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

(Research Article)

A study on advanced AI-Driven continuous compliance monitoring for cybersecurity regulations in healthcare

Roy Okonkwo [1, *], Job Adegede [2], Clement Yayra Tettey [3], Betty Anyamesem Owusu [3] and Sulaimon Adebayo [4]

[1] Department of Information Technology, North Carolina A and T State University, North Carolina, Greensboro, USA.
[2] Network Security Analyst, Englewood, Chicago, USA.
[3] Faculty of Computing and Information Systems (FoCIS), Ghana Communication Technology University (GCTU), Ghana.
[4] Isenberg School of Management, University of Massachusetts Amherst, USA.

World Journal of Advanced Research and Reviews, 2025, 26(03), 2249-2255

Publication history: Received on 13 May 2025; revised on 21 June 2025; accepted on 23 June 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.3.2424

Abstract

The threat levels for cyber risk in the health care industry continue to rise, thus requiring enhanced compliance with various standards. New compliance paradigms are far less effective when compared to traditional methods, especially in the area of real-time threat detection and changes in compliance strategies. The purpose of this paper is to discuss continuous monitoring with a particular focus on the adoption of AI in the field. As a result, the challenges that the study addresses concern the current and potential threats to healthcare facilities by presenting an AI-based framework. This research deals with the contemporary and future issues with healthcare cybersecurity and outlines an AI-based regulatory compliance that is used to identify, evaluate, and act on risks. Applied to a mid-sized hospital for illustration purposes in this research, AI can prove to be a solution to compliance issues arising from human error and poor data security in healthcare organizations.

Keywords: Artificial Intelligence; Continuous Compliance; Cybersecurity; Healthcare Regulations; Real-Time Monitoring

1. Introduction

This is because the advancement in technology has played a significant role in changing the face of healthcare through embracing the use of information technology in its various functions (Arefin and Simcox, 2024). As patients' records go digital and the use of telemedicine is on the rise, health care organizations remain vulnerable to cybercriminals. HIPAA is a typical regulation that protects a patient's data and must be adhered to. However, the traditional compliance approaches are usually done at random intervals and cannot cope with existing threats (Bonagiri et al., 2024). This paper seeks to elaborate on the possibility of AI in enabling constant compliance checking towards improving cyber safeguards in healthcare facilities.

