Artificial Intelligence and Predictive Analytics in Preventing Ransomware Attacks on Critical Healthcare Information Systems in the United States: A Strategic National Security Assessment

Zeliatu Ahmed[1], Aisha Mohammed Suleiman[2], and Matilda Thompson[3]

[1]Department of Information Systems, Cybersecurity, Dakota State University, Madison, USA
[2]University of Iowa, Iowa, USA
[3]University of Ghana, Ghana
[1]ahmedzeliya@gmail.com, [2]aisha.researcher@gmail.com, ORCID ID: 0009-0004-3996-0305
[3]matildathompson108@gmail.com

Abstract:
Ransomware attacks on critical healthcare information systems (HIS) in the United States pose a significant threat to national security, patient safety, and the continuity of healthcare services. As cybercriminals employ increasingly sophisticated attack vectors, traditional security measures have proven insufficient in mitigating these threats. This paper explores the role of artificial intelligence (AI) and predictive analytics in enhancing the cybersecurity posture of healthcare information systems, with a particular focus on preemptive threat detection and response. Through a strategic national security assessment, this study evaluates how AI-driven models can identify ransomware patterns, predict attack vectors, and automate threat mitigation in real time. By analyzing historical ransomware incidents and leveraging machine learning algorithms, this research demonstrates the potential of predictive analytics in fortifying healthcare infrastructure against cyber threats. Furthermore, it assesses the policy and regulatory landscape governing AI implementation in cybersecurity for healthcare institutions. The findings demonstrate that AI-enabled predictive models greatly enhance the early identification of ransomware and allow healthcare systems to intercept in-processing attacks before they compromise critical data. These models successfully provide a mapping of anomalous network activities and predict probable points of entry, allowing for automated, proactive defense mechanisms. The study also highlights current gaps in policy and the pressing need for more standardized regulations to support the widespread adoption of AI in healthcare security. The findings underscore the need for a robust, AI-integrated cybersecurity framework that enhances threat intelligence, reduces response time, and ensures resilience against ransomware attacks. This study provides strategic recommendations for policymakers, healthcare administrators, and cybersecurity professionals to strengthen national security through AI-driven predictive analytics.

Keywords: Ransomware, Artificial Intelligence, Predictive Analytics, Healthcare Information Systems, Cybersecurity, National Security.

INTRODUCTION

The integration of artificial intelligence (AI) and predictive analytics in healthcare systems has become a recognized approach in mitigating cybersecurity threats, especially ransomware attacks. Healthcare fundamentally constitutes the collective efforts of society to ensure, provide, finance, and promote health, most of the time with a significant focus on prevention of diseases and disability (Badawy, et al, 2023). Nonetheless, the increasing frequency of cyberattacks, notably ransomware, presents significant threats to patient care and healthcare information security, underscoring the development for robust predictive models very critical. Ransomware, a type of malware that encrypts critical systems and demands payment to restore data, has sharply increased in attacks that target healthcare providers. Between 2016 and 2021, the number of ransomware events rose doubled per year, compromising the personal health information of tens of millions

of people (McDill, 2023). Two recent systematic assessments of ransomware events revealed a total of 374 instances affecting healthcare delivery entities that severely disrupted operation and/or compromised patient data (Jahic, 2024) (Danner, 2025). To deal with these challenges, the implementation of AI-driven predictive analytics has erupted to enhance the visibility and security of connected devices and systems in healthcare networks. Such visibility enables organizations to proactively monitor network-based vulnerabilities, rapidly identify anomalies, and better understand the changing threat environment (Philips, 2020). Moreover, the risk stratification that this type of predictive modeling allows, enables healthcare providers to safely classify patients based on their level of risk and direct focus on high-risk patients, who may be in immediate need of intervention (Emsisoft Malware Lab, 2024) Given the increasing prevalence of ransomware attacks, it is crucial for health care organizations to employ advanced security technologies, such as artificial intelligence and predictive analytics. These technologies enable more than just threat detection; they also foster prevention measures, including lifestyle modifications and proactive health treatments, leading to better patient outcomes and better protection of sensitive health data (Emsisoft Malware Lab, 2024) (McDill, 2023).

