Risk Management and Healthcare Policy

Dovepress
Taylor & Francis Group

Open Access Full Text Article

REVIEW

AI-Induced Cybersecurity Risks in Healthcare: A Narrative Review of Blockchain-Based Solutions Within a Clinical Risk Management Framework

Gianmarco Di Palma[1,2], Roberto Scendoni[3], Davide Ferorelli[4], Anna De Benedictis[1,5], Vittoradolfo Tambone[2], Francesco De Micco[1,2]

[1]Operative Research Unit of Clinical Affairs, Fondazione Policlinico Universitario Campus Bio-Medico, Rome, Italy; [2]Research Unit of Bioethics and Humanities, Department of Medicine and Surgery, Università Campus Bio-Medico di Roma, Rome, Italy; [3]Department of Law, Institute of Legal Medicine, University of Macerata, Macerata, Italy; [4]Interdisciplinary Department of Medicine (DIM), Section of Legal Medicine, University of Bari "aldo Moro", Bari, Italy; [5]Research Unit of Nursing Science, Department of Medicine and Surgery, Università Campus Bio-Medico di Roma, Rome, Italy

Correspondence: Gianmarco Di Palma, Operative Research Unit of Clinical Affairs, Fondazione Policlinico Universitario Campus Bio-Medico, Rome, Italy, Email g.dipalma@policlinicocampus.it

Background/Objectives: Artificial intelligence (AI) is revolutionizing the healthcare industry, improving diagnoses, treatments, and clinical processes. However, its integration poses significant cybersecurity risks, including data breaches, algorithmic opacity, and vulnerabilities in AI-controlled medical devices. This narrative review analyzes these threats and evaluates blockchain technology as a potential mitigation strategy within a Clinical Risk Management framework.

Methods: The literature search was conducted on PubMed, Scopus, and Web of Science, considering peer-reviewed publications from 2000 to January 2025. 1,204 articles were identified. Inclusion criteria included studies on cybersecurity risks in healthcare, blockchain applications in the clinical setting, and regulatory references (eg, General Data Protection Regulation). Conference abstracts, non-English articles, and non-peer-reviewed contributions were excluded. To ensure methodological rigor, the Scale for the Assessment of Narrative Review Articles criteria were applied.

Results: The thematic analysis highlighted recurring critical issues: difficulties with informed consent, unauthorized access to sensitive data, and systemic vulnerabilities in hospital digital infrastructures. Blockchain presents a promising solution thanks to its decentralization, immutability, and transparency. Integration with smart contracts enables dynamic consent management, secure data sharing, and real-time monitoring of medical devices. Permissioned networks improve traceability and regulatory compliance, while Layer 2 solutions and optimized consent protocols address scalability challenges.

Conclusion: Despite its potential, blockchain adoption faces obstacles: high costs, regulatory rigidity, and poor acceptance among healthcare professionals. The review highlights the need for pilot projects, interdisciplinary collaboration, and regulatory updates for effective integration. Combining AI and blockchain in Clinical Risk Management can transform clinical risk management from reactive to proactive, improving patient safety, data governance, and accountability.

Keywords: clinical risk management, artificial intelligence, blockchain, cybersecurity, healthcare, patient safety

Introduction

Definition and Origins of Clinical Risk Management

Clinical Risk Management (CRM) is a cornerstone of modern healthcare, focusing on the prevention of adverse events—unintentional and potentially avoidable harm—by addressing systemic complexities beyond individual errors.[1] It emphasizes an interdisciplinary approach that combines risk analysis, continuous training, and technological innovation to improve patient safety.[2] CRM promotes the use of advanced systems for error reporting and sentinel event detection, alongside standardized procedures and causal analysis techniques like Root Cause Analysis to identify and mitigate risks effectively.[3,4] The integration of technologies such as artificial intelligence

Received: 3 June 2025
Accepted: 13 September 2025
Published: 29 October 2025

and digital information systems enhances the ability to monitor, assess, and respond to clinical risks with greater speed and precision.[5] The conceptual foundation of CRM dates back to the 1970s and 1980s, focusing on reducing medical errors and their impact on patients, particularly critical incidents such as surgical and medication errors. These early efforts highlighted the need for systematic approaches to improve safety. The 1999 report "To Err is Human" by the Institute of Medicine revealed the widespread nature of avoidable harm, bringing patient safety to the forefront of healthcare priorities.[6] Initially, CRM efforts concentrated on identifying adverse events through error reporting systems and implementing standardized processes to reduce error frequency and severity, while improving communication among healthcare professionals.[7] By the early 21st century, CRM had evolved to incorporate systemic models that considered interactions between human factors, organizational processes, and technology. This marked a shift from reactive to proactive strategies aimed at anticipating and preventing risks. Over the past two decades, significant advancements have included the introduction of tools like Failure Mode, Effects and Criticality Analysis (FMECA) and Root Cause Analysis, which have improved the evaluation of clinical processes and identification of critical points. Additionally, the integration of Artificial Intelligence (AI) into CRM has enabled early identification of risks and errors, further enhancing patient safety measures.[8]

