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

(Review Article)

# Human-AI collaboration in healthcare security

Sateesh Kumar Rongali * and Durga Bramarambika Sailaja Varri

*Judson University 1151 N State St, Elgin, IL 60123* and University of Central Missouri, 108 W South St, Warrensburg, MO 64093, US.*

World Journal of Advanced Research and Reviews, 2025, 25(03), 2505-2510

Publication history: Received on 18 February 2025; revised on 22 March 2025; accepted on 25 March 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.3.0562

## Abstract

Healthcare security gets a transformative boost from Artificial Intelligence (AI) implementation which improves patient protections as well as protects healthcare information systems while simultaneously generating operational efficiency. Modern healthcare organizations which depend heavily on digital data systems use AI technologies to develop advanced cybersecurity methods that protect their confidential patient data. Healthcare facilities require real-time artificial intelligence analysis of data volumes together with anomaly detection for their defense against escalating cybersecurity threats in healthcare. Healthcare security benefitted considerably from AI technologies but organizations encounter multiple challenges because AI raises privacy issues in patient data and creates biases within algorithmic decisions while patients depend heavily on automated systems. Computer systems powered by AI face challenges regarding ethical standards because they must demonstrate transparency and accountability whenever they control patient healthcare decisions or security systems. The study investigates the coexistence of humans alongside AI systems in healthcare security by establishing the essentialness of human expertise for handling ethical and legal intricacies of healthcare data security. The paper explains that AI systems need to show transparency along with continual updates and compatibility with traditional security systems but still require human oversight for fair accountability assessments. The paper analyzes AI-human teamwork to provide evidence about best practices for handling AI risks and achieving better patient safety and trust in healthcare.

**Keywords:** Algorithmic Bias; Artificial Intelligence (AI); Cybersecurity; Data Privacy; Ethical Considerations; Healthcare Security; Machine Learning (ML); Threat Detection

## 1. Introduction

The healthcare field now rapidly adopts digital solutions to enhance clinical results plus administration process efficiency and better treatment quality for patients. The growing dependence of healthcare organizations on electronic health records (EHRs) as well as telemedicine platforms and digital systems requires the management of huge sensitive patient data quantities. Healthcare systems grew progressively susceptible to security risks since their digital transformation because these vulnerabilities affect the privacy of patient data as well as disrupt operations and damage patient-provider trust and medical facility operations.

Protecting patient data constitutes an absolute necessity because healthcare information needs to remain secured at all times. Conventionally important security measures do not provide sufficient protection against the advanced complexity and size and modern sophisticated cybersecurity threats. AI technology has proven itself as an effective method to boost healthcare security systems. Machine learning-based AI systems acquire the capability to examine vast datasets and recognize unusual behavior patterns while forecasting security risks before swiftly responding to identity security incidents instantaneously. The features of artificial intelligence enable its use for proactive attack prevention and improved threat recognition as well as non-stop data shield maintenance.

* Corresponding author: Sateesh Kumar Rongali

AI implementation in healthcare security requires solutions for various technical obstacles. The successful implementation of AI systems requires addressing multiple issues because these systems deliver automated solutions that cut down detection and security risk mitigation durations. The main obstacles within AI deployment consist of data security concerns together with algorithmic prejudice and dependence on AI systems running amiss. Business entities in healthcare need to handle existing regulations while also moving forward.

The substantial AI progress made in recent times has not eliminated flawlessness from artificial systems. AI systems deliver results according to the quality of training data they receive because biased or missing information during training creates incorrect and prejudiced decisions. A security threat identification system that receives biased training data with unequal representation of different patient groups will detect threats from those populations more frequently so it generates elevated false alerts and discriminatory incidents. The exceptional speed at which AI detects and responds to threats does not extend to its ability to determine broader threatening contexts. Human action becomes the most essential step at this particular point.

The integration of AI into healthcare security needs human professionals to succeed because their knowledge is vital to preventing system failures. The proper function of AI lies in providing additional support to human decision-makers instead of substituting their activities directly. The decision-making process for ethical issues together with incident assessment and both legal and regulatory standard compliance needs people who are professionals. Organizations that blend human expertise with AI systems produce security systems which maximize the potential of each technology to protect healthcare data.

This paper investigates the cooperative functions of human operators and AI systems for improving healthcare security. The discussion examines both the advantages and barriers of implementing AI into medical security platforms while proposing operational methods to reduce security risks related to AI adoption. This paper evaluates how Artificial Intelligence enhances security operations through data security and threat management until incident resolution while discussing mandatory privacy management and ethical accountability standards. The ultimate objective of this research is to establish an extensive grasp of AI cooperation with humans in healthcare defense methods as well as patient information security and digital healthcare system trust establishment.