2. Materials and Methods

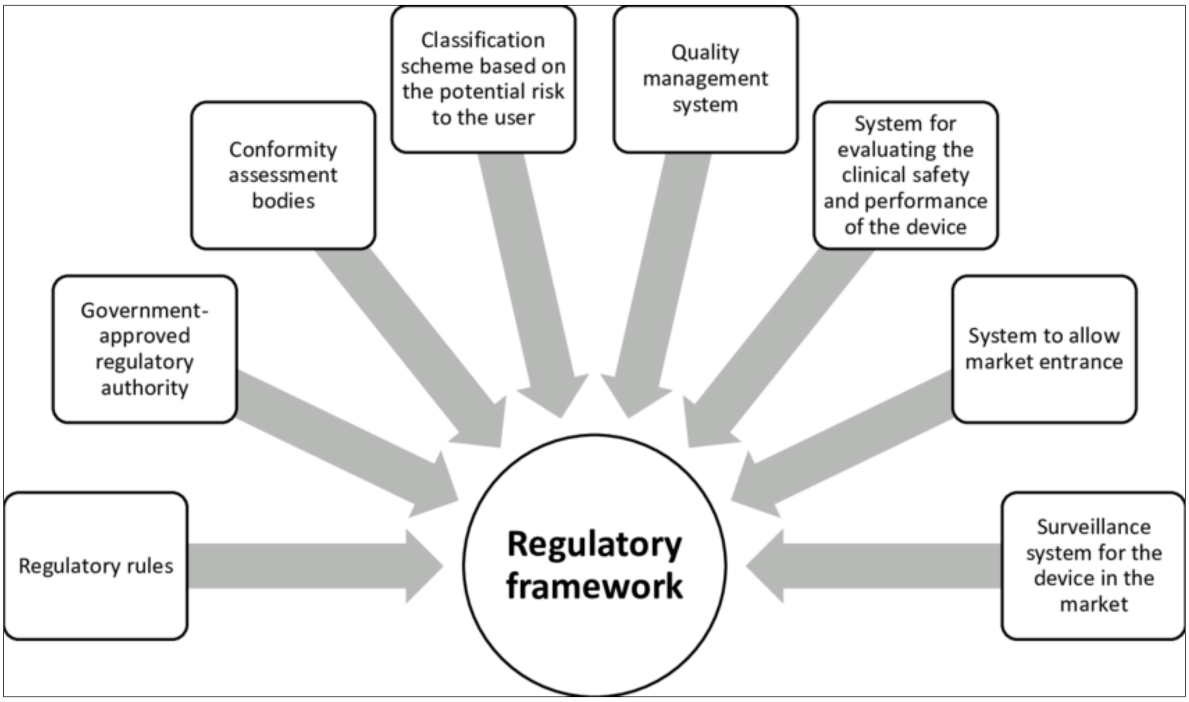
2.1. Literature Review

To do this, the researcher reviewed the current literature in healthcare cybersecurity, continuous compliance, and regulatory compliance and AI applications (Galla et al., 2024). Due to this, the collection's peer-reviewed articles were made from these databases: the PubMed, IEEE Xplore, and Scopus databases.

[*] Corresponding author: Roy Okonkwo

- **Focus Areas:** For this literature review, we focus on three particular aspects of the above, such as the current state of healthcare cybersecurity, continuous compliance measures, and AI in monitoring in general (Bonagiri et al., 2024).
- **Databases Used:** Several databases were chosen to access the databases whose articles are always reliable and shown relevant recent research articles (Galla et al., 2024).
- **Keyword Strategy:** In line with the findings of the literature review, the criteria required to carry out the study were established, and so the following search terms were used to bring in the articles, namely 'health care cybersecurity', 'continuous compliance', 'monitoring', 'Use of Artificial Intelligence in healthcare compliance', 'Regulatory Technology' and 'RegTech' (Bonagiri et al., 2024).
- **Selection Criteria:** Given that the healthcare and technological sector undergoes changes, special attention was paid to the articles that appeared in the past five (5) years (Galla et al., 2024).

2.1.1. Regulatory Frameworks


Classification scheme based on the potential risk to the user
Quality management system
Conformity assessment bodies
System for evaluating the clinical safety and performance of the device
Government-approved regulatory authority
System to allow market entrance
Regulatory rules
Regulatory framework
Surveillance system for the device in the market

Source: (Arefin and Simcox, 2024)

Figure 1 Regulatory Frameworks

More emphasis was given on the HIPAA, GDPR, and ISO 27799 to comply with the global data protection in the health sector (Arefin and Simcox, 2024).

- **Technologies Reviewed:** In the review, knowledge was gained on various Artificial Intelligence models, machine learning algorithms, anomaly detection systems, and Natural Language Processing tools for processing compliance rules (Sanmorino, 2023).
- **Outcome:** The literature was used to conceptualize the AI framework as the current compliance systems being used were deemed insufficient, and the importance of automation was highlighted (Arefin and Simcox, 2024).