EVOLUTION OF AI AND PREDICTIVE ANALYTICS IN HEALTHCARE

Predictive analytics has come a progressed significantly over the past couple of decades, especially with the development of technologies and tools to analyze data. Predictive analytics can be viewed as an evolution of traditional statistical techniques that were used across many fields like healthcare in identifying trends and informing decision making. Initially, it began as the use of basic statistical techniques to project future occurrences based on past data which has now evolved. However, with the advent of Artificial Intelligence (AI) and machine learning, a paradigm shift in data processing has taken place, allowing for more advanced analysis and predictive capabilities. With the advent of big data, the sheer volume of available information necessitated the development of more advanced analytical methods. Additionally, with organizations recognizing the value of data-driven insights, predictive analytics has emerged as an essential tool to glean insights from complex health trends (WebAsha, 2025) (Sweeney, 2017), allowing organizations to improve efficiencies in operation. This transformation has allowed healthcare practitioners to utilize massive volumes of data, ranging from historical to real-time, to improve decision making and enhance outcomes for patients (Kaneria, 2025) (Sheth, 2024).

Growing technologies like artificial intelligence and Internet of Things (IoT) have further pushed the advancement of predictive analytics even further. Modern algorithms can combine many sources of data, from electronic health records (EHR), administrative records, to insurance data that produce insights that can be acted upon. This data-driven approach helps detect potential health risks at an earlier stage and enables the development of patient-specific treatment plans, thus improving patient outcomes (WebAsha, 2025). Notable developments which include the use of wearable biosensors and automated monitoring systems enable healthcare providers to detect early deterioration of patients which improves general healthcare quality (CyberPeace, 2024).

CURRENT ISSUES OF RANSOMWARE ATTACKS ON US HEALTHCARE INFORMATION SYSTEMS

Ransomware attacks can be lethal to healthcare information systems in the United States, threatening both patient safety and operational integrity. Hospitals are targeted by hackers for two main reasons. The first is healthcare information, e.g., electronic medical records and secondly due to security vulnerabilities in IT processes. Due to the sensitive nature of healthcare information, and the life-or-death urgency of the sector, hospitals, clinics, and other healthcare facilities are targets of opportunity for cybercriminals looking for vulnerabilities to exploit. Modern healthcare's heavy reliance on digital systems only exacerbates this vulnerability. From electronic health records (EHRs) to diagnostics tools, scheduling systems and even lifesaving equipment, virtually every aspect of modern healthcare is dependent on interconnected technology. All of these systems can be brought to a standstill with a successful ransomware attack, delaying treatments, compromising care, and putting patient lives in immediate jeopardy (DriveLock, 2024).

In recent years, the healthcare industry has leaned towards artificial intelligence (AI) and predictive analytics as essential tools to fight these threats. Global ransomware attacks targeting the healthcare sector have steadily

increased, almost doubling since 2022 with 389 total claimed victims in 2023 compared with 214 in 2022. In the US, attacks against the healthcare sector rose 128 percent in 2023 with 258 victims, compared to 113 in 2022. LockBit and ALPHV/BlackCat are the two most prevalent Ransomware-as-a-Service (RaaS) providers and combined, they accounted for over 30 percent of all claimed healthcare attacks globally (CTIIC, 2024).

