSECURITY IN HEALTHCARE

Anand Laxman Mhatre
anand.mhatre@gmail.com

Abstract

Although digital technologies are streamlining operations in health facilities and enhancing the quality of care, these technologies are vulnerable to data privacy threats such as insider threats, ransomware attacks, phishing attacks, and vulnerability attacks. These attacks have financial, reputational, and operational implications for providers and patients. The good news is that providers can limit their exposure to data privacy threats by assimilating various technologies and practices. This document discusses these technologies and practices.

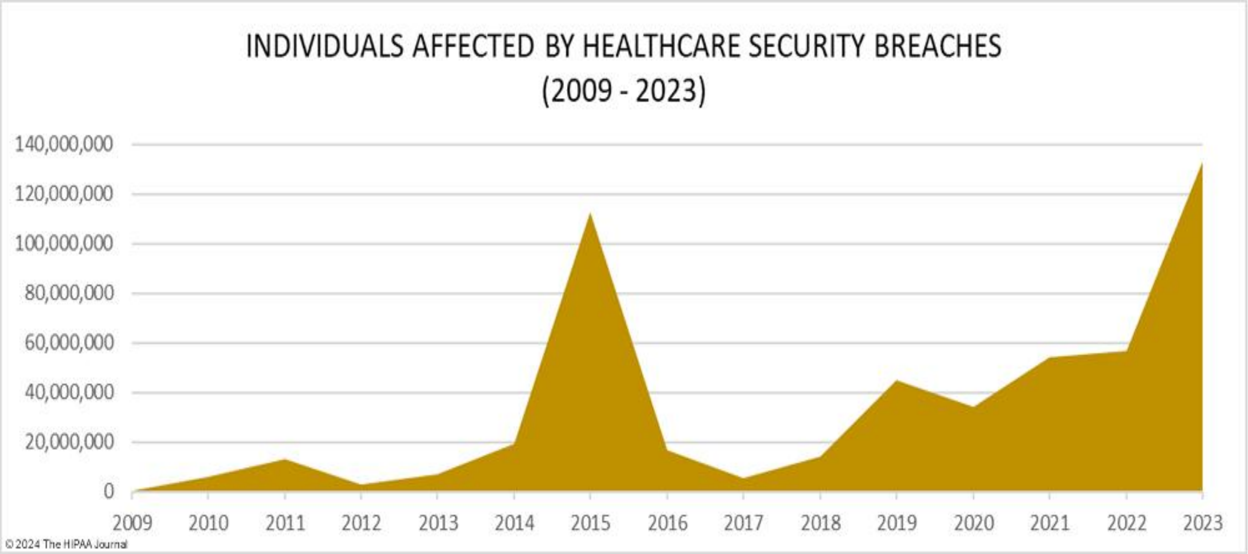
Index Terms: cybersecurity, healthcare, digital technology, data privacy.

I. INTRODUCTION

Digital technologies are increasingly being exploited in the healthcare sector. Today, virtually all patient data is stored in digital formats. Diagnosis of conditions and prescriptions of medications are supported by digital systems. Billing, patient engagement, team collaborations, and administrative tasks have all migrated to digital platforms. The advent of telemedicine and remote care programs has placed digital technologies at the center of patient care. Although the assimilation of digital technologies in healthcare is streamlining operations and increasing the quality-of-care delivery, it comes at a cost – cyber insecurity [1].As patient data move to online platforms, the risk of being accessed or intercepted by cybercriminals increases. For providers to conveniently leverage digital technologies, the danger of data exposure must first be alleviated.

II. CYBERSECURITY AND DATA PRIVACY CHALLENGE

Cybersecurity and data privacy challenges are growing in the healthcare sector. Despite massive investments to curb the problem, insights from multiple sources indicate that the number of patients whose records have been accessed without authorization is growing yearly. According to the HIPAA Journal, between 2017 and 2023, the number of individuals affected by breaches annually grew from less than 10 million to over 130 million, denoting a growth of 13fold in just five years [2]. In 2023, data breaches in healthcare increased by 156 percent to reach 133,068,542, averaging 373,788 breaches per day. It's not just the number of breaches increasing; the scale and impact of breaches are also advancing. According to estimates by Axios, the American healthcare system is losing between $500 million and $1 billion in daily revenue due to cybercrime [3].



