World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Protecting patient privacy in the age of smart healthcare: practical cybersecurity measures for individuals and healthcare providers

Oche Joseph Otorkpa [1, *], Ololade Esther Olaniyan [2] and Adefunmilola Adebola Onifade [3]

[1] *Department of Public Health, School of Public Health, Texila American University, Georgetown, Guyana.*
[2] *Department of Applied Statistics and Decision Analytics, Western Illinois University, USA.*
[3] *Department of Family Medicine, Federal University Teaching Hospital, Lokoja, Nigeria.*

World Journal of Advanced Research and Reviews, 2024, 23(01), 3047–3050

Publication history: Received on 23June 2024; revised on 28 July 2024; accepted on 31 July 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.1.2334

Abstract

The rise of smart healthcare technologies, including wearable devices, telemedicine, and the Internet of Medical Things (IoMT), has significantly transformed patient care. However, these advancements have also introduced critical cybersecurity vulnerabilities. This paper explores the escalating threats to patient privacy in the digital age, highlighting substantial increase in cyberattacks on healthcare systems, with data breaches averaging $10.1 million per incident. Analysis reveals several prominent cyber threats to smart healthcare technologies, such as ransomware, phishing, Distributed Denial of Service (DDoS) attacks, Man-in-the-Middle (MitM) attacks, malware, SQL injection, and insider threats, all of which compromise the confidentiality and integrity of patient data. Notably, ransomware attacks have surged by 123% in recent years, severely disrupting patient care and privacy. To mitigate these risks, this commentary proposes actionable cybersecurity measures for both healthcare providers and individuals. Healthcare organizations should conduct thorough risk assessments, implement stringent access controls, encrypt sensitive data, provide comprehensive cybersecurity training for staff, and establish robust incident response plans. Concurrently, individuals are encouraged to remain vigilant about cybersecurity threats, secure their personal devices, use only reputable healthcare applications, be cautious with data sharing, and regularly monitor their health information. By adopting these strategies, both healthcare providers and patients can better safeguard sensitive health information and strengthen the security framework of smart healthcare systems.

Keywords: Smart healthcare; Cybersecurity; Patient privacy; Cyber threats; Data protection

1. Introduction

As the digital revolution continues to permeate every aspect of our lives, the healthcare sector is experiencing unprecedented advancements through smart healthcare technologies (George & George, 2024). These innovations, ranging from wearable devices to telemedicine, promise to enhance patient outcomes, streamline operations, and offer personalized care (Cancela, Charlafti, Colloud, & Wu, 2021). However, with these advancements come significant challenges, especially when it comes to issues of patient privacy because around 92% of healthcare organizations have reported experiencing a data breach in the past three years (Pool, Akhlaghpour, Fatehi, & Burton-Jones, 2024).

The age of smart healthcare promises improved patient outcomes and personalized care but also poses significant cybersecurity challenges (Zeadally, Siddiqui, Baig, & Ibrahim, 2020). In 2023 alone, the healthcare sector saw a 55% increase in cyberattacks and more than 93 million healthcare records exposed or stolen with data breaches costing an average of $10.1 million per incident Choi, Chen, and Tan (2023).

*Corresponding author: Oche Joseph Otorkpa

Smart healthcare technologies are vulnerable to various types of cyberattacks that can compromise patient data and disrupt medical services. Ransomware attacks, which saw a 123% increase in 2023, involve cybercriminals encrypting healthcare data and demanding a ransom for its release, often halting hospital operations (SANS Institute, 2023). Phishing attacks trick healthcare staff into revealing sensitive information or clicking malicious links, leading to data breaches. Distributed Denial of Service (DDoS) attacks flood healthcare networks with traffic, causing service outages that can delay patient care. Man-in-the-Middle (MitM) attacks intercept communications between devices, potentially altering medical data (Aijaz, Nazir, & Anwar, 2021). Malware attacks introduce malicious software into systems, leading to unauthorized access and disruptions. SQL injection attacks exploit application vulnerabilities to access databases, while insider threats from staff can also result in breaches. Advanced Persistent Threats (APTs) involve prolonged network access to steal data or disrupt operations. Furthermore, Internet of Medical Things (IoMT) devices are targeted for their vulnerabilities, leading to unauthorized access. These varied attacks highlights the urgent need for robust cybersecurity measures to safeguard the integrity and availability of smart healthcare technologies (Alshamrani, Myneni, Chowdhary, & Huang, 2019).

A recent study reveals that 72% of consumers are concerned about health data misuse, with lack of informed consent being the top data privacy worry (Medssafety, 2024). Protecting sensitive health information is critical, requiring both healthcare providers and individuals to adopt practical cybersecurity measures.