The Concept of Error in Healthcare

Clinical risk management (CRM) extends beyond patient safety by promoting a culture of learning and shared responsibility. A "no-blame culture" encourages addressing errors in a constructive rather than punitive manner, addressing systemic problems rather than individual errors.[9–11] This approach promotes transparency and collaboration, reducing underreporting and improving system safety.[12–14] Balancing non-punitiveness with accountability requires clear policies and leadership support.[15–18] Healthcare errors, which are inevitable in complex environments,[19] can be classified as slips (errors in execution), mistakes (errors in planning) and lapses (errors in memory).[20–23] James Reason highlights active errors, which have a direct impact on patients, and latent errors, embedded in systems and processes, which require systemic analysis to address root causes.[21,24]

Artificial Intelligence in Healthcare: Opportunities and Risks

Artificial Intelligence (AI) has become an essential tool for many healthcare professionals, with applications ranging from administrative management to advanced diagnostics. The healthcare sector has enthusiastically adopted this innovation, improving many aspects of patient care.[25] The European Union, aware of the potential risks, has chosen to contribute scientifically to ensure the protection of patients and their families, addressing the dangers associated with the use of intelligent systems in clinical practice.[26] AI offers significant advantages in hospitals, increasing the speed and accuracy of diagnoses.[27] Algorithms can process huge amounts of data quickly, facilitating the work of doctors and improving the quality of care. Intelligent systems support healthcare professionals, such as in real-time monitoring of vital parameters, with the ability to alert in case of significant variations, allowing timely interventions. Another application concerns the management of chronic diseases, with algorithms suggesting lifestyle changes or therapeutic adjustments for better control of the pathology.[28,29] In addition, AI facilitates access to care, allowing telemedicine and remote diagnosis, especially in disadvantaged areas.[30] However, despite the obvious advantages, the indiscriminate use of these systems can generate problems. Intelligent systems can be subject to "hallucinations", producing incorrect or inaccurate outputs, which requires careful supervision of the generated responses.[31] Real-life incidents show that generative AI poses unique cybersecurity risks in healthcare, including data leaks, algorithm manipulation, and deepfake misuse, highlighting the need to integrate targeted mitigation strategies into clinical risk management frameworks.[32] The introduction of AI in healthcare implies unconventional risk management and risk managers must develop new mitigation strategies to address emerging risks.[33] If algorithms operate in isolation, the risks are limited, but complex problems arise when intelligent systems must communicate with each other, managing complex tasks and exchanging data, with the risk of error propagation.[34] The integration of Artificial Intelligence (AI) in healthcare should be understood not only as a technological innovation, but as part of a broader paradigm shift known as Industry 4.0. This fourth industrial revolution is characterized by the convergence of cyber-physical systems, Internet of Things (IoT), cloud computing, and AI, enabling smart, autonomous, and interconnected environments across sectors—including healthcare.

As highlighted by Ersoy (2022), Industry 4.0 transforms production and service models by digitizing and integrating the entire value chain, improving agility, efficiency, and decision-making capabilities. In healthcare, this translates into enhanced diagnostic precision, predictive analytics, and real-time monitoring systems. AI, in this context, is not an isolated tool but a core component of a systemic transformation that affects clinical workflows, patient engagement, and data governance.[35] Moreover, Tehci & Ersoy emphasize that Industry 4.0 extends beyond manufacturing to include marketing and service delivery, promoting models such as customer-oriented and just-in-time production. These principles align with the evolution of healthcare toward patient-centered care, where AI-driven systems support personalized treatment, remote monitoring, and ethical data management. Incorporating the conceptual framework of Industry 4.0 allows for a more comprehensive understanding of AI's role in healthcare, particularly in relation to cybersecurity, interoperability, and clinical risk management.[36]

The emergence of AI and blockchain technology have introduced a new management dimension to the clinical governance landscape, while AI, with its ability to analyze large volumes of data and support clinical decisions, has the potential to implement quality of care, it also raises concerns about data security, to the transparency of algorithms and the protection of privacy. On the other hand, blockchain technology offers features such as decentralization, immutability, and transparency, which can help enhance cybersecurity and sensitive data management in healthcare. Therefore, the use of AI technologies, with the security profile guaranteed by blockchain, can lead to advanced risk management, ensuring regulatory compliance on the one hand and supporting the implementation of more robust controls within complex healthcare contexts on the other. Clinical Risk management is a solid basis for the integration of AI and blockchain in healthcare, the frameworks of this discipline, and particularly Enterprise Risk Management, can guide the implementation of these emerging technologies in a secure way, In this sense, blockchain presents itself as a risk mitigation strategy, capable of conferring security, Transparency and regulatory compliance in clinical data management and cybersecurity.[37–39] The traditional classification of clinical errors is based on consolidated categories, such as errors of commission, omission, diagnosis and execution, tools that have historically made it possible to identify the causes of adverse events and to propose corrective interventions, but the introduction of artificial intelligence systems has brought to light new types of errors that do not always lend themselves to being framed in traditional models, errors that can result from algorithmic biases, lack of transparency in predictive models, malfunctions of automated systems, or complex interactions between operators and technology, and therefore require a review and expansion of traditional categories to include technological and systemic factors. In this context, the "no-blame culture" of Clinical Risk Management, with its focus on seeing mistakes as opportunities for learning and improvement and not as opportunities to attribute individual blame, aligns perfectly with the challenges posed by AI-related incidents and cybersecurity risks, because it allows for the adoption of systems-based analysis, by holistically assessing the interactions between people, processes and technologies, identifying vulnerabilities and critical points and promoting solutions that strengthen the entire system, ensuring safety, reliability and sustainability of clinical practices even in the presence of complex technological tools.