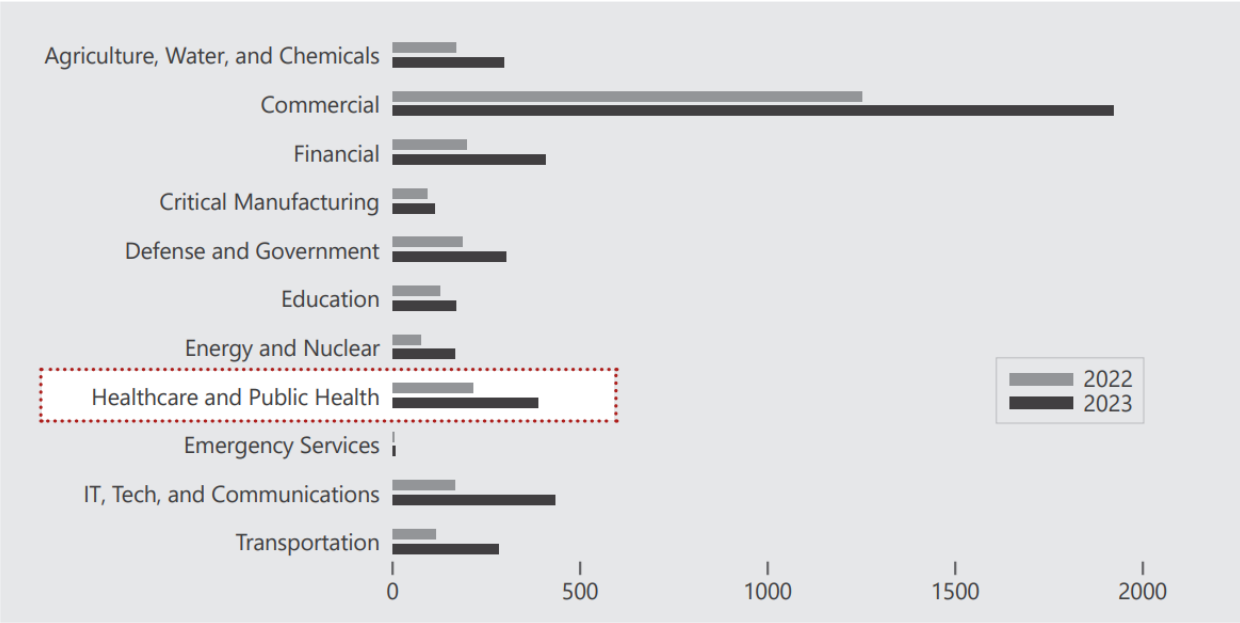

Figure 1: *Comparison Of Total Ransomware Attacks Worldwide by Sector, 2022 Versus 2023 (CTIIC, 2024)*

A 2024 study by Microsoft found that nearly 400 United States healthcare organizations had been infected by a ransomware, with the average ransom payment being as high as $4.4 million. Beyond the immediate financial consequences, the downtime associated with restoring operations after an attack can cost an organization up to $900,000 per incident. The consequences of these attacks extend beyond financial losses; they massively disrupt core healthcare services, delaying patient medical care, interrupt medical procedures and endangers lives (Beek, 2025).

An analysis conducted by Comparitech in 2024 highlights the disturbing magnitude of ransomware attacks on healthcare information systems. Their study highlighted 5,461 successful ransomware attacks globally, according to claims of ransomware groups on data leaked sites which at least 1,204 were confirmed by the targeted organizations. Together, these breaches led to the exposure of 195.4 million records, highlighting the enormity of data exposure in the healthcare industry (Alder, 2025). Notably, these attacks were most severe in North America and Europe, with cybercriminl organizations like RansomHub, LockBit, Medusa and Play responsible for the most confirmed incidents. RansomHub topped the list with 89 verified attacks, followed by LockBit with 83, Medusa with 62, and Play with 57. While these figures are still alarmingly high, they represent a slight decline in the numbers from 2023, where there were 1,474 confirmed ransomware attacks, leaking 261.5 million records. Even with this downturn, the financial toll from these attacks remains staggering. The average ransomware demand in 2024 was more than $3.5 million; total confirmed payments to ransomware groups reached $133.5 million. Moreover, the calculated average ransom payment totaled $9,532,263, highlighting the high-stakes nature of the cyber extortion schemes (Alder, 2025).

One of the most devastating ransomware attacks to take place in 2024 was the BlackCat/ALPHV ransomware attack on Change Healthcare. As a result, Change Healthcare's systems were down for weeks, seriously affecting the billing operations of health care providers across the United States. The financial fallout from this event was immense, with UnitedHealth Group, the parent company of Change Healthcare, ultimately reporting that the firm suffered a total loss of $2.9 billion over the full year due to the attack. Change Healthcare, in an attempt to prevent the release of stolen data cost the company a $22 million ransom payment,

only for the cyberattackers to engage in an exit scam, which led to a greater financial and operational crisis for the company. Specifically, five out of ten of the most damaging ransomware attacks of 2024 targeted healthcare organizations, reflecting the urgency of the need for cybersecurity improvements in the sector (American Hospital Association, 2025) (Alder, 2025).

