JIRRS
Journal International Review of Research Studies

Received: 13/06/2026 - **Accepted:** 01/08/2026
Vol: 1.10
DOI: 10.66104/yvw8a115
Pages: 1-10

CYBERATTACKS IN HEALTHCARE AND RATIONALE FOR CYBERSECURITY

Oluwatosin ADEMIJU [1]
1 Bayero University Kano; olu.ade1@gmail.com; https://orcid.org/0002-0000-5692-7261

Corresponding author: olu.ade1@gmail.com

Abstract

Modern healthcare systems have been dominated by virtual approaches and digital technologies. This has increased the concern for security of healthcare devices and data due to lack of information confidentiality and data integrity in this sector. Information category at risk and importance of patient safety make cybersecurity unique in the field of health. Regarding to the context of this problem construction of cyber resilience in healthcare organisation has become a vital task. A comprehensive solution to this problem can be obtained by the combination of human behavioural changes, technological enhancements, process modifications and by new legislations and regulations.

Keywords: Confidentiality; Cyberattacks; Cybersecurity; Cyber-resilience; Healthcare

1. Introduction

Length of life and quality of life are the two dimensions that define health [1]. Healthcare technologies serve as a helping hand to save, enhance, and extend life [2], [33], [34]. Incorporation of latest technology into health sector has increased the precision of healthcare along with an escalation in demand for advanced security [3]. Healthcare is one among the most targeted sectors by the attackers that continually come across evolving cyber threats due to its abundance in valuable data and weak security posture. According to SANS cyber threat report, cyber-attacks were reported by about 94% of healthcare organizations [4], but only a few among the actual number were reported in the public domain while the

others remain undetected or unreported [5], [35], [36].

Even before the emergence of digital technology in the healthcare field privacy breaches were a concern but the increase in interconnectivity has opened multiple doorways for the access[2]. Motivated by financial and political gain cyber-attacks on health industry can be either transnational or state sponsored [2], [5]. In a recent attack against the World Anti-Doping Agency, the attackers released medical reports of eminent athletes [6] but their intention remains unrevealed. Apart from

CC BY

JIRRS
Journal International Review of Research Studies
Received: 13/06/2026 - **Accepted:** 01/08/2026
Vol: 1.10
DOI: 10.66104/yvw8a115
Pages: 1-10

technological vulnerabilities being targeted these forms of attack also exploit human factors, the weakest link in cybersecurity.

Effectual cybersecurity must thus become an inherent part of healthcare organisations. This work aims to explore answers to the following questions:

• Why health sector is being targeted by attackers?

• How healthcare industry become vulnerable?

• What are the risks associated with in healthcare sector and how can it be accessed?

• What counter measures can be taken to enhance healthcare security?

Secondary data was used as a source for the study. Data's were collected from Journals, Reports, Google Scholar database and other online resources. The keyword used for search was cybersecurity in healthcare. From the returned search results full text articles in English language from past few years, which provide precise evidence of the necessity of cybersecurity in the field of healthcare was selected for the data collection.

2. Literature Review

Cyber-attacks start popping up in the healthcare sector during the early 2000's[7] . During the year 2015 about 113 million health records were reported to have compromised and of that 78.8 million were stolen in a single attack [8], [37], [38]. The following years witnessed more attacks and data breaches with sophisticated tools and techniques over a growing attack surface [9]. A study conducted by the world economic forum on healthcare cyber-attacks reveal that the threat plagued the sector during the Covid 19 pandemic [9]. The pandemic accelerated the growth of telemedicine and other digital health facilities [10]. As technology develops and healthcare gets more digitalized the potential risk of cyber incidents also increased [10].

The 2017 WannaCry attack affected about a third of NHS trust in the UK (United Kingdom) [10]. About 80,000 hospitals affected, 7000 appointments cancelled including surgeries and even some emergency departments were shuttered [7], [10]. The study by National Audit Office on WannaCry identified it as an unsophisticated attack and suggested that it could have been prevented by the NHS with basic IT best practices [10]. Most of the affected devices relied on unpatched systems and the attackers made use of

software vulnerabilities within the system. Even though being the world's largest healthcare provider with significant cyber capability, a small negligence resulted to a large loss.