Data breaches and cybercrime manifest in various forms. The most common forms in healthcare are;

- **Insider threats:** These are threats that stem from internal staff illegally or maliciously accessing patient data to jeopardize patient privacy or data integrity. Privileged misuse, misdelivery, and miscellaneous errors are forms of insider threats.
- **Ransomware attacks:** These are attacks on healthcare networks that encrypt data with the intention of crippling operations to impel providers to pay a ransom [8].
- **Phishing attacks:** These are social engineering techniques that trick patients or caregivers into revealing sensitive information that attackers use for financial gains. Most healthcare attacks start as phishing attacks.
- **Vulnerability attacks:** These are attacks that target specific points of weakness in healthcare systems. For example, weak authentication protocols.

Cyber insecurity and data breaches have multiple implications for healthcare providers and patients. Providers that suffer breaches may suffer reputational consequences, operations disruptions, innovation and collaboration hurdles, and financial losses in the form of lost funds, legal fees, and penalties. Patients may suffer the loss of privacy and economic losses if their data is used to access their financial accounts. Although it is nearly impossible to completely address cybersecurity and data breach challenges, healthcare facilities can embrace various techniques to improve the impenetrability of their systems.

III. DATA PROTECTION MEASURES IN HEALTHCARE

It is the responsibility of healthcare providers to install mechanisms for proactively protecting against data breaches. Some of the best strategies and technologies healthcare security experts can leverage to enhance their systems' cybersecurity include;

A. Multifactor authentication

Verification and authentication is the first security layer for healthcare systems. Healthcare organizations can enhance the safety of their networks by deploying robust verification and authentication protocols. Multifactor authentication protocols are more secure than single-factor authentication [4]. Healthcare systems with Multifactor authentication protocols safeguard against threats such as brute force and dictionary attacks. The technology is also effective against petty attackers who target user passwords. Ideal multifactor authentication protocols can leverage factors such as traditional passwords and one-time PIN (OTP) sent over an email or an SMS.

B. Access control

This technology allows system users to access resources they only need to accomplish their roles. The technique secures patient data in two ways. If a user account is compromised, attackers cannot access all system resources. The attack is limited to only resources used by the account owners. In case of insider threat, the user can again only access resources within their reach, leaving other system resources secure.

C. Data Encryption

Encryption is a technology that ensures system data remains undiscernible even when compromised. Encryption should be applied to both data at rest and data in transit. Advanced Encryption Standard (AES) and Transport Layer Security (TLS) technologies are ideal for healthcare systems [5].

D. Cybersecurity awareness

According to Infosec, 74 percent of data breaches result from user mistakes [6]. Techniques such as phishing attacks are easy to spot and avoid. Through adequate training, healthcare staff and patients can spot data privacy threats and prevent exposure. For example, they can identify spoofed websites based on URL formats and detect phishing emails based on communication techniques.

E. Intrusion detection systems

Intrusions are inevitable. Regardless of the security features of health systems, intrusions will eventually occur sooner or later. It is paramount for providers to ensure that in case of a breach, intruders are detected before they can cause serious harm to the network. Artificial intelligence intrusion detection systems can be deployed in healthcare networks to monitor suspicious activities and raise an alarm as soon as possible. Some of these systems can be configured to automatically shut down the network to control the severity of attacks.

F. Cloud data servers

In-house data servers tend to be vulnerable to data breaches. The security protocols employed tend to be weak, and the expertise of in-house security teams is usually limited. Healthcare providers can enhance the safety of their patient data by migrating to cloud-based data servers. Cloud data servers are managed by top-notch cybersecurity experts, and the security models leveraged are usually top-class.

Threats	Data protection mechanisms
• Insider threats • Ransomware attacks • Phishing attacks • Vulnerability attacks	• Multifactor authentication • Access control • Data encryption • Cybersecurity awareness • Intrusion detection systems • Cloud data servers

Table summarizing data privacy threats and technologies for increasing cybersecurity

IV. STEPS TO IMPLEMENTING DATA PROTECTION IN HEALTHCARE

Implementing data security is not a random process. It is a structured course guided by a clear understanding of potential data security issues, priorities, and available budget. Key steps to consider when implementing data security are;

- **Understand threat landscape:** This involves assessing the system to understand sensitive data and how it is stored, accessed, and transmitted. Then, potential risks and vulnerabilities are identified, and how they can impact the data.
- **Understand regulations:** It is vital that policies such as HITECH and HIPAA are understood and how they apply to the data stored in the systems. This information can guide data privacy areas that should be prioritized.
- **Involve stakeholders:** Engage system users to gather insights such as regulatory compliance, current policies related to data in systems, and handling processes. Stakeholders can also provide information on potential data privacy areas to prioritize.
- **Select a solution with appropriate costs:** Once the threat landscape is mapped and the objectives and priorities are defined, the next step is purchasing a solution that covers the areas of data privacy identified. It is advisable for the solution to only have the required features. Extra unnecessary features can increase the cost of the solution with no real impact on the organization. It is also recommended that the solution be purchased from vendors with healthcare expertise.
- **Deploy with an iterative methodology:** Implement the solution starting with high-priority areas. Progressive implementation of the solution allows implementation teams to learn and apply the experience in future deployments.

