JIRRS
Journal International Review of Research Studies

Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

CYBERATTACKS ON HEALTHCARE SYSTEMS AND THE NEED FOR CYBERSECURITY: A SYSTEMATIC LITERATURE REVIEW

Roland Obiora CHIMA [1]; Temitayo Opeyemi ODEYEMI [2]; Abiodun OJO [3]; Emmanuel Oluwasayomi AHMADU [4]; Damilola Eunice AKINBINU [5]

[1] Department of Computer Science, University of Nigeria, Nsukka; chima.roland.obiora@gmail.com; https://orcid.org/0009-0007-6376-5317

[2] Department of Geography, University of Ilesa, Ilesa, Nigeria; temitayo_odeyemi@unilesa.edu.ng; https://orcid.org/0009-0000-4569-8068

[3] Sheffield Hallam University; joeph8501@gmail.com; https://orcid.org/0009-0002-5679-7373

[4] School of Healthcare Administration, Union Commonwealth University, Kentucky, USA; emmanuel.ahmadu.unionky.edu; emmanuelahmadu07@gmail.com; https://orcid.org/0009-0004-1786-0151

[5] Ekiti State University; damilola.akinbinu@eksu.edu.ng; https://orcid.org/0009-0008-3674-8674

Corresponding author: chima.roland.obiora@gmail.com

Abstract

Healthcare systems and hospitals are fundamental components of a country's infrastructure. Digital technology and virtual techniques have dominated modern healthcare systems. The absence of information confidentiality and data integrity in this industry has raised concerns about the security of healthcare equipment and data. The healthcare have been subjected to several cyberattacks in recent years, which have caused service interruptions that can last anywhere from weeks to months. The frequency of occurrences has increased over the past ten years, and these assaults have the potential to critically hinder a country's capacity to manage disruptions as well as present a public health risk. Cybersecurity in the health sector is distinct due to the information category at risk and the significance of patient safety. The most recent cyberattacks on the healthcare sector are included in this study, which also gives a broad overview of the impacts of cyberattacks on patients, healthcare professionals, and hospital systems as well as the management techniques used by hospitals to recover from the attacks. To achieve a swift and

CC BY

JIRRS
Journal International Review of Research Studies

Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

effective response to a cyberattack, it is suggested that hospitals invest in emergency preparedness for cyberattacks by creating a downtime procedure manual, holding training exercises, and providing downtime supplies like approved paper charts and surgical and emergency service protocol. Building cyber resilience in healthcare organizations has become essential in light of this issue. Changes in human behavior, technical advancements, process alterations, and new laws and regulations can all work together to provide a holistic answer to this issue. This study also delves into a number of preventative and preparation techniques in order to either prevent cyberattacks or effectively manage them with few disruptions.

Keywords: Confidentiality; Cyberattacks; Cybersecurity; Cybersecurity Awareness; Cyber-resilience; Healthcare Cyber-Attacks; Healthcare Institutions.

1. Introduction

Health is defined by two factors: longevity and quality of life (US Government, 2008). Health is categorized by two factors: longevity and quality of life (US Government, 2008). Healthcare technology can help prolong, improve, and preserve lives (Coventry & Branley, 2018). The use of cutting-edge technology in the healthcare industry has improved healthcare accuracy and raised need for sophisticated security (Argaw, 2020). Due to its inadequate security posture and wealth of valuable data, the healthcare industry is one of the most targeted by attackers who constantly encounter emerging cyber threats. About 94% of healthcare businesses reported cyberattacks, according to the SANS cyber threat report (Zarour, 2021). However, only a small portion of these reports were made public, with the majority going unnoticed or unreported (Martin et al., 2017).