In 2021 May 14, the Health Service Executive (HSE) of Ireland's national health system was affected by a human operated Conti ransomware attack [10]. Detection

CC BY

JIRRS
Journal International Review of Research Studies
Received: 13/06/2026 - **Accepted:** 01/08/2026
Vol: 1.10
DOI: 10.66104/yvw8a115
Pages: 1-10

of malicious activity on the health network disabled several health systems and majority of services were forced to shut down [10]. Healthcare professionals were not able to access the online database and all the health facilities went offline. This incident has made the governing bodies to rethink on the importance for investing on healthcare cybersecurity like all other sectors. 30 servers of Dusseldorf University hospital in Germany were affected by ransom during September 2020 [10]. One death was reported due to patients' ambulance redirected to another hospital [10], [39].

Germany was not severely affected by cyber-attacks that time as adoption to digital health technology was a slow process there [10]. When they began adopting technological innovations, now IT security is mandatory in every health sector in Germany. About 27 major health sector cyber-attacks were reported in the year 2020 by the French media [10]. Ransom attacks such as those affected the Villefranche hospital forced French government to adapt to new cybersecurity standards [10]. They have recently announced to invest in cybersecurity about € 350 million to protect the healthcare infrastructure [10].

Spanish healthcare industry was the one that was worst hit by cyber-attacks during the Covid 19 pandemic. More than 50,000 attacks were reported in 2020 with an average of 430 attacks per week per organization [10]. This has increased to 626 attacks in January 2021 alone. The form of attack varies from phishing emails to more powerful ransomware attacks. Ransomware is identified to be more prevalent in Spain as per studies [10]. Emergency action plans to strengthen cyber defense capabilities were initiated in Spain to curb this situation.

3. Discussion

Information relating to the research questions revealed through the review of literature are as follows:

A. Why health sector is being targeted by attackers?

Health sector poses an incredible amount of data with high monetary and intelligence value [11]. This richness in valuable and immutable data with a weak defence system makes health sector an appealing target for attackers [2]. The targeted particulars include personal identification information, financial details, patients protected health information and data related to medical research and innovation [11]. Availability of immovable specifics within medical records have made them a demanding material in the

dark web and were reported to have sold ten to twenty times faster than credit card credentials [12,13]. Credit card details once stolen can be blocked but a person's identity details remain same forever. Healthcare institutions are usually targeted because through successful attacks that threaten risk to public life, attackers believe that it is more likely for them to demand and get high payments to liberate the

CC BY

JIRRS
Journal International Review of Research Studies
Received: 13/06/2026 - **Accepted:** 01/08/2026
Vol: 1.10
DOI: 10.66104/yvw8a115
Pages: 1-10

details [10]. Scientific innovations in health sector could also be a reason for cyber terrorist and nation state attackers to target the sector [10].

B. How health sector become vulnerable?

Innovations in healthcare technology have introduced many devices that play critical role in modern healthcare. Most medical devices are not designed with security in mind, they are just made to perform a single purpose [14]. Even though medical devices will not store any data the extensive network of interconnected medical devices open an entry point for attackers to initiate attack on the server that holds data [15].

Healthcare industry provides best solution for patient health issues through collaborative working of different units [14]. This involves data access both onsite and remotely and on multiple devices [14]. The urgent nature of medical industry to share information may not have time to consider the security implications of the devices being used [14], [40], which can put the whole organisation under risk. Health industry is one among the largest employment provider so risk due to human error cannot be excluded [10]. The healthcare professionals are well trained for their job, but they are not educated on best cybersecurity practices. The lack of knowledge and expertise in online security practices can result in increased human errors contributing to rise in opening gateways for data breaches. The year 2017 alone marked about 46% of data breaches due to human error [16], [33].