A compilation of healthcare data breach statistics from 2009 to date revealed a troubling trend, as shown in the figure1 below. There has been a general upward trend in the number of records exposed each year, with a massive increase in 2015. Until 2023, 2015 was the worst year in history for breached healthcare records, with270 unique incidents and more than 112 million records exposed or impermissibly disclosed. This surge in 2015 was particularly severe due to three massive data breaches at health plans: Anthem Inc., Premera Blue Cross, and Excellus. The Anthem breach affected 78.8 million of its members, while the Premera Blue Cross and Excellus data breaches both affected around 10 million individuals (HIPAA Journal, 2024).

2. Healthcare Data BreachesFrom 2009 – 2024 and the Reporting Entity

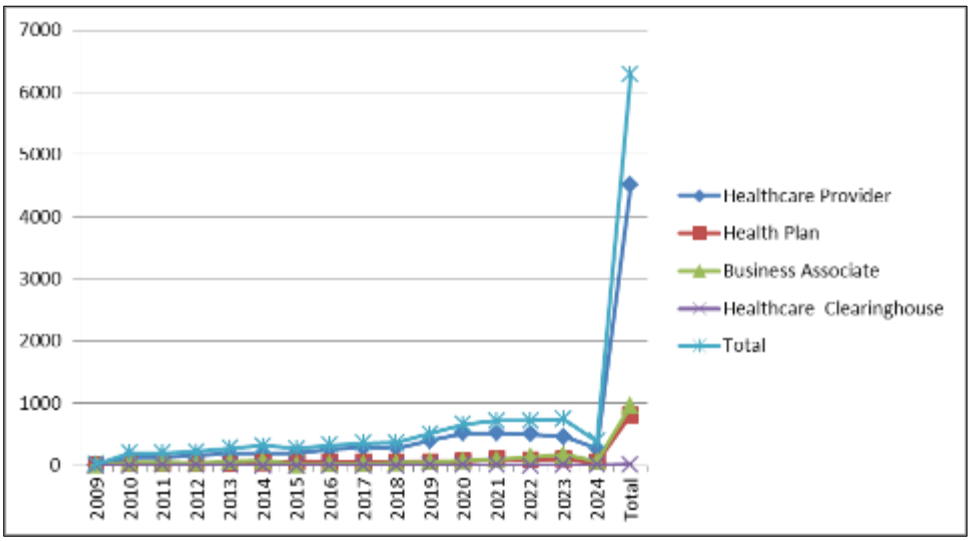

Figure 1 This chart illustrates the increasing trend in healthcare data breaches reported to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) from 2009 to 2024, highlighting significant spikes in breach incidents over the years

3. The Growing Importance of Cybersecurity in Healthcare

The integration of smart technologies in healthcare has led to a dramatic increase in the volume of data generated, stored, and transmitted (Aceto, Persico, &Pescapé, 2020). Electronic Health Records (EHRs), IoMT devices, and cloud-based services have become integral to modern healthcare systems (Mishra & Singh, 2023). While these technologies offer numerous benefits, they also present attractive targets for cybercriminals. Data breaches in healthcare can lead to devastating consequences, including identity theft, financial loss, and compromised patient care (Parkavi, Iswarya, Kirithika, Madhumitha, & Varsha, 2023).

3.1. Practical Cybersecurity Measures for Healthcare Providers

Many cyberattacks begin with a seemingly harmless link, leading to a virus that replicates, a worm that spreads automatically, or a Trojan that hides malware. These threats can infect and compromise software and systems. Healthcare providers bear a significant responsibility in protecting patient privacy (Hall, Bobinski, Orentlicher, Cohen, Bagley, & Sawicki, 2024). Implementing robust cybersecurity measures is essential to mitigate risks and ensure the confidentiality, integrity, and availability of patient data. Key strategies include:

- Comprehensive Risk Assessments: Regularly conduct thorough risk assessments to identify potential vulnerabilities within the organization's IT infrastructure. This involves evaluating hardware, software, networks, and IoMT devices to pinpoint areas of weakness that can be explored by cybercriminals.
- Strong Access Controls: Implement strict access controls to ensure that only authorized personnel have access to sensitive patient data. This includes multi-factor authentication, role-based access controls, and regular audits of access logs are critical.
- Data Encryption: Encrypt data at rest and in transit to protect it from unauthorized access. Encryption ensures that even if data is intercepted or stolen, it remains unreadable without the appropriate decryption key.
- Employee Training: Conduct regular cybersecurity training sessions for all staff members and others with access to critical smart health infrastructure. Educating employees about phishing attacks, password hygiene, and the importance of safeguarding sensitive information can significantly reduce the risk of human error.
- Incident Response Plan: Develop and maintain a robust incident response plan to address potential data breaches promptly. This plan should include procedures for identifying, containing, and mitigating the impact of a breach, as well as notifying affected patients and relevant authorities of the incident.