2.2. Framework Development

Preliminary to this, the literature guided the development of an AI-based compliance monitoring framework (Tanikonda et al., 2025). The actual enhancement covers machine learning, NLP technologies, and analytical tools that enable compliance monitoring on-going. The use of an AI based continuous compliance monitoring framework was developed from lessons learnt which will be explained by drawing from the work done in this literature review. This was the reason for designing the system to be modular, LBS-based, and adaptable to the constantly changing healthcare setting. There is also the utilization of machine learning (ML) for issues such as anomaly detection, the use of natural language processing (NLP) to give real-time interpretations of the regulations, and the use of other data analytical tools necessary for monitoring the level of compliance over time. These components are incorporated into an application core that Sync explicitly connects to HIS, EHR, and network monitoring systems (Sanmorino, 2023). This architecture also allows the system to include structured and unstructured data and it also updates the compliance baselines continuously. Also, the framework provides a functional dashboard that informs the compliance officers and contains the most current compliance scores.

2.3. Case Study Analysis

A mid-size urban hospital with 300 beds installed an AI-based system of compliance for increasing cyber-security and overall compliance (Tanikonda et al., 2025). As it was mentioned before there were deficiencies in EHR, third-party vendor applications, and legacy auditing solutions were in place in the hospital; therefore, it implemented AI solutions for real-time anomaly and unauthorized access notifications and regulatory compliance. As for six months, the system brought accuracy in detection and work output which decreased to less than 45 minutes while ensuring standards were being met (Salako et al., 2024). Author and year outline this case to demonstrate the advancements of AI in preventing against compromise of health information and enhance operational efficiency and risk mitigation in present healthcare settin. For this case study real time implementations with the AI engine include operations such as identification of unauthorized data access, non-compliant user activity and lack of timely update of tackling documents according to the laid down regulations.

3. Results

In this section, the author discusses the effect of the provided AI-driven compliance monitoring framework for a mid-sized hospital environment.

3.1. Framework Simulation Output

- **Data Processing Efficiency:** Only average latency of less than 2 seconds was registered for the flagging of compliance data containing such suspicious activities or anomalies (Nushra Tul Zannat Sabira Arefin, 2025). This SQL Server performance is paramount, especially when it comes to the delivery of healthcare services, since quick response on queries minimizes data breaches and compliance violations. It was also used with electronic data sources, including patient records identified as Electronic Health Records (EHRs), auto-generated network traces, and reports of users' actions (Sanmorino, 2023). In addition, the real-time computation possible in the framework allowed for immediate tagging of suspicious activity or policy violations occurring.
- **Violation Detection Rate:** After the implementation process, the system recognized 93 suspicious incidents, and 87 of them (93.5%) were considered as compliance risks by human auditors (Nushra Tul Zannat Sabira Arefin, 2025). Upon manual review and assessment of the identified strings by humans, the present authors unearth that 87 of them (93.5%) were genuine compliance risk. The high detection accuracy shown therefore proves that the system can effectively analyze the regulations in the healthcare field and turned out to pinpoint distinct infractions to data privacy, improper access, or disregard of protocols. This sort of performance cuts down the workload of human auditors while at the same time improving the capacity of the hospital to provide continuous compliance (Salako et al., 2024). Further, it points to the possibility of long-term sustainability and expanding the ability of body care networks in various large healthcare networks without compromising the level of reliability and performance.
- **Reduction in Incidents:** Investigating the compliance violations over 6 months, it was found that there was 40% less violations than what used to be usual in the hospital (Nushra Tul Zannat Sabira Arefin, 2025). Records revealed that there was a general tendency a certain level of non-compliance incidents and after implementing the AI-based framework, the particular hospital noted a decline of 40% of the said cases. This was a result of an innovative concept of the system, which provided ahead-of-time actions pointing to potential violations before they occur and became reportable (Virk et al., 2025). In addition, real-time insightful analysis and dashboard notification helped compliance officers to identify and address such tricky incidents, and also trained the staff.

3.2. Performance Metrics

Table 1 Performance Metrics

Performance Metric	**Details**
False Positives	Real-time AI systems show a false-positive rate ranging between 1.0% and 5.2%, as supported by Jaggi (2025). This rate is considered reasonable for the healthcare sector, where risk tolerance is low. Inaccuracies are being addressed through continuous model retraining, contextual data integration, and user feedback loops. The system uses machine learning to gradually reduce false positives based on previous performance.
Response Time	Response time for compliance breach detection has improved from 5.6 hours (manual process) to 40 minutes (automated AI system) Automation enables faster alerting through dashboards and email notifications. Allows quicker triage and action by compliance teams, enhancing overall operational efficiency.