Even though the medical technology has advanced incredibly, not every aspect of healthcare sector has followed this pace [14]. With greater emphasis on patient care, the health sector lacks funding for IT infrastructure [5] and continue to use inherent system that are outdated, such as Windows XP that stopped support since 2014 [17]. This negligence in software updates and system security aids attackers and malwares to keep away from early detection. In addition to all this, factors such as narrow resources, shattered governance and societal behaviour also combines to make health sector vulnerable to cyber-attacks [5], [35].

C. What are the risks associated with healthcare sector?

The healthcare sector is affected with countless cyber related issues varying from malware attacks to distributed denial of service attacks [18]. All these attacks present unique challenges to the healthcare sector as people's life are threatened apart from monetary loss and privacy breach [18]. Mostly observed and emerging threats in health sector includes the following:

• Data theft for financial gain - where a person's personal data is stolen for economic gain.

• Data theft for impact - medical records of highprofile people are stolen and released publicly.

• Ransomware – malwares are used to block users from accessing a system or threatening to delete data from system unless the demand for money is met.

CC BY

JIRRS
Journal International Review of Research Studies
Received: 13/06/2026 - **Accepted:** 01/08/2026
Vol: 1.10
DOI: 10.66104/yvw8a115
Pages: 1-10

• Denial of service attack – disrupting a network or system by flooding it with surplus requests with a motivation of blackmailing, revenge, or activism.

• Business email compromise – creating fake personal communication with an aim of financial gain.

• Insider attack – system disruption or data loss due to intentional or unintentional insider activity within the sector.

• Third party vendors – Healthcare being a vast sector recruit vendor for certain jobs' such as cleaning. They may also be provided access to the organizational network, without accessing the accompanying risk [19].

• Poor disposal of old hardware – Even after deleting or reformatting the data on the hardware it is possible to retrieve the data within it [19]. So, poor disposal of hardware with health records can also make health industry vulnerable to attacks.

• Lack of security of online medical devices – As the growth of Internet of Medical Things (IoMT) increased, devices are designed to share data to world outside the doctor's room [19]. Thus, chances for hackers to gain access to data and manage or manipulate it is more.

• Unrestricted and unsecure access to healthcare systems and mobile devices - Necessary security standards are not always met when personal devices are accessed [19]. Similarly, open computers connected to sensitive information can be accessed by unauthorized users [19]. All these serve as helping hands for attackers to intrude into the organizational system. Sophisticated malwares and phishing schemes are the common means that attackers use to compromise a system [19].

Emails with authentic looking links are mostly sent to organizations to introduce nefarious cyber presence into the network. Cyber-attacks can threaten and disrupt numerous services within the healthcare field ranging from drug delivery to surgeries, placing patients' life at risk [3]. An example is the global WannaCry attack of 2017 that affected the British National Health Service hospitals resulted in postponing of surgeries and shifting people to nearby hospitals [20]. Medical devices are another area of target of the attackers [5]. People were warned in 2016 about the vulnerability of hackers taking control of Animas OneTouch insulin pump [21]. These attacks even compromise trust in doctor - patient relationship making patients unwilling to share their personal data [22].

D. What counter measures can be taken to enhance healthcare security?

Protecting the confidentiality, integrity and availability of useful healthcare data is the main aim of cybersecurity [5]. But it cannot guarantee cent percentage effectiveness to stop healthcare attacks, but adoption of proper cybersecurity practices can reduce the severity of the attacks. Planning and implementing effective security measures to mitigate the risk of cyber-attacks also require good understanding of the past and present trends in cybersecurity world.

CC BY

JIRRS
Journal International Review of Research Studies
Received: 13/06/2026 - **Accepted:** 01/08/2026
Vol: 1.10
DOI: 10.66104/yvw8a115
Pages: 1-10

Steps that can be taken to improve healthcare security are as follows:

• Strengthening of cyber resilience is one of the best approaches to ensure security. This can be achieved with practicing safe and up to date backups, which prevents permanent data loss [5].