Prior to the advent of digital technology in the healthcare industry, privacy violations were a worry; now, increased connectivity has created several avenues for access (Coventry & Branley, 2018). Cyberattacks on the health sector may be state-sponsored or international, driven by political and financial gain (Coventry & Branley, 2018; Martin et al., 2017). The perpetrators of a recent hack on the World Anti-Doping Agency published medical records of notable athletes (BBC News, 2016), although their motivation is yet unknown. These attacks take use of human factors, the weakest link in cybersecurity, in addition to targeting technology flaws.

Among the ways that technology is transforming medicine include telemedicine, artificial intelligence, and electronic medical records (EMR). More services depend on the accessibility and usability of computer systems to function effectively as healthcare systems become increasingly paperless (Abbou, Kessel & Ben Natan, 2024; Ojo, 2026; Wasserman & Wasserman, 2022). However, the ease of technology comes with a higher vulnerability to attacks and viruses (Olaniyi, Ayomide, Ogieva & Ogwuche, 2026).

CC BY

JIRRS
Journal International Review of Research Studies
Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

In the context of healthcare, a cyberattack is defined as any intentional, malevolent attempt to compromise patient privacy, compromise healthcare data, or interfere with operational systems (such as medical equipment, electronic medical records, and hospital networks) (Ahmetoglu & Das, 2022; Wasserman & Wasserman, 2022). When these cybersecurity breaches take place, healthcare institutions have unique challenges that go beyond financial and reputational consequences (Abbou, Kessel & Ben Natan, 2024; Dare, 2024).

Not only do patients rely on hospitals to protect their records and personal health information, but hospitals are legally bound by health insurance to maintain this confidentiality. Healthcare cyberattacks are a direct threat to patient safety by preventing access to medical records, causing medical equipment (e.g., insulin pumps, pacemakers, ventilators, imaging) to malfunction, and hindering delivery of lab results (Dare, 2025; Olaniyi, Bamise, Gbadegesin & Oloyede, 2026; Wasserman & Wasserman, 2022). Many medical devices and online portals are interconnected in healthcare systems, so a security breach can cause widespread implications across multiple departments and stakeholders that affect all aspects of hospital operations (Abbou, Kessel & Ben Natan, 2024; Sittig & Singh, 2016).

Studies have shown that healthcare technology can help prolong, improve, and preserve lives (Coventry & Branley, 2018). The use of cutting-edge technology in the healthcare industry has improved healthcare accuracy and raised need for sophisticated security (Argaw, 2020). Due to its inadequate security posture and wealth of valuable data, the healthcare industry is one of the most targeted by attackers who constantly encounter emerging cyberthreats. About 94% of healthcare businesses reported cyberattacks, according to the SANS cyber threat report (Zarour, 2021). However, only a small portion of these reports were made public, with the majority going unnoticed or unreported (Martin et al., 2017).

Prior to the advent of digital technology in the healthcare industry, privacy violations were a worry; now, increased connectivity has created several avenues for access (Coventry & Branley, 2018). Cyberattacks on the health sector may be state-sponsored or international, driven by political and financial gain (Coventry & Branley, 2018; Martin et al., 2017). The perpetrators of a recent hack on the World Anti-Doping Agency published medical records of notable athletes (BBC News, 2016), although their motivation is yet unknown. These attacks make use of human factors, the weakest link in cybersecurity, in addition to targeting technology flaws.

Due to a lack of standardized cybersecurity protocol for medical devices and telehealth platforms, these systems are particularly susceptible to cyberattacks that can expose all connected networks to risk (Alder, 2024). By targeting an out-of-date medical device, hackers can potentially gain access to a hospital system's EMR and sensitive patient information or deliver false results to physicians (Al-Qarni, 2023). Likewise, hackers can also intercept telehealth calls or messages, especially if patient-owned devices lack proper security measures (e.g., outdated operating system, not passcode-protected, non-encrypted communication) causing a breach

CC BY

JIRRS
Journal International Review of Research Studies
Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

in health insurance regulations and a means of manipulating data (Omigbodun, Familusi, Akinsola, Adeniran & Adeniran, 2026).