The objective of this study is to examine the risks associated with cyber-attacks and personal data breaches arising from the integration of artificial intelligence in the healthcare sector and propose blockchain technology as a potential solution to mitigate these risks.

Materials and Methods

This is a narrative review aimed at analyzing the available literature on AI-induced cybersecurity risks in healthcare and the potential of blockchain technology as a possible solution to mitigate such risks. The bibliographic search was carried out by consulting the PubMed, Scopus and Web of Science databases, taking into consideration publications between the beginning of the 2000s and January 2025. This time interval was chosen because it represents the period in which the first clinical applications of artificial intelligence in healthcare appeared and, at the same time, the first critical issues related to IT security and data protection emerged. The time span allows us to analyze the evolution of the topic, from the initial stages of implementation to the most recent mitigation strategies based on advanced technologies such as blockchain.

The search string applied for the preparation of this review is as follows:

> (artificial intelligence' OR AI) AND (healthcare OR 'health care' OR medical OR clinical) AND (cybersecurity OR 'data privacy' OR 'information security' OR 'data breach' OR 'data protection') AND. (blockchain OR 'distributed ledger OR DLT OR GDPR)

This search was conducted on January 10, 2025, to ensure inclusion of the most recent and relevant studies. The screening of the articles was conducted by three reviewers with different levels of experience in the field of Clinical Risk Management: a junior researcher, a professional with intermediate experience and a senior expert.[40] The initial search yielded 1,204 results, which were then screened for duplicates. After removing duplicate entries, 902 unique records were retained for further analysis.

Articles addressing issues related to cybersecurity in healthcare, the applications of blockchain technology in the healthcare sector and regulatory frameworks were included in the study. On the other hand, works that focus exclusively on the use of blockchain in non-healthcare contexts were excluded, unless they offered useful guidance on security mechanisms applicable to healthcare. In addition, only articles published in peer-reviewed journals, systematic reviews, and high-impact conference proceedings were considered, while conference abstracts and publications written in languages other than English were excluded.

In order to ensure the methodological rigor of this narrative review, the SANRA (Scale for the Assessment of Narrative Review Articles) criteria were applied. SANRA is a validated six-item tool designed to assess the quality of narrative reviews, focusing on the following dimensions: justification of the article, clarity of stated objectives, appropriateness of literature sources, quality of data presentation, depth of scientific reasoning, and relevance to clinical practice.

Given the narrative nature of this study, SANRA was employed to support transparency and consistency in the synthesis of literature and the discussion of findings. The manuscript meets all six criteria, confirming its relevance, scientific robustness, and practical applicability in the context of healthcare risk management and cybersecurity.[41] Cybersecurity risks were summarized through a thematic analysis, which made it possible to identify recurring patterns in the literature, including the vulnerability of interconnected medical devices, issues related to informed consent and critical issues in the protection of sensitive data.

Results

Risks Related to Cybersecurity

Data Privacy and Informed Consent in AI Integration

The increasing use of artificial intelligence (AI) in healthcare, accelerated by the media wave, has raised concerns about data privacy, confidentiality and the protection of patients' rights.[42] These risks include the exposure and potential misuse of sensitive data, which could lead to violations of individual rights and non-medical uses of personal information.[43] Informed consent continues to represent an extremely delicate aspect in the context of the integration of artificial intelligence in healthcare, since it remains essential that the patient is placed in a position to understand sufficiently to be able to express an informed decision regarding the use of their personal data, however the extreme heterogeneity and complexity of AI systems makes this goal very difficult to achieve in concrete terms.