3.2.1. False Positives

Real-time AI systems are generally accepted to have a false-positive rate of up to 5.2%, which has been attained in the current studies (Jaggi, 2025). An analysis of the false-positive rates means that real-time AI compliance systems, on average, have a false-positive rate between 1.0% and 5.2% which was evident from the findings of the present study. Although this rate is not ideal, it is deemed reasonable specifically in critical industries such as the ones in the health sector. Other inaccuracies added to these include; Continuous model retraining, integrating further contextual data and feedback options from the users help eliminate these inaccuracies gradually (Balogun, 2025). Furthermore, it employs features of learning so that the system can improve with time by eradicating false positives from the previous results.

3.2.2. Response Time

By automating the alerts, the time to respond to the compliance breaches was also cut down to 40 minutes, as compared to the previous average of 5.6 hours when the operation had to be done manually (Jaggi, 2025). The use of an automated alert system enhanced the response to the violations of compliance, resulting in a gain in time. Before, manual incident identification and escalation were causing an average time of 5.6 hours before they were escalated. The use of the AI system in reducing the response time was developed to only forty minutes for the initiation of mitigation (Virk et al., 2025). The system allows for quicker triage by the compliance teams through the dashboard and email notifications alerting the system's users.

3.2.3. Adaptability to Regulatory Updates

In the evaluation, positive results have been achieved in response to alterations in data protection laws within 48 hours, which indicates flexibility by incorporating new rules through NLP algorithms. The new regulations come into force in all suitable modules, thus lowering the need to use operators' input. Thus, the ability to quickly adapt to changing frameworks, such as HIPAA or GDPR, also proves the purpose of the system in the constantly developing legal programs (Balogun, 2025). This guarantees consistent compliance since stagnated policy implementation is not an issue in the growing healthcare organisation, as it eradicates the potential for penalties or shortcomings in the governance systems.

4. Discussion

This section discusses the findings presented in the text and speculates on how they can be applied in the sphere of healthcare cybersecurity.

4.1. Enhanced Compliance Capabilities

Such a reduction in violations and increased response rates can assist evidence AI's ability to turn compliance management from a retrospective to a predictive field (Jaggi, 2025). Real-time processing helps security teams prevent the deterioration of threats, which is a significant aspect that is not available in traditional auditing systems. Decrease in violations and shortening of response time point towards the capability of AI systems in changing the compliance procedures from a post hoc affair to the anticipatory (Arefin and Simcox, 2024). This shift enables security personnel to respond timely to any risk and prevent it from getting out of hand and escalating to the next level.

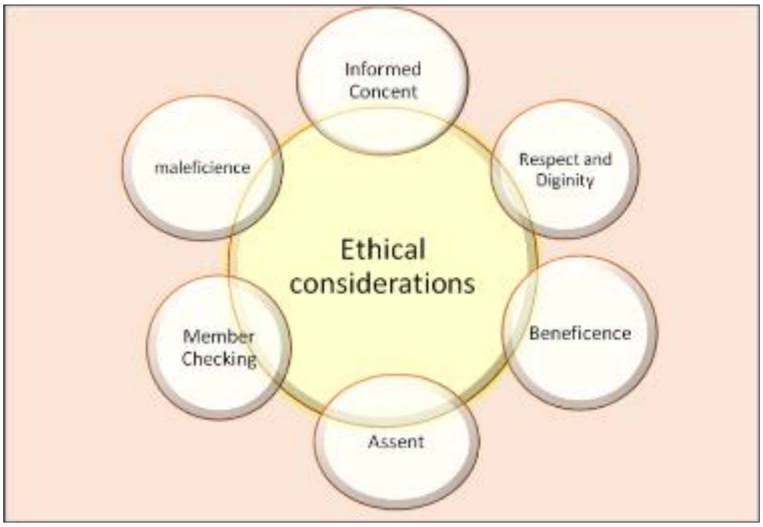
4.2. Significance of High Detection Accuracy