• Quality IT as a base with equally important IT infrastructure is very much crucial for information security [3]

• Humans being the weakest link in cybersecurity proper awareness and training should be given to ensure safe security practices [23,24]. Social engineering methods are the common mode used by attackers to target the end users. Thus, identifying and filling the knowledge gaps through appropriate training can help to develop a human firewall against cybercrimes [25].

• Penetration testing as part of vulnerability management can be practiced by organizations to reduce risk with early detection [25].

• Studies reveal that 70% cybercrimes arise from dissatisfied employees [26], thus restricting and controlling administrative privileges with application of multifactor authentication can reduce insider threat within the sector [14,27].

• An incident response plan along with post incident steps should be prepared, regularly tested, exercised, and should be stored offline [28].

• Sharing information among stakeholders in all sectors is a best practice that helps in developing cybersecurity of healthcare [29], [30]. This helps in situational awareness, identifying vulnerabilities and good decision making.

• Adopting advanced cryptographic mechanisms and trust distribution technique for sharing privacy conscious data [3].

• Develop and use common security standards applicable to healthcare sector [2].

• Cyber insurance incentives can be used for security improvements [2]. The year 2020 marks about $ 7.5 billion estimated global sales in cyber insurance [31].

• Healthcare providers should establish strict personal device regulations and proper plans for disposal of hardware that contain sensitive health information of the past [30].

Limitations

Cybersecurity being a vast topic and while extending its relation to the field of healthcare, it was exceedingly difficult to identify all the threats and trends associated with the system. The study was limited with focus on healthcare cyber-attacks within Europe and to articles published only in English language within last few years. Many articles from the search result were also forced to exclude due to lack of relevant information.

CC BY

JIRRS
Journal International Review of Research Studies
Received: 13/06/2026 - **Accepted:** 01/08/2026
Vol: 1.10
DOI: 10.66104/yvw8a115
Pages: 1-10

4. Conclusion

We all are familiar with a popular saying that Health is Wealth. This statement signifies the importance of health in our life. Technological uplift has increased the efficiency of healthcare systems to enhance the health of growing population [1] but has also shot up the need for security. Data is the most vulnerable asset in health sector being targeted by attackers. The need for cybersecurity is not only to protect data but also to maintain privacy and trust in patients. Time and money should be invested to maintain and ensure security of healthcare technology along with confidentiality of health records [32]. Being the most targeted sector for cyber-attacks this field demands cybersecurity as a deep-rooted part of its culture. Aligning cyber security and patient safety programmes will not only assist health organisations secure patient safety and privacy, but it will also assure the continued effective delivery of high-quality treatment by preventing disruptions that could negatively impact clinical outcomes.

Funding

This research received no external funding.

Conflicts of Interest

The author declare no conflict of interest.

References

[1] US Government, "Economic Report of the President - Chapter 4: The Importance of Health and Health Care.", U.S. Government Printing Office, 2008.

[2] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward", Maturitas, vol. 113, pp. 48-52, 2018. Available: 10.1016/j.maturitas.2018.04.008.

[3] S. Argaw et al., "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks", BMC Medical Informatics and Decision Making, vol. 20, no. 1, 2020. Available: 10.1186/s12911-020-01161-7.

[4] M. Zarour et al., "Ensuring data integrity of healthcare information in the era of digital health", Healthcare Technology Letters, 2021. Available: 10.1049/htl2.12008.

[5] G. Martin, P. Martin, C. Hankin, A. Darzi and J. Kinross, "Cybersecurity and healthcare: how safe are we?", BMJ, p. j3179, 2017. Available: 10.1136/bmj. j3179.

CC BY

JIRRS
Journal International Review of Research Studies
Received: 13/06/2026 - **Accepted:** 01/08/2026
Vol: 1.10
DOI: 10.66104/yvw8a115
Pages: 1-10

[6] BBC News, "Wiggins and Froome medical records released by 'Russian hackers'", 2016.

[7] M. Glick, "Cyberattacks on Health Care Are Rising — But Many Hospitals Aren't Prepared", Discover Magazine, 2021. [Online]. Available: https://www.discovermagazine.com/technology/cyberattacks-onhealth-care-are-rising-but-many-hospitals-arent-prepared.