A significant example is represented by Large Language Models, which are increasingly used not only to provide decision-making support to the clinician but also to interact directly with the patient through forms of automated communication, but these are systems that work according to opaque logics, the so-called "black box" models, which generate answers on the basis of statistical correlations and not explicit or fully knowable rules, and this determines an objective difficulty in being able to explain in a clear and transparent way how these models work, what data are used and how a certain decision is reached, with an inevitable reduction in the degree of decision-making autonomy of the patient himself.[44]

A similar problem also concerns diagnostic and predictive models based on deep learning algorithms, now widely used in radiology, oncology and even genomics, which are based on the need to have enormous amounts of clinical data and on constant training, so it becomes evident that patient data can be reused according to the improvement of the algorithm itself, A circumstance that raises complex questions both from an ethical and legal point of view, as it becomes particularly difficult to explain these aspects in an exhaustive and understandable way, especially if we consider that the methods of processing and the objectives of use of data can change over time.[45]

A further critical issue is represented by the dynamic and adaptive character that many of these algorithms possess, as their performance does not remain static but evolves progressively according to the new data acquired, and this leads to the consequence that informed consent can no longer be understood as a single and conclusive act, but rather as a continuous process, which would require periodic updates in order to ensure that the patient maintains effective awareness of changes in the use of their data and the potential risks that arise from them.

Finally, the combination of generative AI systems with automated diagnostic tools introduces a further level of risk, which takes the form of the possibility of generating inaccurate content or inadequately verified interpretations, the phenomenon of the so-called "hallucinations" in LLMs is an example, with potentially significant repercussions on the therapeutic choices that follow.[46] Therefore, being able to guarantee the patient a sufficient understanding of these risks becomes extremely complex and makes it necessary to rethink consent models, which should be clearer, more flexible and supported by simplified and truly accessible forms of communication.[47]

Cybersecurity Risks in Healthcare Systems

The risk of cyber-attacks, as well as the unauthorized use of data, is a huge concern, with issues including privacy violations, identity theft, and the potential targeting of medical devices controlled by AI systems,[48] and in particular the use of interconnected medical devices, managed by smart systems, has introduced new vulnerabilities in the healthcare sector, devices such as pacemakers, insulin pumps and imaging equipment are particularly vulnerable to threats such as ransomware and denial of service (DoS) attacks, as their connectivity makes them susceptible to unauthorized access.[49] These risks can be grouped into three main categories, data access risks, device operation risks and system-level risks.

Unauthorized Access to Data

Among the risks of data access are unauthorized access to highly sensitive clinical information, privacy violations, identity theft, blocking of hospital IT systems as a result of ransomware that prevents access to patient data, a further example concerns unauthorized access to radiology reports through portable devices connected to the hospital network, which demonstrates how data compromise can have direct and immediate impacts on clinical management and treatment decisions, and yet another example can be the possibility that malicious actors, exploiting vulnerabilities in IT systems, access or extract electronic health records containing detailed information on diagnoses, ongoing drug treatments, medical history and personal data of patients, data that, once compromised, not only jeopardizes confidentiality but can be used to manipulate procedures, influence prescriptions or even sold on the illicit market of health information, demonstrating how data security is not just a technical issue, but can have direct and dramatic consequences on the lives and health of patients, And this applies to every type of healthcare facility, in fact, the lack of adequate controls or protocols can transform every single connected device, every single electronic record, into a potential vehicle of real, immediate risk, which can materialize in clinical, legal, ethical damage, showing how fragile the boundary between auxiliary technology and technology that can become dangerous is.[50–52]

Risks Related with the Operation of Devices

Risks related to the operation of devices, on the other hand, include unauthorized alteration of the operation of AI-controlled medical devices, changes in the dosages delivered by insulin pumps, variations in the signals transmitted by pacemakers, exposure of devices to ransomware and DoS that can compromise the continuity of care, an additional example in this category is unauthorized interference in automatic ventilation systems in intensive care, which could generate errors that are immediately dangerous for patients.

In this context, the first episode of an alleged cybermurder in Düsseldorf, Germany, in September 2020, is particularly alarming, marking a key moment in the history of cybersecurity and contemporary healthcare, the city's university hospital suffered a ransomware attack that prevented access to system data until a ransom was paid, as a result of the attack the hospital's computer systems were blocked making it impossible to access medical data and To manage new emergencies, among the patients who arrived, a woman in critical condition for heart problems was transferred to another

https://doi.org/10.2147/RMHP.S544523

hospital about 30 kilometers away, unfortunately the timing of the transfer was crucial and the patient died before receiving the necessary treatment, the German authorities opened an investigation for manslaughter since the link between the cyber attack and the death of the patient appeared clear.

This event marked a significant change, highlighting how vulnerabilities in IT systems can have direct and lethal impacts on people's lives, the Düsseldorf case raised important ethical and legal questions by emphasizing the urgency of greater vigilance on the security of IT systems in crucial areas such as healthcare, it also highlighted the need to adopt stronger cybersecurity measures and risk management strategies to protect the digital infrastructures from increasingly sophisticated threats, this dramatic episode represents not only a warning about the potential effects of cybercrime but also a reminder of the shared responsibility between health institutions, technology providers and governments, so that technology, while improving patient care, does not turn into an additional risk.[53–55]