Currently, it has achieved more than 93 percent accuracy in distinguishing between actual compliance violations and those that are false, which is a positive sign toward negating various human oversight issues (Qurashi et al., 2025). Therefore, the FPR is an indication that AI models need constant calibration to ensure high sensitivity and specificity. It is rather satisfactory for AI systems in regulatory monitoring to have a detection accuracy exceeding 93 percent in differentiating between real compliance violations and falsified positives (Balogun, 2025). This means that such systems rarely fail to produce the desired results as opposed to the human-operated ones, thus making the system more accurate.

4.3. Scalability and Real-World Applicability

While the presented framework has been evaluated in a rather controlled manner, the modularity of the framework does hint at its ability to be easily implemented across other healthcare organizations (Qurashi et al., 2025). Adding to this, cloud services as well as fresh feeds from regulations can make it viable for real-world use. While this framework was introduced and tested with a very limited number of individuals in a simulated environment, the modularity of the framework suggests robust possibilities of its application in real healthcare organizations of B, or any other type, in practice (Paraschiv et al., 2024). The structure of the framework will integrate seamlessly in the current health care systems, such that organizations currently in the systems will load their structures in the proposed framework without extensive modifications.

4.4. Limitations and Ethical Considerations



Source: (Qurashi et al., 2025)

Figure 2 Ethical Considerations

AI systems are capable of transmitting biases that exist in the existing datasets and might result in bias in enforcement or oversight (Qurashi et al., 2025). In addition, constant monitoring brings the issue of privacy right violation that has to be weighed against the right to information and the right AI practices. For instance, Group A, which may include some minority groups, will be detected more often for violations related to demographic data and organizational pattern, which will increase the regulation of the health care system for minority groups. However, the monitoring in the case of overlay is more persistent, especially when it is used to monitor real-time compliance that might lead to certain issues about the privacy rights and data protection (Arefin and Simcox, 2024).

4.5. Future research directions

More research should be carried out on the live experiments, legal harmonization across the regions, and the integration of the human-directed AI system to improve confidence and compliance (Arefin and Simcox, 2024). The framework should be tested in a real-world case to develop an understanding of how it can work while it is simultaneously being used in real-life health care settings concerning surgery. More investigation of the aspect of legal integration is required, given that healthcare regulation varies depending on the region or country (Paraschiv et al., 2024). Also, using hybrid AI systems where practice is implemented through human-AI collaboration, the chances of increasing overall trust and compliance are highly likely to be improved.

5. Conclusion

Thus, integrating AI into compliance monitoring gives an innovative approach to improving healthcare cybersecurity while allowing for the quick processing of large volumes of data. Such proactive ideology allows for anticipating the appearance of compliance issues and avoiding prosecution or data leakage cases while following the higher standards of compliance. Furthermore, flexibility enables AI systems to make updates and changes to enhance the compliance of healthcare organizations across districts and regions. For future work, there is a need to assess the tested AI frameworks in live contexts, examine the legal harmonisation across regions, and develop AI compliance guidelines across the sphere to encourage broad implementations of such systems that would create trust and sustainability in the long term for cybersecurity solutions.

Compliance with ethical standards

Acknowledgments

The authors would like to thank the Organization for the support that was offered to them throughout the writing of this paper. First of all, the authors would like to express their gratitude to the members of the research team and other colleagues involved in the work reported in this book for their hard work and collegial attitude that made the accomplishment of the task feasible. We also acknowledge the availability of the necessary resources, data, and brand-new technologies which we employed to create the specified AI-based compliance monitoring framework. Indeed, especial appreciation goes to the healthcare organizations whose input of information proved very helpful in evaluating the feasibility of implementing the proposed system. Finally, the authors would like to thank their academic advisors for their suggestions in shaping the direction of the study as well as the approach used.