Each year, the number of online security breaches rises and is growing at an alarming rate (Wasserman & Wasserman, 2022). In the last decade, the number of reported hospital cyber-attacks has tripled in many parts of the world (Alder, 2024). Threatening the hospital workflow and commitment to patient safety, these cyberattacks can lead to devastating financial and health consequences. Hospitals have a duty under health insurance to protect patient confidentiality and personalized health information (Wasserman & Wasserman, 2022; Ojo, Adebayo & Sheidu, 2026; Alder, 2024; Kroll, 2024).

Thus, compared to other industries, the healthcare industry has been found to spend more on resolving data breaches (Wasserman & Wasserman, 2022). Although some hospitals may have protocols in place for scheduled system downtime events, they are often short-term plans that are not suited for prolonged offline services. Meanwhile, in a 2024 report released by Kroll a leading independent provider of global risk and financial advisory solutions over 26% of healthcare organizations have low cybersecurity maturity that lacks all recommended threat and detection capabilities (Kroll, 2024).

Only 3% of healthcare industries actually have mature cybersecurity features that go beyond basic monitoring (Kroll, 2024). In a field so reliant on computer systems, it is crucial to have guidelines in place to not only improve hospital cybersecurity, but also to ease the transition to paper charts in the event of a cyberattack. By mitigating the clinical impact of security breaches on the hospital system, healthcare providers can continue to deliver quality care for their patients and ensure patient safety. Preventing cyber threats can help hospitals avoid costly ransomware attacks, protect irreplaceable patient data, ensure patient safety, and prevent the fallout from class action lawsuits and damage to their reputation (Akinloye, 2024; Kumar, Singh & Ahmad, 2022; Ojo, Odibo, Adebayo & Akintayo, 2026; Wasserman & Wasserman, 2022).

The objectives of this study are to identify recent healthcare cyber-attacks and their methods of security breach; describe experiences and challenges faced following the loss of all electronic health record access; and provide recommendations and prevention strategies for future attacks.

2. Literature Review

Cyber-attacks start popping up in the healthcare sector during the early 2000's (Glick, 2021). 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 (Healthcare Cybersecurity, 2022). The following years witnessed more attacks and data breaches with sophisticated tools and techniques over a growing attack

CC BY

JIRRS
Journal International Review of Research Studies
Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

surface (Duguin, 2021). A study conducted by the world economic forum on healthcare cyber-attacks reveal that the threat plagued the sector during the COVID-19 pandemic (Duguin, 2021). The pandemic accelerated the growth of telemedicine and other digital health facilities (Rees, 2021). As technology develops and healthcare gets more digitalized the potential risk of cyber incidents also increased (Rees, 2021).

The 2017 WannaCry attack affected about a third of NHS trust in the UK (United Kingdom) (Rees, 2021). About 80,000 hospitals affected, 7000 appointments cancelled including surgeries and even some emergency departments were shuttered (Glick, 2021; Rees, 2021). 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 (Rees, 2021). 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 (Rees, 2021). Detection of malicious activity on the health network disabled several health systems and majority of services were forced to shut down (Rees, 2021). 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. Thirty (30) servers of Dusseldorf University hospital in Germany were affected by ransom during September 2020 (Rees, 2021). One death was reported due to patients' ambulance redirected to another hospital (Rees, 2021).

Germany was not severely affected by cyber-attacks that time as adoption to digital health technology was a slow process there (Rees, 2021). When they began adopting technological innovations, now IT security is mandatory in every health sector in Germany. About twenty-seven (27) major health sector cyber-attacks were reported in the year 2020 by the French media (Rees, 2021). Ransom attacks such as those affected the Villefranche hospital forced French government to adapt to new cybersecurity standards (Rees, 2021). They have recently announced to invest in cybersecurity about € 350 million to protect the healthcare infrastructure (Rees, 2021).

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 four hundred and thirty (430) attacks per week per organization (Rees, 2021). 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 (Rees, 2021). Emergency action plans to strengthen cyber defense capabilities were initiated in Spain to curb this situation.