System-Level Risks in Healthcare Settings

In addition to risks related to individual devices or access to data, another crucial aspect to consider are system-level risks, ie those vulnerabilities that emerge from the set of IT infrastructures of a hospital or healthcare organization and their interconnection, and these risks do not concern a single device or a single medical record, but the entire digital ecosystem, and precisely for this reason they can have pervasive, immediate, direct consequences on patient safety, because it only takes a weak point, an outdated server, an old workstation or obsolete software to compromise the entire system, and these are not abstract theories, but concrete, everyday scenarios, in which the lack of updates or adequate protocols opens the door to unauthorized intrusions, malware, ransomware and all kinds of cyber attacks.[56]

The main risks at the system level include, for example, the use of obsolete software and hardware, which no longer receive security updates, leaving the door open to intrusions, malware or ransomware, in practice even if all the latest devices are secure, an old generation server or workstation can become the weak point of the entire system, a practical example can be represented by a laboratory that uses a ten-year-old radiological archiving system, no longer supported by the manufacturer, a cyberattack that affects that system can block access to all patient images, making any urgent diagnosis or intervention impossible and turning what should be a fundamental aid into a dangerous obstacle.

Another risk concerns the lack of secure interoperability between different systems, because modern hospitals have hundreds of different applications, devices, platforms that need to communicate with each other: electronic health records, medication management systems, ICU monitoring devices, imaging systems, laboratories and so on, and if the interfaces are not designed with uniform security criteria, A vulnerability in a small component can propagate and compromise the entire network, a practical example can be a ventilator connected to a multi-parameter monitor, an attacker penetrating through the monitor can theoretically interfere with the automatic ventilation of patients, causing immediate risks to their lives and turning what should be an essential support into a potential tool for damage.

Other system-level risk factors include humans and available resources, staff who are not adequately trained in cybersecurity, weak passwords, improper use of portable devices or USB sticks, lack of sufficient staff or budget for updates and ongoing maintenance of IT systems, all of which increase the likelihood that a vulnerability will be exploited and that the impact of the attack will be very severe, as in the case of hospital system shutdowns during critical emergencies, or slowdowns in care that can turn into immediate damage for patients.

In summary, system-level risks show how healthcare security cannot be limited to protecting individual devices or data, but must address the entire network, digital infrastructures, considering the complexity, interconnection, interaction between people, software, devices, procedures and protocols, only in this way is it possible to reduce the probability of catastrophic incidents and really protect patients' health, Because technology, if not managed safely, can transform from an ally to a concrete danger, and these are not theoretical abstractions, but real, concrete risks, which every hospital, large or small, public or private, must face on a daily basis.[56,57]

The Role of Blockchain in Safeguarding Healthcare Data

Some studies highlight the need for ethical and transparent integration of AI technologies, in compliance with the European Union's General Data Protection Regulation (GDPR), to ensure that data is used safely and in line with regulations, reducing the risk of system failures or algorithmic bias.[58] Another significant risk concerns privacy violations related to the use of big data. Many healthcare facilities have already faced data protection issues during cyber-attacks; some of them have shared or stored sensitive healthcare data on publicly accessible servers, resulting in unauthorized exposure of the information. Although data used for research purposes must be anonymized, elements such as treatment dates, medical notes or personal information are not always removed.[59] This type of exposure represents a significant risk, especially with the use of AI, which requires large amounts of data to function effectively. Unauthorized access to healthcare data can also facilitate insurance fraud, highlighting the vulnerability of these infrastructures.[60] The growing interconnectivity of healthcare systems, driven by the adoption of advanced technologies and the integration of artificial intelligence, has inevitably exposed the sector to increasingly sophisticated and recurring cyber risks. For example, 624 cyber-attacks against hospitals and healthcare systems were recorded in 2023, more than double the 304 in 2022,[61] with devastating impacts on data security and operations of healthcare facilities. The effects of these breaches go beyond the simple loss of privacy, healthcare data, considered among the most sensitive and valuable information, are a primary target for cybercriminals who can use them for illicit purposes such as fraud, blackmail or sales on the dark web.[62] Such data leaks can also generate a sense of distrust towards healthcare institutions, pushing patients to forgo or delay treatments for fear of further breaches. As seen in the Dusseldorf case, cyber-attacks do not only impact privacy, but can have direct consequences on the operational efficiency of hospitals, when IT systems are rendered unusable by ransomware or other forms of malware, doctors and healthcare professionals are unable to access electronic medical records, diagnostic results and patient monitoring tools, this paralysis can delay diagnoses and treatments, compromising patient safety. But cyber-attacks also have high costs, healthcare facilities often have to pay ransoms to regain access to their data or invest significant resources to restore systems and improve cyber security.[63,64] These costs, combined with losses resulting from service disruption, can put the economic sustainability of healthcare organizations at risk, especially those already under financial pressure. To address this growing threat, it is essential that healthcare systems take a proactive approach to cyber security, including the implementation of advanced monitoring tools, continuous staff training and the creation of incident response plans; Indeed, only through a combination of cutting-edge technologies and integrated risk management will it be possible to protect not only data, but also the health and trust of patients.[65] Obtaining informed consent for the use of patient data is a topic of intense ethical debate. Patients typically consent to the use of data upon admission for therapeutic or administrative purposes, such as billing. However, when data is used for research or non-therapeutic purposes, separate consent is required. If data has been anonymized, the GDPR no longer applies, allowing healthcare facilities to use such data without further legal restrictions.[66] However, while anonymized data should theoretically be protected, there are concerns that combining this information with other sources could identify individuals.[67] Among the proposed solutions are strengthening the security of cloud storage systems and raising awareness among healthcare professionals about the risks associated with these technologies, in order to create a healthcare environment compatible with the safe and responsible use of AI. The growing complexity of the sector requires collaboration between researchers, policy makers and healthcare professionals to develop stricter regulations and more effective security mechanisms, preventing privacy violations and ensuring the ethical and safe use of AI in healthcare. Although GDPR does not apply to anonymized data, concerns remain about the possibility of re-identifying individuals through the combination of such data with other sources, a risk that requires further regulatory and technical interventions. Addressing the challenges of health data security and management requires innovative technological solutions, with blockchain emerging as one of the most promising (Figure 1). Table 1 provides a structured overview of AI-induced cybersecurity threats and their corresponding blockchain-based mitigation strategies (Table 1).