[8] "Healthcare Cybersecurity", HIPAA Journal, 2022. [Online]. Available: https://www.hipaajournal.com/category/healthcarecybersecurity/.

[9] S. Duguin, "If healthcare doesn't strengthen its cybersecurity, it could soon be in critical condition", World Economic Forum, 2021. [Online]. Available: https://www.weforum.org/agenda/2021/11/healthcare-cybersecurity/

[10] D. Rees, "Cyber attacks in healthcare: the position across Europe", Pinsentmasons.com, 2021. [Online]. Available: https://www.pinsentmasons.com/out-law/analysis/cyber-attackshealthcare-europe. [Accessed: 14- Dec- 2021].

[11] J. Riggi, "The importance of cybersecurity in protecting patient safety | Cybersecurity | Center | AHA", American Hospital Association, 2021. [Online]. Available: https://www.aha.org/center/cybersecurityand-risk-advisory services/importance-cybersecurity-protectingpatient-safety.

[12] A. Zistler, "Hacking healthcare IT in 2016: lessons the healthcare industry can learn from the OPM breach - Medical Design and Outsourcing", Medical Design and Outsourcing, 2016. [Online]. Available: https://www.medicaldesignandoutsourcing.com/hackinghealthcare-it-in-2016-lessons-the-healthcare industry-can-learn-fromthe-opm-breach/.

[13] C. Williams, R. Chaturvedi and K. Chakravarthy, "Cybersecurity Risks in a Pandemic", Journal of Medical Internet Research, vol. 22, no. 9, p. e23692, 2020. Available: 10.2196/23692 [Accessed 3 January, 2022].

[14] "9 reasons healthcare is the biggest target for cyberattacks", Swivel Secure, 2021. [Online]. Available: https://swivelsecure.com/us/solutions/healthcare/healthcare-is-thebiggest-target-for-cyberattacks/.

[15] D. Kotz, C. Gunter, S. Kumar and J. Weiner, "Privacy and Security in Mobile Health: A Research Agenda", Computer, vol. 49, no. 6, pp. 22-30, 2016. Available: 10.1109/mc.2016.185 [Accessed 26 November 2021].

[16] "5 Industries That Top the Hit List of Cyber Criminals in 2017 – Cyber Security Solutions, Compliance, and Consulting Services – IT Security", Cyber Security Solutions, Compliance, and Consulting Services - IT Security, 2017. [Online]. Available: https://www.infoguardsecurity.com/5-industries-top-hit-list-cybercriminals-2017/. [Accessed: 07- Nov-2021].

CC BY

JIRRS
Journal International Review of Research Studies
Received: 13/06/2026 - **Accepted:** 01/08/2026
Vol: 1.10
DOI: 10.66104/yvw8a115
Pages: 1-10

[17] R. Millman, Itpro.co.uk, 2016. [Online]. Available: https://www.itpro.co.uk/public-sector/27740/nine-in-10-nhs-trustsstill-use-windows-xp. [Accessed: 03- Nov- 2021].

[18] "8 Big Security Threats to Cybersecurity in Healthcare 2018", Consolidated Technologies, Inc., 2018. [Online]. Available: https://consoltech.com/blog/security-threats-healthcare-systems/amp/.

[19] "Cyber Attacks: In the Healthcare Sector", CIS, 2021. [Online]. Available: https://www.cisecurity.org/blog/cyber-attacks-in-thehealthcare-sector/. [Accessed: 06- Nov 2021].

[20] W. Millard, "Where Bits and Bytes Meet Flesh and Blood", Annals of Emergency Medicine, vol. 70, no. 3, pp. A17-A21, 2017. DOI: 10.1016/j.annemergmed.2017.07.008.

[21] R. Staff, "Johnson & Johnson letter on cyber bug in insulin pump", Reuters, 2016. [Online]. Available: https://www.reuters.com/article/us-johnson-johnson-cyber-insulinpumps-t-idINKCN12414G.