CC BY

JIRRS
Journal International Review of Research Studies
Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

Health Sector Remains the Focus by Cyber-attackers

Health sector poses an incredible amount of data with high monetary and intelligence value (Riggi, 2021). This richness in valuable and immutable data with a weak defence system makes health sector an appealing target for attackers (Coventry & Branley, 2018). The targeted particulars include personal identification information, financial details, patients protected health information and data related to medical research and innovation (Riggi, 2021). 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 (Zistler, 2016), (Williams, Chaturvedi & Chakravarthy, 2020). 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 details (Rees, 2021). Scientific innovations in health sector could also be a reason for cyber terrorist and nation state attackers to target the sector (Rees, 2021).

3. Methodology

This study adopts a systematic literature review, where author(s) independently searched for previous publications on certain search words such as cyber-attacks as shown in this study via Google Scholar by conducting an initial search for “hospital cyberattack.” Due to the simplicity of user interface, wider scope of academic content and sources, and significantly greater access to free full-text articles, PubMed was primarily used as the bibliographic database. All IT (information technology) related articles were excluded from this review, and streamlined to “hospital” and “cyberattack”, having the following sub-search words such as “healthcare cyberattack technology”, “healthcare data breaches”, and “hospital cyberattack prevention case study”, fully written in English and published since 2016. After a thorough search, only 29 articles were considered valid for this study as they meet the topic relevance.

4. Discussion

From the study, it was revealed that many of the data breaches were a result of phishing and ransomware attacks. To address or prevent these incidents from reoccurring, hospitals have begun to implement ongoing education for employees to maintain awareness and promote safe practices for cybersecurity. They have also begun to prioritize developing robust security measures and protocols to protect patient data and information (Lippi & Ferrari, 2024; Sittig & Singh, 2016).

CC BY

JIRRS
Journal International Review of Research Studies
Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

The strategies to combat cyberattacks in hospitals can be divided into the steps needed to make a proactive incident response plan (Al-Qarni, 2023). This consists of planning and preparation, detection, analysis and evaluation, containment and eradication, recovery, and post-incident activities (Al-Qarni, 2023). Standard protocol in most situations involves hospitals shutting down the network and changing the passwords of their most privileged accounts. Cybersecurity personnel are then tasked with inspecting all devices connected to the network to identify the breach, fix it, and make sure the network is secure enough to be relaunched.

Preventive Strategies of Cybersecurity in Healthcare

The most fundamental efforts include investing in cybersecurity personnel separate from the IT staff, who tend to do an inefficient job, as they have their hands full with the day-to-day software updates and hardware maintenance required to keep the network afloat (Alder, 2024), (Shariff, Bejaimal & Sontrop, 2013). Hospitals must organize programs to educate physicians and staff on the most common methods of cyberattacks and their implications, the importance of cybersecurity, and the best practice guidelines in the event of an attack (Alder, 2024; Kroll, 2024). Senior leaders can be sources of guidance and counselling, drawing on their more extensive experience working with paper charts and hospital flow coordination. It should be emphasized that cybersecurity is a group effort and that individual lapses can provide entry points for attackers.

Regular briefings on the latest hacking techniques can reinforce and equip hospitals to better defend themselves (Rizzoni, Magalini & Casaroli, 2022). Mock drills for downtime scenarios not only help hospitals identify areas of strengths and weaknesses in their systems but also improve the ease of transferring to pen and paper or alternate methods (Abbou, Kessel & Ben Natan, 2024). These mock drills can consist of simulated cyberattacks with no functioning computers for hospital employees or exercises for IT staff to locate and subdue sources of cyberattacks in the hospital (Abbou, Kessel & Ben Natan, 2024; Argaw, Troncoso-Pastoriza & Lacey, 2020). It is crucial that these mock drills be conducted as frequently as fire and safety drills to prevent lapses in patient care during an attack. Hospitals must have a standard protocol set in place, which must be practiced and reinforced during these drills (Akinloye, 2026; Al-Qarni, 2023; Argaw, Troncoso-Pastoriza & Lacey, 2020).