THE ROLE OF AI AND PREDICTIVE ANALYSIS IN RANSOMWARE PREVENTION ON CRITICAL HEALTHCARE INFORMATION SYSTEMS

AI is leading the fight against cybersecurity threats with capabilities beyond just providing extra layers of defense. Its real-time threat identification, breach containment, and proactive risk mitigation play a major role in proactive ransomware mitigation.

AI-driven threat identification utilizes machine learning algorithms to process large quantities of data sets and identify patterns and anomalies — for instance, abnormal log-in activity or access to EHR systems without authorization. By continuously analyzing network activity, AI contributes to healthcare organizations pre-empting potential attackers before they trigger full-blown ransomware hijacks. In contrast to conventional signature-based detection techniques that rely on known malware signatures, AI systems use historical attack information to identify emerging threats in real time (Cambridge Health, 2025). Predictive analytics refers to utilizing existing historical data, statistical algorithms, and machine learning techniques in order to determine the probability of future outcomes. Organizations across finance, healthcare, marketing, and insurance domains use this technique to predict future trends, business outcomes, and potential risks. Predictive analytics is focused on using data obtained from customers, social media, online transactions, etc to predict customer actions, trends in the market, and upcoming occurrences (Srivastava, 2023).

One of the key roles of AI in ransomware prevention is breach containment. Internet of Things (IoT) security solutions that are powered by artificial intelligence can automatically quarantine a compromised network, stop the spreading of ransomware, or disable a compromised account on its own. Such rapid responses mitigate the cycle of attack and help healthcare institutions in reducing downtime and data loss extensively. Additionally, AI also enhances security by monitoring user behavior patterns to spot any irregularities that could potentially reveal insider threats or compromised accounts, thus fortifying the organization's cyber defenses. Furthermore, by analyzing network traffic, AI can identify anomalies like spikes in data encryption or strange file access, which may serve as an early signal of a potential ransomware attack. AI makes it possible to send real-time warnings to cybersecurity teams, so they can take immediate preventive measures before significant damage becomes irreversible. By doing so, this proactive approach ensures that healthcare organizations are protected against the rising risk of ransomware attacks, protecting sensitive patient information and allowing them to maintain operational continuity (Cambridge Health, 2025).

AI's ability to analyze huge amounts of data assists healthcare providers in predicting patient outcomes and identifying potential health risks, allowing them to deliver proactive and personalized care. Predictive analytics can help provide better outcomes for patients and lower costs for the healthcare system in general, making it an invaluable tool for many medical professionals (Nnamdi (2024). AI can also be used to optimize operations in healthcare organizations, leading to greater efficiency and less waste (Maleki Varnosfaderani and Forouzanfar, 2024). Disease management is arguably the most important use case of AI predictive analytics. Machine learning algorithms can use patient data, including medical history, laboratory results, and vitals, to predict the probability of developing a specific disease or health condition. This can allow healthcare providers to quickly identify patients with risk factors and offer early treatment to prevent or manage the condition (Sheng et al., 2021). AI can also assist healthcare providers in individualizing treatment plans utilizing patient data, enhancing patient outcomes and lowering expenses in the process. It is capable of changing predictive analytics in drug discovery. AI algorithms are also used to analyze databases, identifying potential drug targets and effectively speeding up these processes while lowering the cost of introducing new drugs to the market. Additionally, AI assists healthcare organizations in identifying candidates who would benefit from a particular drug, which can ultimately lead to improved patient outcomes and more personalized healthcare (Srivastava, 2023).

CHALLENGES AND LIMITATIONS OF AI AND PREDICTIVE ANALYSIS IN PREVENTING RANSOMWARE IN HEALTHCARE

AI and predictive analysis certainly bring notable advancements to the fight against ransomware, but their use in healthcare cybersecurity is not without its obstacles. As cyber threats today are evolving, the complex integration of AI and the intrinsic limitations to machine learning models, each presents significant barriers which makes foolproof ransomware protection a daunting challenge.