[22] "Governance of trust in precision medicine", EPFL IRGC, 2018.

[23] B. Ondiege, M. Clarke and G. Mapp, "Exploring a New Security Framework for Remote Patient Monitoring Devices", Computers, vol. 6, no. 1, p. 11, 2017. Available: 10.3390/computers6010011.

[24] L. Pycroft et al., "Brainjacking: Implant Security Issues in Invasive Neuromodulation", World Neurosurgery, vol. 92, pp. 454-462, 2016. Available: 10.1016/j.wneu.2016.05.010.

[25] The CIS Critical Security Controls for Effective Cyber Defense. CIS Critical Security Control, 2016.

[26] D. Harries and P. Yellowlees, "Cyberterrorism: Is the U.S. Healthcare System Safe?", Telemedicine and e-Health, vol. 19, no. 1, pp. 61-66, 2013. Available: 10.1089/tmj.2012.0022.

[27] A. Wright, S. Aaron and D. Bates, "The Big Phish: Cyberattacks Against U.S. Healthcare Systems", Journal of General Internal Medicine, vol. 31, no. 10, pp. 1115-1118, 2016. Available: 10.1007/s11606-016-3741-z.

[28] "Strategies to Mitigate Cyber Security Incidents – Mitigation Details", 2017. [Online]. Available: https://www.cyber.gov.au/acsc/view-allcontent/strategies-to-mitigate-cyber-security-incidents.

[29] Healthcare and Public Health Sector-Specific Plan. Washington: Department of Homeland Security, 2015.

[30] Piggin R. Cybersecurity of medical devices - addressing patient safety and the security of patient health information. London: BSI; 2017. p. 3–22.

CC BY

JIRRS
Journal International Review of Research Studies
Received: 13/06/2026 - **Accepted:** 01/08/2026
Vol: 1.10
DOI: 10.66104/yvw8a115
Pages: 1-10

[31] Insurance 2020 & beyond: Necessity is the mother of reinvention. PwC, 2015.

[32] Kruse, C., Frederick, B., Jacobson, T., & Monticone, D. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1-10, 2017.

[33] Olaniyi, A. A., Ayomide, A. A., Ogieva, M. O., & Ogwuche, G. (2026). Adoption of Intelligent Transport Systems (ITS) in Urban Transportation Planning. Discover Global Society, 4(13), 1-23. https://doi.org/10.1007/s44282-025-00312-3

[34] Olaniyi, A. A., Bamise, E. O., Gbadegesin, A. A., & Oloyede, F. S. (2026). Green Practices, Guest Satisfaction and Loyalty in the Hotel Industry. Journal International Review of Research Studies, 01(04), 1- https://doi.org/10.66104/cnpnrz3

[35] Omigbodun, O. T., Familusi, O. B., Akinsola, S. A., Adeniran, A. A., & Adeniran, A. O. (2026). AI-Powered Workflow Automation in Small Businesses. Open Journal of Economics and Commerce, 7(1): 13-45. https://doi.org/10.22259/2638-549X.0701003

[36] Omigbodun, O. T., & Akinloye, D. (2026). Context and Application of Agnew's General Strain Theory to Explain Crime. Journal International Review of Research Studies,1(06), 1-11.

[37] Akinloye, D. N. (2024). Grandparent-grandchild communication: synthesis of integrative model. Psychology Nexus, 1(1), 1-15

[38] Akinloye, D. (2026). Exploring the magnitude of Artificial Intelligence on family communication. Journal International Review of Research Studies, 1(06), 1-21.

[39] Dare, A. (2024). Communication and online platforms: pitfalls, possibilities, and pressures.ttu-ir.tdl.org.

[40] Dare, A. (2025). Communication pattern and the influence of social media contents on young adults' wellbeing in Texas, United States of America. Journal of Communication, 6(12), 1-22. https://doi.org/10.46303/ressat.2023.13

Author Responsibility Statement

OA: Conceptualization, Writing - original draft, Introduction, Methods, Analysis, Discussion, Conclusion. The author read and approved the final manuscript.

CC BY