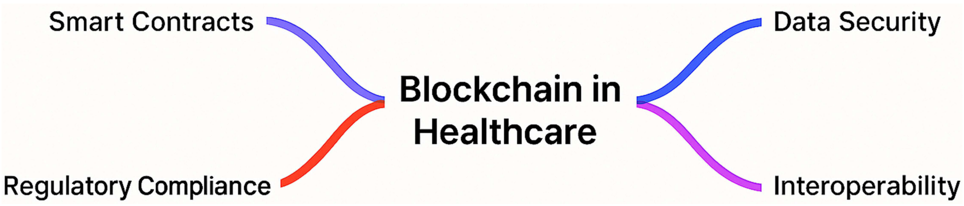

Figure 1 Main applications of blockchain in healthcare, with focus on data security, interoperability, smart contracts, and regulatory compliance.

Table 1 Mapping AI-Induced Cybersecurity Threats to Blockchain-Based Solutions

Cybersecurity Threat	Description	Blockchain-Based Solution
Data Privacy Violations	Unauthorized access, misuse, or sale of sensitive patient data	Immutable audit trails and permissioned access control ensure traceability and data integrity
Informed Consent Complexity	Difficulty in explaining AI systems and data usage to patients	Smart contracts enable dynamic, transparent consent management and version tracking
AI "Black Box" Decision-Making	Lack of transparency in algorithmic outputs	Blockchain logs algorithmic decisions, enabling retrospective analysis and accountability
Ransomware Attacks on Hospital Systems	Blocking access to critical medical data and systems	Decentralized data storage and distributed consensus reduce single points of failure
Manipulation of AI-Controlled Medical Devices	Unauthorized changes in device behavior (eg, insulin pumps, ventilators)	Real-time monitoring via smart contracts and immutable logs of device activity
System-Level Vulnerabilities	Obsolete software, weak interoperability, and human error	Blockchain ensures secure interoperability and enforces protocol compliance across systems
Insurance Fraud and Data Re-identification	Use of anonymized data to identify individuals or commit fraud	Cryptographic hashing and pseudonymization reduce re-identification risks
Lack of Accountability in Clinical Operations	Difficulty in attributing responsibility for clinical decisions	Blockchain links actions to authorized nodes, enabling precise attribution and auditability

Solutions and Innovations

The Blockchain Technology

Blockchain represents an unalterable register of transactions or data verified and certified in the presence of a distributed control.[68] The two pillars of this technology are accountability, or the possibility of a rigid control, and data protection, which can include anonymization or pseudonymization. Blockchain was born in the field of cryptocurrencies but its application potential extends to many sectors, including healthcare. It represents in all respects a distributed digital register, subject to encryption and based on peer-to-peer communication in which new data can be inserted, but without deleting or overwriting them.[69] In any case, such changes can only be made through the shared consensus between the participants in the register itself, the network is also able to resist any external attacks.[70] So the advantage of this system, in addition to high security, is to guarantee communication and sharing by authorized participants without the need for central control.[71]