Department-specific guidelines are the most efficient way to develop downtime protocols (Rizzoni, Magalini & Casaroli, 2022). These should, however, adhere to the structure provided by the hospital. As the number of social engineering attacks involving phishing increases, efforts to ward off these tactics need to be highlighted. Strategies include refraining from engagement with emails from sources outside the network and avoiding using hospital emails to log onto out-of-network websites

CC BY

JIRRS
Journal International Review of Research Studies
Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

(Argaw, Troncoso-Pastoriza & Lacey, 2020). Policies mandating periodic password changes and multi-factor authentication are crucial for preventing data breaches in hospitals (Argaw, Troncoso-Pastoriza & Lacey, 2020; Wright, Aaron & Bates, 2016). However, finding the right balance between robust security and being mindful of the user experience is important. Overly complex procedures can lead to frustration and non-compliance among busy healthcare professionals (Wasserman & Wasserman, 2022). Since the EMR has been adopted, doctors have completely shifted away from conventional methods of recording patient information, ordering investigations, and prescribing medications.

This undisputed reliance on online systems makes it difficult for new doctors to adjust to these vast changes during downtime events. Many physicians find themselves struggling without the assistance of automated clinical decision-making systems, system warnings for managing drug-drug interactions, and selectable prescription dosages (Omigbodun & Akinloye, 2026). Teaching institutions must take care that residents and medical students are not trained to rely heavily on these physician crutches. During any offline events, doctors rely heavily on clinical pharmacists to rule out allergies and drug interactions (Haase, Whitworth & Yalamanchili, 2021).

However, to maintain smooth hospital flow and promote patient safety, clinical knowledge and judgment must supersede these physician aides. Having print-outs ready to make the switch easier and using them during mock drills helps prevent an impact on patient care (Abbou, Kessel & Ben Natan, 2024). By including this strategy as a part of the medical school curriculum and incorporated into clinical simulations, newer doctors are more likely to be unfazed by such scenarios in the real world.

A 2021 cyberattack simulation conducted by Willing et al. found that in an ICU setting, it is crucial for staff to be aware of the dangers of cyberattacks and recognize signs of system hacking (Willing, Dresen & Gerlitz, 2021). Participants who experienced less stress during the simulation were able to demonstrate better communication skills and respond more quickly to the issue at hand. Mock drills that incorporate the implementation of strategies and guidelines can provide healthcare providers with the training necessary to adapt to offline events and ensure patient safety (Abbou, Kessel & Ben Natan, 2024; Argaw, Troncoso-Pastoriza & Lacey, 2020), (Willing, Dresen & Gerlitz, 2021) Likewise, simulating phishing scenarios has also been shown to effectively test and improve recognition of phishing schemes (Abbou, Kessel & Ben Natan, 2024; Argaw, Troncoso-Pastoriza & Lacey, 2020).

While many hospitals currently require annual training and compliance that includes a session on phishing and cyberattacks, these mandatory modules have not been shown to reduce the number of successful fishing attempts (Kumar, Singh & Ahmad, 2022; Ojo, 2026) This could be due to training fatigue and the extended amount of time required to complete mandatory online training, resulting in

CC BY

JIRRS
Journal International Review of Research Studies
Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

decreased engagement and attention. This in turn can contribute to low retention and downplaying the importance of cybersecurity (Argaw, Troncoso-Pastoriza & Lacey, 2020; Willing, Dresen & Gerlitz, 2021; Gordon, Wright & Glynn, 2019).