3.2. Practical Cybersecurity Measures for Individuals

Individuals also play a crucial role in protecting their own health information. As patients increasingly engage with smart healthcare technologies, they must adopt cybersecurity best practices to safeguard their data. Practical measures include:

- Awareness and Vigilance: Stay informed about common cybersecurity threats and be vigilant against phishing attempts, suspicious emails, and fraudulent websites. Recognizing the signs of a potential cyberattack is the first step in preventing it.
- Secure Devices: Ensure that all personal devices, including smartphones, tablets, and computers, are secured with strong passwords and updated with the latest security patches. Enable device encryption and use security software to detect and prevent malware.
- Use of Trusted Apps and Services: Only use healthcare apps and services from reputable sources. Before downloading or using any healthcare-related app, review its privacy policy and user reviews to ensure it handles data securely.
- Data Sharing Awareness: Be cautious about sharing personal health information online or through unsecured channels. When interacting with healthcare providers, verify that their communication methods are secure and encrypted.
- Regular Monitoring: Regularly monitor financial statements and health records for any unusual activity. Promptly report any discrepancies or signs of identity theft to the relevant authorities.

4. Conclusion

The age of smart healthcare brings tremendous opportunities for improving patient care, but it also necessitates a heightened focus on cybersecurity. Both healthcare providers and individuals must take proactive measures to protect sensitive health information from cyber threats. By implementing comprehensive risk assessments, strong access controls, data encryption, employee training, and robust incident response plans, healthcare providers can significantly enhance their cybersecurity posture. Simultaneously, individuals must remain vigilant, secure their devices, use trusted apps and services, be cautious with data sharing, and regularly monitor their information. Together, these efforts will help ensure that the promise of smart healthcare is realized without compromising patient privacy.

Compliance with ethical standards

Disclosure of conflict of interest

The authors have no relevant financial or non-financial interests to disclose.

References

[1] Aceto, G., Persico, V., &Pescapé, A. (2020). Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. Journal of Industrial Information Integration, 18, 100129.

[2] Aijaz, M., Nazir, M., & Anwar, M. N. (2021, December). Classification of Security Attacks in Healthcare and associated Cyber-harms. In 2021 First International Conference on Advances in Computing and Future Communication Technologies (ICACFCT) (pp. 166-173). IEEE.

[3] Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2), 1851-1877.

[4] Cancela, J., Charlafti, I., Colloud, S., & Wu, C. (2021). Digital health in the era of personalized healthcare: opportunities and challenges for bringing research and patient care to a new level. Digital Health, 7-31.

[5] Choi, S. J., Chen, M., & Tan, X. (2023). Assessing the impact of health information exchange on hospital data breach risk. International Journal of Medical Informatics, 177, 105149.

[6] George, A. S., & George, A. H. (2024). Towards a Super Smart Society 5.0: Opportunities and Challenges of Integrating Emerging Technologies for Social Innovation.

[7] Hall, M. A., Bobinski, M. A., Orentlicher, D., Cohen, I. G., Bagley, N., & Sawicki, N. N. (2024). Health Care Law and Ethics:[Connected EBook]. Aspen Publishing.

[8] HIPAA Journal. (2024.). Healthcare data breach statistics. Retrieved July 20, 2024, from https://www.hipaajournal.com/healthcare-data-breach-statistics/

[9] Medssafety. (2024, July 23). Survey reveals 72% of consumers concerned about health data misuse, as lack of informed consent tops data privacy worries. MedsSafety. https://medssafety.com/study-reveals-72-of-consumers-concerned-about-health-data-misuse-as-lack-of-informed-consent-tops-data-privacy-worries/

[10] Mishra, P., & Singh, G. (2023). Internet of medical things healthcare for sustainable smart cities: current status and future prospects. Applied Sciences, 13(15), 8869.

[11] Parkavi, R., Iswarya, M. J., Kirithika, G., Madhumitha, M., & Varsha, O. (2023). Data Breach in the Healthcare System: Enhancing Data Security. In Handbook of Research on Data Science and Cybersecurity Innovations in Industry 4.0 Technologies (pp. 418-434). IGI Global.

[12] Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: a scoping review. International Journal of Information Management, 74, 102719.

[13] SANS Institute. (2023, July 20). Ransomware cases increased greatly in 2023. SANS. https://www.sans.org/blog/ransomware-cases-increased-greatly-in-2023/

[14] Zeadally, S., Siddiqui, F., Baig, Z., & Ibrahim, A. (2020). Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics. PSU research review, 4(2), 149-168.