## 2. AI's Role in Healthcare Security

The medical security can transform through Artificial Intelligence technologies because these tools enhance security threat response times combined with better accuracy and enhanced efficiency. Digital expansion of healthcare systems leads to an increasing number of cybersecurity risks which range from unapproved access to medical files to difficult ransomware incidents. The combination of machine learning (ML) and natural language processing (NLP) technologies in AI serves as a protective measure to minimize security threats while increasing general security performance.

### 2.1. Data Protection

Healthcare organizations and their patients face major consequences because protecting patient data remains an essential priority throughout medical services. The fundamental capability of AI has proved essential for protecting the security of this data through achieving confidentiality and integrity as well as guaranteeing availability. By analyzing electronic health record (EHR) and other complex data access outlines machine learning framework distinguishes abnormal patterns that might reveal potential system experience cyberattacks.

AI systems recognize out-of-ordinary access behaviors when unidentified parties attempt compilation of particular patient files or healthcare workers review non-relevant medical data. Security personnel receive alerts regarding suspicious activities permitting them to investigate potential weak points that could evolve into major security violations (Binns & Hu, 2023). Through AI monitoring of encryption protocols coupled with data transmission across networks security is maintained during information transfer. Through its real-time analysis AI systems identify security flaws in operational procedures so they can offer proposals for better encryption techniques and reinforced access protocols.

AI enables healthcare organizations to anonymize patient information before they apply it to research studies or share it with external providers. The protection of data integrity by AI technology results in secure medical information thus lowering the risk of privacy violations alongside potential regulatory fines.

### 2.2. Threat Detection

Complex cyberattacks endanger healthcare organizations through their deployment of ransomware programs and utilization of phishing schemes as well as their delivery of malware. The attacks consist of technical vulnerabilities and social engineering methods which make them difficult to detect by using traditional security defenses. The tracking of new security threats by machine learning systems is effectively managed through its data analysis capabilities to study vast data collections while discovering elusive patterns that security personnel would miss.

The main asset that allows AI to detect threats arises from its built-in capability to learn continuously from additional data. Network security improves when AI systems process additional healthcare data and network traffic because they develop expertise in recognizing stealthy patterns that deviate from previous behavior. AI systems detect deviations in user behavior by tracking changes to normal activities including instances where users access excessive data amounts or try to penetrate security frameworks. The observed unusual activities might signal that malware has infected the system or cyberattackers are launching an assault.

AI models obtain real-time threat intelligence from worldwide sources to guarantee they remain updated on contemporary attack methods and malware varieties and cyber security techniques developed by attackers. The proactive nature of these capabilities enables healthcare organizations to maintain an advanced position against cybercriminals which leads to stronger prevention of attacks from developing further.

### 2.3. Incident Response

Rapid response must be followed by effective measures in the case of security breaches and cyberattacks to prevent further harm to systems. Security teams obtain faster issue resolution because AI delivers automated responses to established threats during incident response activities. Under ransomware attack detection an AI system immediately activates device network isolation to stop malware from spreading throughout the system. AI functionality enables automated execution of established response protocols that encompass unauthorized IP address blocking and system administrator alerts and backup recovery protocols activation.

AI systems use analytical techniques to trace security incidents along with determining their attack origins and boundaries and capability to create destruction. Analysis of network traffic with system logs and other relevant data using AI helps security teams correctly identify the source of breaches while determining the total extent of spilled information. The gained valuable information enables human experts to make optimal decisions both for containment and remediation steps and recovery strategies (Jones & Brown, 2022).

The post-incident tasks can be automated using AI through incident report generation and systematic vulnerability assessment and forensic analysis. By carrying out these tasks through automation the recovery process becomes faster and more efficient and regulatory documentation gets automatically created as a result.

### 2.4. AI-Driven Predictive Security

The ability of AI systems to detect upcoming security threats together with their preventive intervention is a highly promising healthcare security application. Artificial intelligence systems using predictive analytics examine historical attack records to establish trends which enable them to make forecasts about upcoming security weaknesses. AI systems evaluate previous attack data to identify patterns which enable them to forecast healthcare organizations and departments that would most likely become targets using information about their digital profiles and public visibility alongside their internal security shortcomings.

AI conducts vulnerability analysis to determine the highest-priority areas which demand attention through evaluation of possible attack situations. AI enables healthcare organizations to identify system vulnerabilities through continuous scanning which supports their proactive software and system update process until attackers exploit the vulnerabilities. The predictive features of this technology increase both security level and minimize cyberattack success probabilities (Kumar & Maan, 2020).

The critical position of artificial intelligence in healthcare security becomes increasingly important because it delivers better data security and it detects threats immediately while speeding up incident responses. The analysis of big data through patterns helps this technology execute sophisticated cyber threat defense. The purpose of Artificial Intelligence systems is to boost human specialist capabilities rather than function as their substitute. The implementation of AI in healthcare security demands thorough evaluation of ethical matters along with data privacy concerns and human involvement to make decisions.