V. IMPACT OF ADVANCED DATA SECURITY MEASURES IN HEALTHCARE SYSTEM

The obvious benefits of having robust data privacy measures in healthcare information systems include;

- Improved patient trust and satisfaction.
- Reduced risk of data breaches and cyberattacks.
- Better compliance with regulatory requirements.
- Enhanced data integrity and accuracy.
- Enhanced capacity for innovation and collaboration.
- Positive reputation and competitive advantage.
- Savings on unnecessary costs in the form of compensations, legal fees, and penalties.

VI. LIMITATIONS

Although the aforementioned strategies can significantly contribute to healthcare digital systems' safety, none can single-handedly guarantee absolute security. For adequate protection, these strategies should be implemented together. Nonetheless, attackers are always looking for new avenues to access healthcare data, making breaches almost inevitable. Consequently, it is a rule of thumb to always back up healthcare data. Besides, healthcare facilities should consider concentrating their cyber efforts on critical infrastructures with low risk tolerance [7]. Such infrastructures include servers that hold sensitive patient data and networks that facilitate communication between providers and patients.

VII. STUDY ASSUMPTIONS

The information and data used to compose this paper are from third parties. It is assumed that the data and information from these studies is credible. It is also assumed that the data owners had no conflict of interest when collecting and analyzing the data. Since we did not have a reliable approach to verify the validity of the data, we only used data and information from reputable sources and peer-reviewed scholarly articles. It is assumed that information from reputable agencies and scholarly articles is trustworthy.

VIII. CONCLUSION

As healthcare providers migrate their operations to online-based platforms, there is a need to install technologies that can protect against data breaches and cyberattacks. Some of the technologies providers can integrate into the systems to guarantee the safety of patient data include multifactor authentication protocols, reliable data encryption technologies, access control techniques, and intrusion detection systems. Data privacy threats can also be contained by raising awareness among care staff and patients on cyberattacks and how to respond to them. Though these approaches are quite effective incontaining data breaches, their efficacy in ultimately safeguarding against data leakages depends on how strategically they are implemented. Providers should understand the threat landscape, regulatory requirements, and security priorities before installing these mechanisms.

REFERENCES

1. Fuentes, M. R. (2017). Cybercrime and other threats faced by the healthcare industry. Trend Micro, 5566.
2. The HIPAA Journal (2024), Security Breaches in Healthcare in 2023. Retrieved From: https://www.hipaajournal.com/security-breaches-in-healthcare/#:~:text=2023%20was%20the%20worst%2Dever,records%20were%20breached%20every%20day.
3. Axios (2024), Health care providers losing up to $1B a day from cyberattack. Retrieved From: https://www.axios.com/2024/03/11/hospitals-doctors-cyberattack-losses
4. Mohamed, T. S. (2014). Security of Multifactor Authentication Model to Improve Authentication Systems. Inf. Knowl. Manag. J, 4, 81-86.
5. Lampropoulos, K., Zarras, A., Lakka, E., Barmpaki, P., Drakonakis, K., Athanatos, M., ... & Khabbaz, M. D. (2023). White paper on cybersecurity in the healthcare sector. The HEIR

solution. arXiv preprint arXiv:2310.10139.

6. Infosec (2023), Human error is responsible for 74% of data breaches. Retrieved From: https://www.infosecinstitute.com/resources/security-awareness/human-error-responsible-data-breaches/
7. Kalyan, C. M. (2024). What are Cyber-Threats, Cyber-Attacks and how to defend our Systems. International Journal of Mechanical Engineering Research and Technology, 16(2), 339-349.
8. Rahim, M. J., Rahim, M. I. I., Afroz, A., & Akinola, O. (2024). Cybersecurity Threats in Healthcare IT: Challenges, Risks, and Mitigation Strategies. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 6(1), 438-462.