The fundamental constituents of a blockchain are the node, or main participant of the blockchain, the block, or essential unit that makes up the chain in which the registration of the acquired data takes place, the ledger, which represents the shared register on which the information is accumulated, the transaction, that is the exchange of data between the nodes, which will have to verify their nature and insert them into the block once validated. The hash functions, which mathematically encode communication into alphanumeric codes, represent the cryptographic connection system between the blocks, a block is defined as valid when its hash is lower than a specific value defined as "target".[72,73] In the healthcare sector, blockchain also represents a distributed ledger that can guarantee the security, transparency and integrity of clinical data.[74,75] Healthcare blockchains are generally "permissioned", meaning access is limited to authorized users only. Nodes are hospitals, clinics, laboratories, doctors, patients and regulatory bodies. The healthcare transaction occurs by adding the results of a diagnostic test to the medical record or electronic medical record, the hospital (authorized node) creates a transaction that includes the healthcare data, digitally signing it and the patient can be involved at various levels to authorize access or even just the modification of the data. At this point, the transaction is hashed to generate a unique alphanumeric identifier, the Digest, which guarantees the integrity and authenticity of the transaction itself, the sending node proceeds to digitally sign the transaction with its private key. The healthcare transaction is distributed to the nodes of the network where it is verified against the predefined rules of the blockchain. In the validation and recording phase, nodes validate the transaction and enter it into a block, at which point the health data is recorded and becomes accessible to all authorized nodes.[76–81] Integration with smart contracts further expands the potential of blockchain. These self-executing programs enable the automation of complex processes, such as secure data sharing between entities, automatic payment of insurance claims, or management of access authorizations.[82–84] By automating these procedures, management times are reduced and errors or breaches are minimized, improving overall operational efficiency.

In terms of interoperability, the decentralized architecture of blockchain enables seamless connection between different healthcare systems. Solutions such as private or hybrid blockchains are particularly suited to this sector, offering an optimal balance between security, access control and scalability. These systems can facilitate distributed management of electronic health records (EHR), ensuring secure and continuous access to data between hospitals, providers and patients. However, the challenge of scalability remains, which is crucial for large-scale implementation in healthcare systems. Emerging technologies such as sharding or layer 2 solutions (eg, Lightning Network) are paving the way for greater transactional capacity without sacrificing security or decentralization.[85] Furthermore, regulatory compliance requires a joint effort by governments, the technology industry and healthcare providers to define clear standards for interoperability and security. When we refer about Layer 2 we mean all those solutions that are used to move a large number of transactions outside the main layer, therefore no longer all on-chain and from time to time they are brought back to the chain with anchors, ie proofs, and this is done with mechanisms such as state channels or rollups. So, for example, if there is a laboratory that continuously sends data to an electronic medical record, it is not possible to write every result directly to the blockchain because, therefore, through an L2 channel, hundreds of updates can be made in real time and occasionally writing a hash or a test packet on the chain so as to guarantee auditability but without blocking the network. As far as Lightning Networks are concerned, these were born in the Bitcoin world but the concept also applies in healthcare, ie we are talking about a network of payment channels where it is possible to make very fast micro-payments at reduced costs without writing on the chain every time, in healthcare the principle can be applied for example to IoMT devices that transmit data and if there was a micro-reimbursement model for each telemetry stream then through the channels there is it could do everything in real time and only closing infrequently on the main layer, therefore, less friction and more scalability. Therefore, blockchain represents a significant technological advancement in healthcare data management. Its ability to ensure integrity, transparency and security, combined with advanced tools such as smart contracts and innovative consensus protocols, makes it a strategic solution to address the challenges of healthcare digitalization. Consensus protocols are those rules that are used by nodes to agree on what the true state of the registry is, in healthcare, considering the tightness of the timing, permissioned systems are preferred that use, for example, Byzantine Fault Tolerance, a property of a system that allows it to continue to function correctly even if some of the participating nodes behave arbitrarily or maliciously (the so-called "Byzantine faults") or Raft, An easy-to-control consensus algorithm. For example, Hyperledger Fabric uses Raft for the ordering service so as to achieve a fast finality, high throughput and control over who participates ie payer hospitals and so on. In some decentralized medical record systems, the Tendermint is used, which is Byzantine Fault Tolerance and has low latency and deterministic purpose, fundamental characteristics for clinical flows.

Blockchain in Clinical Risk Management Processes

The increasing digitalization of healthcare systems has made Clinical Risk Management processes, ie the management of clinical risks within hospitals and healthcare facilities, increasingly vulnerable to issues related to data security, regulatory compliance and the reliability of clinical information. In this scenario, the adoption of blockchain technology is configured as an advanced and powerful tool to mitigate risks, improve incident tracking and ensure the transparency, auditability and immutability of audit trails.[86]

Clinical Governance

The blockchain, thanks to its decentralized, encrypted and immutable structure, allows every clinical or operational event to be recorded in a secure and transparent way, from the patient's entry to the administration of the most complex treatments. This permanent record creates a digital audit trail that cannot be changed retroactively, making reliable information immediately available for clinical risk assessment. In practice, it makes it possible to continuously and systematically monitor the use of connected medical devices, drug administrations, diagnostic procedures and any health intervention, promptly identifying anomalies, deviations from protocols or risk situations, and allowing the healthcare team to activate preventive interventions in real time, before negative effects can be caused on patients trails.[86]

Adverse Event Tracking

Smart contracts, real self-executable programs integrated into the blockchain, automate and secure risk management processes and clinical incidents. For example, a smart contract can automatically record an error in the administration of a drug, immediately generate an alert to the responsible personnel, initiate review and correction protocols, and ensure that the event is recorded in an immutable and verifiable log. All this drastically reduces the risk of human error, accelerates the response to adverse events and allows the construction of a complete and permanent database, essential for retrospective analyses, to identify recurring patterns and to continuously optimize Clinical Risk Management processes.[87]