## 3. Challenges in Human-AI Collaboration for Healthcare Security

The implementation of AI for healthcare security enhancement faces multiple challenges which stem from its integration with current systems. Healthcare professionals need solutions to tackle these obstacles before AI adoption because this allows proper AI application that strengthens medical expertise while reducing safety hazards. Healthcare security faces several primary obstacles in human-AI teamwork such as protecting patient data along with the way algorithms process information and overdependence on these systems and difficulties in integrating systems together.

### 3.1. Data Privacy Concerns

Healthcare institutions exist as the most vulnerable ground regarding data privacy safeguards. AI systems that handle healthcare security must analyze extensive patient data sets under U.S. HIPAA and similar regulatory mandates so their handling of confidential information becomes a direct security concern. The proper compliance of AI technologies with privacy regulations stands vital since patient data violations through misuse lead to major legal consequences alongside ethical problems. Machine learning systems require design features that prevent unintentional disclosure of critical information during investigative activities and sharing operations (Smith & Zhang, 2021).

### 3.2. Algorithmic Bias

Historical datasets used for AI training sometimes reveal demographic-based or geographic-based prejudices when training includes restricting healthcare accessibility. Security-related decision outputs from AI algorithms will feature biased characteristics when training occurs with data that includes discriminatory elements. The training data contains erroneous patterns leading to the unfair tagging of specific patient groups as security risks. Systems with biased training data might generate wrong classifications that result in discriminatory behavior and unequal patient treatment thereby creating distrust and treatment problems for healthcare. Provoking unbiased results demands well-organized training data selection and ongoing AI output assessment with human supervisor availability to handle necessary interventions.

### 3.3. Over-reliance on AI Systems

Healthcare security encounters a crucial risk when implementing AI because it leads organizations to depend excessively on autonomous technology systems. The automated capacity of AI to work through large datasets to spot security flaws does not extend to healthcare-specific understanding regarding both medical scenarios and human behavior. The complete interpretation of ethical and legal and practical implications associated with security decisions remains beyond AI capabilities which results in potentially dangerous consequences. AI must receive human evaluation to ensure its recommendations get proper contextual interpretation because only humans can maintain healthcare regulations and ethical standards alignment. Heavy dependence on AI systems without suitable human intervention generates the risk of security errors along with missing vulnerabilities which need human evaluation.

### 3.4. System Integration

Healthcare institutions maintain dual healthcare systems through old legacy frameworks alongside contemporary digital systems which creates barriers for AI-based security system implementations. Healthcare organizations face numerous complications regarding platform interoperability when implementing AI tools because they demand extensive issuance of real-time data analysis and direct comprehensive analysis. The integration problems between different security systems delay AI security deployment and reduce its effectiveness across diversified system networks (Zhang & Xie, 2021). Organizations serving the healthcare field need to put funds into developing the necessary infrastructure for running AI technologies because this implementation can demand substantial time and financial resources. For AI tools to prosper they need to operate successfully with current security frameworks which enables their proper functionality.

## 4. Solutions to Overcome Challenges

A mixture of technological progress and ethical principles together with domain expertise must be applied to resolve human-AI collaboration problems for healthcare security. Multiple solutions exist to address the challenges in AI frameworks related to data security, biased algorithms and AI dependency and system compatibility problems which guarantee the efficiency, fairness and security of AI systems.

### 4.1. Ensuring Data Privacy and Compliance

The integration of AI systems into healthcare security needs to fulfill all requirements established by privacy regulations including HIPAA compliance. The implementation of secure encryption methods for static data storage and transmission represents ways to solve privacy issues. Healthcare organizations should utilize AI systems with privacy-native features including differential privacy that enables AI algorithms to run data analytics without disclosing patient records (Patel & Kumar, 2021). The combination of transparent data processing systems with clear organization policies regarding data governance serves to reduce risks while building trust between users and healthcare institutions.

### 4.2. Mitigating Algorithmic Bias

The prevention of algorithmic bias requires AI systems to work with training data collections that represent various patient populations in their full diversity. The training process of AI depends on data duration that incorporates a favorable distribution of patients who represent diverse characteristics between age groups as well as gender profiles and citizens from all ethnicities and financial backgrounds to lessen algorithmic biases in programming decisions. Perpetual system performance review and audit operations serve to detect and eliminate biases that manifest unintentionally. The evaluation process of AI systems should integrate a multidisciplinary group including data scientists alongside healthcare providers alongside ethical specialists alongside regulatory authorities to actively handle ethical issues during development.