One of the key issues is the constantly changing landscape of ransomware. Cyber criminals are getting smart and are constantly improving their attacks, utilizing advanced evasion techniques to stream past legacy security solutions. AI and ML models need to continually adapt to these new threats. However, updating them requires huge data collection efforts paired with constant retraining and response time (Alraizza & Algarni, 2023). The rapidly evolving landscape of cyberattack techniques renders AI algorithms obsolete in real time, as threat actors experiment with novel tactics far quicker than defense systems can usually adapt. In addition, adversarial attacks are a direct threat to AI-based security systems. Adversarial machine learning techniques can also be employed by attackers to manipulate AI and ML models, resulting in misclassification of ransomware threats, generating false negatives. For example, malware signatures could be slightly modified, or data input patterns adjusted to help the cybercriminal evade detection, with AI-based solution becoming irrelevant. This requires the creation of robust and adaptive models of AI that can resist attempts to manipulate them (Kovács, 2022).

An additional key constraint is the dependence on high-quality data for optimal AI performance. AI and ML models must have access to large volumes of diverse, well-characterized data, in order to detect the ransomware behavior with accuracy. However, obtaining such data is a challenge, particularly in the healthcare domain where privacy regulations prevent access to sensitive patient information. Another challenge associated with AI-driven security solutions is that many of them are built on inadequate or low-quality datasets, resulting in a lack of consistency when it comes to threat detection and mitigation efforts. Moreover, AI-based detection systems still suffer from a long-standing problem of false positives. While AI models can recognize potential ransomware threats, they are also prone to flagging benign actions or activities as malicious. Such scenarios can disrupt the healthcare environments, exhausting resources in the process and triggering operational challenges. Overzealous threat detection can bring critical healthcare functions to a questionable halt, increasing wait times for patients and delaying service delivery. Achieving a proper balance between sensitivity and specificity in AI models continues to be a challenging proposition (Jegede et al., 2022).

However, the technical and operational challenges of incorporating machine learning-based protection strategies into existing healthcare cybersecurity systems are considerable. Since many healthcare organizations utilize legacy systems not built around modern AI driven security frameworks, they most often operate under default settings that make them vulnerable to cyber attacks. AI-based threat detection systems require significant investment in terms of infrastructure upgrades, training of the workforce, and changes in workflow that take both time and money to implement. The healthcare sector is often slower to adopt these solutions due to resistance to change, in addition to financial and technical constraints (Jack & Ali, 2024).

FUTURE DIRECTIONS

Considering the rise of ransomware attacks in the United States targeting critical healthcare information systems which is becoming both sophisticated and frequent, the role of AI and predictive analytics in cybersecurity must evolve to adapt to these new threats. Federated learning is an important area of advancement, allowing healthcare institutions to train AI models in a collaborative manner while keeping data private. This is an advantage as healthcare information is sensitive and this decentralized manner allows data from predictive analytics tools to learn without compromising patient confidentiality. Another important aspect when it comes to ransomware prevention is behavioral analysis. By leveraging AI-trained predictive models, organizations can continuously monitor user activity for anomalies and signs of an impending ransomware attack, enabling rapid intervention. For developing more secure cyber defense strategies, hybrid approaches that combine diverse detection technologies like heuristic analysis, anomaly detection, and

signature detection will help provide a well-rounded method for preventing ransomware attacks. These strategies improve prediction accuracy and reduce false positives which is vital for sustaining operational efficiency in healthcare settings (Djenna et al, 2023). In addition, AI-powered incident response solutions can automate initial mitigation actions, including isolating infected networks, terminating malicious processes, and beginning data recovery protocols. In the case of ransomware, being able to autonomously respond and in real-time is critically important to reducing the potential impact to critical healthcare infrastructure. Collaboration among organizations is also crucial for improving ransomware prevention. Sharing threat intelligence among healthcare institutions, government institutions, and cybersecurity organizations can contribute to improving AI-based threat detection by incorporating the latest ransomware techniques into prediction models. Moreover, for AI and predictive analytics to be applied in an ethical and standardized manner, regulations and policies must support these technologies in order to be adopted. Government policies should ensure that there are clear guidelines for compliance, accountability, and responsible use of AI, particularly in protecting information systems in healthcare. Predictive analytics models also need to undergo continuous learning and adaptation to keep up with evolving malicious ransomware threats. Cybercriminals are continually enhancing their attack vectors, which requires AI models capable of dynamically adapting to emerging threats via real-time data updates and evolving threat intelligence (Guvçi et al., 2023).