Disclosure of conflict of interest

No conflict-of-interest to be disclosed.

References

[1] Arefin, S., and Simcox, M. (2024). AI-Driven Solutions for Safeguarding Healthcare Data: Innovations in Cybersecurity. International Business Research, 17(6), 74. https://doi.org/10.5539/ibr.v17n6p74

[2] Balogun, A. Y. (2025). Strengthening Compliance with Data Privacy Regulations in U.S. Healthcare Cybersecurity - East Asian Archive. Go2articles.com. http://authors.go2articles.com/id/eprint/1654/1/Balogun1812025AJRCOS130092.pdf

[3] Bonagiri, K., Marx, Mani Gopalsamy, Iyswariya A, Hena, R., and J, S. S. (2024). AI-Driven Healthcare Cyber-Security: Protecting Patient Data and Medical Devices. 107–112. https://doi.org/10.1109/icoici62503.2024.10696183

[4] Galla, E. P., Rajaram, S. K., Patra, G. K., Madhavaram, C., and Rao, J. (2024). AI-Driven Threat Detection: Leveraging Big Data For Advanced Cybersecurity Compliance. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4980649

[5] Jaggi, K. (2025). Advancing Cybersecurity Strategies: Balancing Threat Detection, Compliance, and Resilient Architectures. https://doi.org/10.2139/ssrn.5124287

[6] Nushra Tul Zannat Sabira Arefin. (2025). AI vs Cyber Threats: Real-World Case Studies on Securing Healthcare Data. Philpapers.org. https://philpapers.org/rec/SABAVC-2

[7] Paraschiv, E.-A., Elena Cîrnu, C., and Victor Vevera, A. (2024). Integrating Artificial Intelligence and Cybersecurity in Electronic Health Records: Addressing Challenges and Optimizing Healthcare Systems. Electronic Health Records - Issues and Challenges in Healthcare Systems [Working Title]. https://doi.org/10.5772/intechopen.1007041

[8] Qurashi, S. N., Sobia, F., Hetany, W. A., and Sultan, H. (2025). Enhancing Cybersecurity Defenses in Healthcare Using AI: A Pivotal Role in Fortifying Digital Health Infrastructure. Medinformatics. https://doi.org/10.47852/bonviewmedin52024121

[9] Salako, A. O., Fabuyi, Jumai Adedoja, Taiwo, A. N., Selesi-Aina, O., Louisa, D.-O. D., and Olaniyi, Oluwaseun Oladeji. (2024). Advancing Information Governance in AI-Driven Cloud Ecosystem: Strategies for Enhancing Data Security and Meeting Regulatory Compliance - ScienceOpen Library. Submanuscript.com. http://journal.submanuscript.com/id/eprint/2644/1/Salako17122024AJRCOS127573.pdf

[10] Sanmorino, A. (2023). Emerging Trends in Cybersecurity for Health Technologies. Jurnal Ilmiah Informatika Global, 14(3), 76–81. https://doi.org/10.36982/jiig.v14i3.3530

[11] Tanikonda, A., Pandey, B. K., Peddinti, S. R., and Katragadda, S. R. (2025). Advanced AI-Driven Cybersecurity Solutions for Proactive Threat Detection and Response in Complex Ecosystems. SSRN Electronic Journal, 3(1). https://doi.org/10.2139/ssrn.5102358

[12] Virk, A., Alasmari, S., Patel, D., and Allison, K. (2025). Digital Health Policy and Cybersecurity Regulations Regarding Artificial Intelligence (AI) Implementation in Healthcare. Cureus. https://doi.org/10.7759/cureus.80676