Phishing simulations and repeated exposure to phishing tests can be a more effective method in building a resilient cybersecurity culture within healthcare staff (Wright, Aaron & Bates, 2016; Haase, Whitworth & Yalamanchili, 2021). Through consistent, realistic exposure, hospital employees can learn to recognize common phishing tactics and receive immediate feedback in a safe environment. By enforcing the importance of cybersecurity within the hospital workforce through various strategies (e.g., professional education programs, incentives for participating in security training, simple process for reporting suspicious activity), hospitals can foster a culture of accountability and cyber defense amongst healthcare staff.

Protecting the confidentiality, integrity and availability of useful healthcare data is the main aim of cybersecurity (Martin et al., 2017). But it cannot guarantee total stoppage of healthcare cyberattacks, 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.

Ensuring that healthcare operating systems are up to date and that security updates and patches are carried out on time is important to resolve weaknesses in the network (Willing, Dresen & Gerlitz, 2021). Previous studies have shown that almost 85% of healthcare organizations and medical devices run on “old legacy networks,” such as Windows XP, that put them at risk for cyberattacks (Busdicker & Upendra, 2017; Ewoh & Vartiainen, 2024; Ghafur, Kristensen & Honeyford, 2019). Many of these outdated operating systems are no longer supported by security updates or provide routine offline backups. This was the cause of the 2017 WannaCry cyberattack that affected numerous healthcare organizations, including the National Health Service (NHS) in the UK, and over 200,000 computers in more than 150 countries (Ghafur, Kristensen & Honeyford, 2019).

Medical devices (e.g., insulin pumps, pacemakers, MRIs, etc.) can become corrupted, leading to the closure of cardiac, stroke, and trauma services for admissions due to the inability to rely on these devices for accurate diagnostics and treatment (American Medical Association, 2026). Since medical devices and implants are made to last for long periods, hospitals should prioritize investment in equipment that has integrated cybersecurity measures throughout the development process, rather than bolting it on later as an afterthought. Likewise, if outdated device software cannot be updated or replaced, healthcare systems must inform themselves on whether to continue using the device, despite the increased risk of cyber threats.

CC BY

JIRRS
Journal International Review of Research Studies
Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

Blockchain technology allows data such as EMR to be split, encrypted, and stored across multiple computers. This prevents data from being centralized and easily hacked because there is no longer a single attack target and data changes (i.e., altering patient charts, extracting health information) are tracked along a cyber trail. There are many platforms available that support the integration of blockchain technology within EMR systems (e.g., MedRec, BlockHIE) (Ekblaw, Azaria & Halamka, 2016; Hasselgren, Kralevska & Gligoroski, 2020).

Due to consideration of cost-effectiveness and efficiency, widespread adoption of blockchain technology in healthcare data management is still in the early stages but is actively being explored. Hospital systems can also prevent the success of phishing schemes by purchasing domains with names similar to the official hospital domain (e.g., ".com") (Rizzoni, Magalini & Casaroli, 2022). This will help prevent instances in which hospital staff accidentally open phishing emails from unknown senders who appear familiar or trustworthy.

---

5. Conclusion

There is a popular saying that *"Health is Wealth"* signifies the importance of health in human life, and enhances a healthy nation. Technological adoption has increased the efficiency of healthcare systems to enhance the health intake of growing population (US Government, 2008) but has also shot up the need for security. The increasing occurrence of cyberattacks in healthcare in recent years underscores a critical vulnerability within our healthcare systems, highlighting the urgent need for more robust and proactive measures.

This study employs a systematic literature review, and it examined the increasing prevalence of healthcare and hospital cyberattacks and the growing challenges faced in securing their networks. 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. As cyber-attacks become more and more sophisticated, it is essential for healthcare institutions to not only enhance their technological defenses, but also to foster a culture of cybersecurity awareness and preparedness.

Time and money should be invested to maintain and ensure security of healthcare technology along with confidentiality of health records. 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.

CC BY

JIRRS
Journal International Review of Research Studies

Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

Limitations

The limitation of this study is using PubMed as the only database. This could have affected some published articles which are not indexed on PubMed to be hided. Though PubMed is a bibliographic database that supports scientific and medical research, there are some articles published in less well-known journals that are not indexed by PubMed; therefore, those articles will be missing in this article. This approach will enhance the inclusion of articles that are published by sound publishers.