### 4.3. Reducing Over-Reliance on AI Systems

Security decision-making must have human oversight to prevent the misuse of AI systems as such tools. The quick threat identification capability of AI-operated systems against extensive data sets remains only a support function compared to human security evaluation choices. Healthcare organizations should develop a combined security approach by connecting AI systems with cybersecurity staff who will interpret AI information and supply recommendations for defense systems. Security staff members who receive ongoing instruction about analyzing AI outputs and employing decent thinking with AI alerts will use AI systems effectively alongside their human capability (Thompson & Mehta, 2019).

### 4.4. Facilitating System Integration

Healthcare organizations can solve system integration difficulties by choosing modular AI solutions which were designed to interoperate with other systems. These systems allow customization to merge with existing healthcare infrastructure for achieving efficient cross-platform operation of AI tools. Healthcare organizations can improve the flexibility of AI technologies through their investment in scalable security solutions which operate in cloud environments. AI vendors must partner with healthcare providers and IT professionals for efficient integration of AI tools into existing security frameworks designed to satisfy healthcare organization requirements.

## 5. Ethical Considerations in AI-Driven Healthcare Security

AI implementation in healthcare security brings forth critical ethical issues which need proper handling to guarantee proper usage. Privacy of patients remains among the main ethical issues in this context. AI systems need access to very large quantities of sensitive health data and the secure management and HIPAA compliance of this data stands as an essential prerequisite. Medical IT systems need built-in features for maintaining treatment privacy and blocking unauthorized users from accessing or dishonestly handling information.

Mathematical systems raise substantial ethical difficulties when it comes to fair outcomes. Inadequate training of AI models enables existing data biases to strengthen or deteriorate resulting in unfavorable treatment towards particular patient demographics (Chen & Wang, 2020). Security systems employing Artificial Intelligence usually identify specific groups as high-risk targets because their algorithms base decisions on skewed historical information. AI model evaluations must be untiring so scientists can discover and remedy biases which maintain equal treatment between all patient populations regardless of their demographic backgrounds.

The absence of accountability represents another critical problem within this matter. The process of security-related decisions made by AI systems must have human experts take ultimate responsibility as they oversee these choices including blocking patient data access and detecting breaches. The implementation of transparent accountability systems must happen to provide both transparency and safe ways for people to take action when AI systems cause damage or errors. Ethical standards should place humans in charge of overseeing AI functionality because this technology exists to assist human choices rather than performing decisions independently.

## 6. Conclusion

The integration of AI systems in healthcare security brings major advantages that boost protection of data and strengthen both intrusive threat monitoring and quick response to cyber-criminal activities. Accomplished by using machine learning alongside other AI technologies healthcare organizations strengthen their defenses against complex cyber enemies which protects both patient data confidentiality and its integrity. Healthcare organizations encounter multiple obstacles during the implementation of AI technology for security operations. AI penetration into healthcare requires rigorous solutions for privacy matters and bias prevention and minimization of automated system overreliance as well as system integration challenges in order to achieve effective and ethical results.

The implementation of healthcare security benefits from AI tools when they enhance human expertise instead of taking over their role. To minimize risks along with biases continuous monitoring should take place while proper training and rigorous testing must happen because they form essential components. AI systems need to integrate ethical considerations regarding transparency together with accountability and fairness systems to deliver equitable service for all patient communities during their deployment.

## Compliance with ethical standards

### *Disclosure of conflict of interest*

No conflict of interest to be disclosed.

## References

[1] Binns, R., & Hu, Z. (2023). Artificial Intelligence in Healthcare: Ethical and Security Implications. Journal of Healthcare Security, 12(2), 115-128.

[2] Chen, P., & Wang, H. (2020). Machine Learning in Medical Data Protection: Challenges and Opportunities. Journal of Medical Systems, 44(6), 985-997.

[3] Jones, R., & Brown, T. (2022). Human-AI Collaboration in Cybersecurity: A Case Study in Healthcare. Cybersecurity and Health Technology Review, 10(4), 78-92.

[4] Kumar, N., & Maan, A. (2020). AI in healthcare: A comprehensive review and directions for future research. International Journal of Healthcare Management, 13(3), 253-264.

[5] Patel, S., & Kumar, A. (2021). AI-Enabled Security Systems for Hospitals: A Review. Health Information Management Journal, 25(1), 33-47.

[6] Smith, L., & Zhang, K. (2021). Data Privacy Concerns in AI-Driven Healthcare Security. International Journal of Health Informatics, 32(3), 230-245.

[7] Thompson, K., & Mehta, S. (2019). Privacy risks of AI in healthcare: Legal and ethical implications. Health Information Management Journal, 48(4), 206-212.

[8] Zhang, Y., & Xie, J. (2021). Machine learning for cybersecurity in healthcare: A systematic review. Artificial Intelligence in Medicine, 110, 1-10.