CONCLUSION

The integration of AI and predictive analytics in preventing ransomware attacks on critical healthcare information systems represents a major breakthrough in national cybersecurity efforts. AI-powered cybersecurity solutions increase the speed and efficiency of ransomware threat detection and response through predictive modeling, real-time data analysis, and behavioral insights. These technologies offer a proactive approach to threat mitigation, less false positives, and strengthened healthcare cybersecurity resiliency. Nevertheless, to fully realize the potential of AI and predictive analytics in ransomware prevention, continued innovation, inter-organizational collaboration, and strong regulatory support will help in realizing the potential of AI and predictive analytics in preventing ransomware. With the rise of AI capabilities in cybersecurity, it becomes important to adopt a strategic multi-faceted approach which will be essential in protecting healthcare information systems from ransomware and strengthening national security.

REFERENCES:

1. Alder, S. (2025) '2024 was another bad year for healthcare ransomware attacks', HIPAA Journal, 14 January. Available at: https://www.hipaajournal.com/2024-was-another-bad-year-for-healthcare-ransomware-attacks/
2. American Hospital Association (AHA). (2025) 'Change Healthcare cyberattack underscores urgent need to strengthen cyber preparedness for individual health care organizations and as a field', American Hospital Association, January. Available at: https://www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and
3. Badawy, M., Ramadan, N. & Hefny, H.A. (2023) Healthcare predictive analytics using machine learning and deep learning techniques: a survey. Journal of Electrical Systems and Inf Technol 10, 40. https://doi.org/10.1186/s43067-023-00108-y
4. Beek, K. (2025) 'Healthcare sector charts 2 more ransomware attacks', Dark Reading, 30 January. Available at: https://www.darkreading.com/cyberattacks-data-breaches/two-attacks-target-healthcare-sector-adds-growing-list-ransomware-threats
5. Cambridge Health. (2025) 'The role of AI and machine learning in healthcare cybersecurity', Cambridge Health, Available at: https://www.cambridgehealth.edu/healthcare-cybersecurity-privacy/healthcare-cybersecurity-privacy-information/the-role-of-ai-and-machine-learning-in-healthcare-cybersecurity
6. Cyber Threat Intelligence Integration Center (CTIIC)(2024) 'Ransomware attacks surge in 2023; attacks on healthcare sector nearly double', Office of the Director of National Intelligence, 28 February. Available at: https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf

7. CyberPeace (2024) Research Report: AI-Powered Ransomware Attack on a Healthcare Provider. Available at: https://www.cyberpeace.org/resources/blogs/research-report-ai-powered-ransomware-attack-on-a-healthcare-provider
8. Danner, D. (2025) Guide to cybersecurity in the healthcare industry: Regulations & best practices. Available at: https://www.bdemerson.com/article/healthcare-cybersecurity-guide
9. Djenna, A., Bouridane, A., Rubab, S., & Marou, I. M. (2023). Artificial intelligence-based malware detection, analysis, and mitigation. Symmetry, 15(3), 677. https://doi.org/10.3390/sym15030677
10. DriveLock. (2024) 'Impact of ransomware on healthcare systems', *DriveLock Blog*, 5 December. Available at: https://www.drivelock.com/en/blog/impact-of-ransomware-on-healthcare-systems
11. Emsisoft Malware Lab (2024) The state of ransomware in the U.S.: Report and statistics 2023. Available at: https://www.emsisoft.com/en/blog/44987/the-state-of-ransomware-in-the-u-s-report-and-statistics-2023/
12. Guvçi, Ferhat & Şenol, Ahmet. (2023). An Improved Protection Approach for Protecting from Ransomware Attacks. Journal of Data Applications. 69-82. 10.26650/JODA.1312412.
13. Jack, W. and Ali, W. (2024) 'Emerging cybersecurity threats: Trends, implications, and mitigation strategies', EasyChair Preprints, 20 January. Available at: https://easychair.org/publications/preprint/Hwf3/open
14. Jahic, D. (2024) 'Ransomware attacks: Death threats, endangered patients and millions of dollars in damages', *VOA News*, 10 March. Available at: https://www.voanews.com/a/ransomware-attacks-death-threats-endangered-patients-and-millions-of-dollars-in-damages/7520952.html
15. Jegede, Abayomi & Fadele, Alaba & Onoja, Monday & Aimufua, G.I.O. & Mazadu, Ismaila. (2022). Trends and Future Directions in Automated Ransomware Detection. Journal of Computing and Social Informatics. 1. 10.33736/jcsi.4932.2022.
16. Kaneria, B. (2025) *Why AI must increasingly power cybersecurity in healthcare*. Available at: https://www.healthdatamanagement.com/articles/why-ai-must-increasingly-power-cybersecurity-in-healthcare
17. Kovács, A. M. (2022). Ransomware: A comprehensive study of the exponentially increasingcybersecuritythreat. Insights into Regional Development, 4(2), 96–104. https://doi.org/10.9770/ird.2022.4.2(8)
18. McDill, V. (2023) 'Ransomware attacks on America's health care systems more than doubled from 2016 to 2021, exposing the personal health information of millions', University of Minnesota School of Public Health, 17 January. Available at: https://www.sph.umn.edu/news/ransomware-attacks-on-americas-health-care-systems-more-than-doubled-from-2016-to-2021-exposing-the-personal-health-information-of-millions/
19. Philips (2020) Predictive analytics in healthcare: Three real-world examples. Available at: https://www.philips.com/a-w/about/news/archive/features/20200604-predictive-analytics-in-healthcare-three-real-world-examples.html
20. Sheth, K. (2024) *Evolving threat landscapes: The role of predictive analytics in foreseeing cyber attacks*. Available at: https://www.healthdatamanagement.com/articles/why-ai-must-increasingly-power-cybersecurity-in-healthcare
21. Srivastava, D., Pandey, H. and Agarwal, A.K., 2023. Complex predictive analysis for health care: a comprehensive review. Bulletin of Electrical Engineering and Informatics, 12(1), pp.521-531.
22. Sweeney, E. (2017) *AI provides an urgent solution to evolving ransomware threats facing healthcare*. Available at: https://www.fiercehealthcare.com/privacy-security/ai-offers-healthcare-a-quick-fix-for-evolving-ransomware-threats
23. WebAsha (2025) *How AI helps detect and prevent ransomware attacks | A game-changer in cybersecurity*. Available at: https://www.webasha.com/blog/how-ai-helps-detect-and-prevent-ransomware-attacks-a-game-changer-in-cybersecurity
24. Nnamdi, M., (2024). Predictive analytics in healthcare. [online] ResearchGate. Available at: https://www.researchgate.net/publication/379478196_Predictive_Analytics_in_Healthcare
25. Maleki Varnosfaderani, S. and Forouzanfar, M., (2024). *The role of AI in hospitals and clinics: Transforming healthcare in the 21st century*. *Bioengineering (Basel)*, 11(4), p.337. Available at: https://doi.org/10.3390/bioengineering11040337

26. Sheng, J.Q., Hu, P.J., Liu, X., Huang, T.S. and Chen, Y.H., 2021. Predictive analytics for care and management of patients with acute diseases: Deep learning-based method to predict crucial complication phenotypes. Journal of Medical Internet Research, 23(2), p.e18372. doi:10.2196/18372.
27. Alraizza, A., & Algarni, A. (2023). Ransomware Detection Using Machine Learning: A Survey. Big Data and Cognitive Computing, 7(3), 143. https://doi.org/10.3390/bdcc7030143