Funding

This research received no external funding.

Conflicts of Interest

The author declare no conflict of interest.

References

Abbou, B., Kessel, B., & Ben-Natan, M. (2024). When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. *Front Digital Health*, 1321485. https://doi.org/10.3389/fdgth.2024.1321485

Ahmetoglu, H., & Das, R. (2022). A comprehensive review on detection of cyber-attacks: data sets, methods, challenges, and future research directions. *Internet Things*, 20:100615. https://doi.org/10.1016/j.iot.2022.100615

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

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

Alder, S. (2024). Healthcare data breach statistics, In: 2024. Accessed 31st July, 2026.

CC BY

JIRRS
Journal International Review of Research Studies

Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

Al-Qarni, E. A. (2023). Cybersecurity in healthcare: a review of recent attacks and mitigation strategies. *Int J Adv Comput Sci Applicat*, 14(5). https://doi.org/10.14569/IJACSA.2023.0140513

American Medical Association (2026). Cybersecurity in medical practice. https://edhub.ama-assn.org/course/328?utm_source=silverchair_edhub&utm_campaign=activity_alert-edhub&utm_content=weekly_batch&cmp=1&utm_medium=email, 2024. Accessed 31st July, 2026.

Argaw, S. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, 20(1). https://doi.org/10.1186/s12911-020-01161-7.

Argaw, S. T., Troncoso-Pastoriza, J. R., & Lacey, D. (2020). Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. *BMC Med Inform Decis Mak*, 20:146; doi:10.1186/s12911-020-01161-7

BBC News (2016). Wiggins and Froome medical records released by 'Russian hackers, 2016.

Busdicker, M., & Upendra, P. (2017). The role of healthcare technology management in facilitating medical device cybersecurity. *Biomed Instrumentat Technol*, 51(s6):19-25. https://doi.org/10.2345/0899- 8205-51.s6.19

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas,* 113, 48-52, 2018. https://doi.org/10.1016/j.maturitas.2018.04.008.

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

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

Duguin, S. (2021). If healthcare doesn't strengthen its cybersecurity, it could soon be in critical condition. World Economic Forum, 2021. Retrieved from: https://www.weforum.org/agenda/2021/11/healthcare-cybersecurity/

Ekblaw, A., Azaria, A., & Halamka, J. D. (2016). A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. In: *Proceedings of the IEEE Open & Big Data Conference,* 13. p. Montreal, QC, Canada

CC BY

JIRRS
Journal International Review of Research Studies

Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. *Journal of Medical and Internet Research,* 26:e46904; https://doi:10.2196/46904

Ghafur, S., Kristensen, S., & Honeyford, K. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digital Medicine,* 2:98; https://doi:10.1038/s41746-019-0161-6

Glick, M. (2021). Cyberattacks on Health Care Are Rising - But Many Hospitals Aren't Prepared. Discover Magazine. Retrieved from: https://www.discovermagazine.com/technology/cyberattacks-onhealth-care-are-rising-but-many-hospitals-arent-prepared.

Gordon, W. J., Wright, A., & Glynn, R. J. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *J Am Med Inform Assoc,* 26(6):547–552; https://doi.org/10.1093/jamia/ocz005

Haase, K. K., Whitworth, M. M., & Yalamanchili, K. (2021). Clinicians' experiences and reflections from a health system cyberattack. *J Am College Clin Pharmacy*, 4(6):738 742. https://doi.org/:10.1002/jac5.1423

Hasselgren, A., Kralevska, K., & Gligoroski, D. (2020). Blockchain in healthcare and health sciences a scoping review. *Int J Med Informatics,* 134:104040. https://doi:10.1016/j.ijmedinf.2019.104040

Healthcare Cybersecurity (2022). HIPAA. Available: https://www.hipaajournal.com/category/healthcarecybersecurity/

Kroll, L. (2024). The state of cyber defense: diagnosing cyber threats in healthcare. Retrieved from: https://www.kroll.com/en/insights/publications/cyber/state-cyber-defense-healthcare.

Kumar, A., Singh, A. K., & Ahmad, I. (2022). A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare. *Sensors*, 22 (15): 5921. https://doi.org/10.3390/s22155921.

Lippi, G., & Ferrari, A. (2024). Lessons learnt in medical laboratories during a disruptive cyber-attack. *J Laborat Precision Med*, 9. https://doi.org/10.21037/jlpm-23-84.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? *BMJ,* j3179, https://doi.org/10.1136/bmj. j3179.

Ojo, A. (2026). Machine learning- based prediction of heart failure mortality using clinical biomarkers and imbalanced data strategies. *Journal International Review of*

CC BY

JIRRS
Journal International Review of Research Studies

Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

Research Studies, 1(9), 1-11. *Journal International Review of Research Studies* https://doi.org/10.66104/bwtkpv61

Ojo, A., Adebayo, A. A., & Sheidu, B. A. (2026). Insecticide-Resistance Genotyping of Anopheles Mosquito. *Journal International Review of Research Studies, 1*(8), 1-19.https://doi.org/10.66104/emm0kp79

Ojo, A., Odibo, G. C., Adebayo, A. A., & Akintayo, D. A. (2026). Knowledge management and performance of retail pharmaceutical businesses in Nigeria. *Journal International Review of Research Studies, 1*(8), 1-34. https://doi.org/10.66104/5phgj889

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

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

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

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.

Rees, D. (2021). Cyberattacks in healthcare: the position across Europe. Retrieved from: https://www.pinsentmasons.com/out-law/analysis/cyber-attackshealthcare-europe.

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

Rizzoni, F., Magalini, S., & Casaroli, A. (2022). Phishing simulation exercise in a large hospital: a case study. *Digital Health,* 8:20552076221081716. https://doi.org/10.1177/20552076221081716

Shariff, S. Z., Bejaimal, S. A., & Sontrop, J. M. (2013). Retrieving clinical evidence: a comparison of PubMed and Google Scholar for quick clinical searches. *J Med Internet Res*, 15(8):e164. https://doi.org/10.2196/jmir.2624

CC BY

JIRRS
Journal International Review of Research Studies

Received: 22/07/2026 - **Accepted:** 04/08/2026
Vol: 1.10 - October (2026)
DOI: 10.66104/ptx1wg79
Pages: 1-15

Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Appl Clin Inform*, 7:624-632. https://doi.org/10.4338/ACI-2016-04-SOA-0064

US Government (2008). Economic Report of the President - Chapter 4: The Importance of Health and Health Care. U.S. Government Printing Office.

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: review (for the non cyber professional). *Front Digital Health*, 4; doi:10.3389/fdgth.2022.862221

Williams, C., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research, 22*(9), e23692. https://doi.org/10.2196/23692.

Willing, M., Dresen, C., & Gerlitz, E. (2021). Behavioral responses to a cyber-attack in a hospital environment. *Sci Rep,* 11:19352; doi:10.1038/s41598-021-98576-7

Wright, A., Aaron, S., & Bates, D. W. (2016). The Big phish: cyberattacks against U.S. Healthcare systems. *J General Intern Med*, 31(10):1115-1118. https://doi.org/10.1007/s11606-016-3741-z

Zarour, M. (2021). Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters*, https://doi.org/10.1049/htl2.12008.

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

Author Responsibility Statement

ROC: Conceptualization, Writing - original draft, Introduction, Methods, Analysis, Discussion, Conclusion; TOO: Conceptualization, Writing - original draft, Introduction; AO: Conceptualization, Writing; EOA: Methods, Analysis, Discussion; DEA:Introduction, Conclusion, Editing. The authors read and approved the final manuscript.

CC BY