Audit Trail and Data Control

Permissioned networks, ie blockchain networks in which access is strictly limited to authorized nodes, make it possible to precisely establish who can view or modify clinical information. This is crucial to ensure compliance with regulations such as GDPR and to protect patient data from unauthorized access or manipulation. Each transaction or change is permanently recorded and associated with the unique identifiers of authorized nodes, thus creating a transparent, secure and auditable audit trail. In this way, every clinical decision, every intervention and every data update can be reconstructed with pinpoint accuracy, allowing risk managers to identify operational vulnerabilities, critical situations and emerging trends.[88]

Operational Implementations and Use Cases

In a hospital context, a permissioned blockchain can automatically record all drug administrations, surgeries and diagnostic procedures, generating an immutable register accessible only to authorized operators, a useful tool both for the assessment of clinical risks and for internal audits, regulatory checks or regulatory inspections. In the case of connected medical devices, such as insulin pumps or automatic ventilators, smart contracts can constantly monitor critical parameters, generating real-time alerts if anomalies or unauthorized changes are detected. This approach not only protects patients from potential errors or malfunctions, but also provides valuable data for predictive analysis, risk modeling, and the definition of more effective and evidence-based Clinical Risk Management protocols. The integration of blockchain into Clinical Risk Management processes makes it possible to transform hospital digital infrastructures from potential points of vulnerability into active clinical governance tools, tools capable of monitoring, tracking and verifying each process in real time. The combination of smart contracts and permissioned networks improves security, transparency, traceability and regulatory compliance, reduces errors, accelerates incident response and contributes to more effective, reliable and evidence-based clinical risk management. In this way, technology becomes not only a data protection tool, but a real strategic support to ensure patient safety and the overall quality of care provided.

Although many medical devices are integrated into IoT ecosystems today, not all of them require a continuous connection to the network or the cloud, and in this context, edge computing is configured as an effective architectural solution to address the security and latency challenges typical of IoT. Edge computing allows data to be processed directly on or in its immediate vicinity, reducing reliance on the core network, minimizing latency, and limiting exposure to potential external threats. A concrete example is represented by the multi-parameter monitors used in intensive care, which detect vital parameters such as blood pressure, oxygen saturation, heart rate in real time; In an edge architecture, this data can be processed locally to generate immediate clinical alerts (such as tachycardia or hypoxia), without having to wait for transmission to the cloud. In addition, edge computing makes it possible to implement predictive models directly on the device, for example to anticipate the risk of clinical deterioration, improving the timeliness of intervention. Looking ahead, the integration between blockchain and edge computing could outline a hybrid model: blockchain would ensure the traceability and integrity of clinical data, while edge computing would ensure its decentralized and secure processing, with advantages in terms of operational efficiency, resilience and privacy protection.[89–91]

Pilot Applications of Blockchain for Complex and Scalable Healthcare Systems

The growing focus on the digitization of healthcare systems has led to the experimentation of different blockchain platforms, all aimed at ensuring greater security, transparency and efficient management of clinical data, addressing some of the main challenges related to the scalability of distributed systems. It is important to underline that these initiatives, although promising and innovative, still largely remain experimental and have not been fully implemented on a large scale, making the field extremely dynamic and constantly evolving. Among these, SCALHEALTH has explored the integration of Internet of Medical Things (IoMT) devices by leveraging Hyperledger Fabric, decentralized storage and optimized consensus mechanisms to manage large volumes of clinical data in real time; the network, in this solution, is organized on two separate blockchains, one dedicated to health data and the other to financial transactions, with the aim of improving both efficiency and overall security of the system.[92]

Similarly, MedRec, developed by MIT, aims to manage distributed electronic health records through the use of smart contracts and modular structures, allowing controlled and secure access to patient data and ensuring network scalability even in hospitals with large volumes of users, thus addressing the complexities of multi-hospital contexts.[93]

Another significant platform is Patientory, which uses a permissioned private blockchain to ensure the security of clinical data; the modular architecture adopted allows new nodes to be added and growing data flows to be managed without compromising stability and performance, offering a concrete example of how to address scalability problems in complex and interconnected healthcare contexts.[94] Finally, MediLedger focuses on traceability and compliance in the pharmaceutical supply chain: through smart contracts and the use of off-chain data, it is able to handle large volumes of transactions and scale across multiple dimensions, including the number of participants, the volume of transactions and the type of products, showing how blockchain can support complex and interconnected systems in a secure and controlled manner.[95]

Overall, these experiences show how, even in the experimental phase, blockchain is trying to balance security, transparency and the ability to manage large amounts of clinical data; The adoption of modular architectures, permissioned networks and optimized consensus mechanisms represents a first concrete step towards the construction of more secure, resilient and efficient digital health infrastructures, capable of effectively addressing the scalability challenges related to the increasing complexity of modern clinical systems.[96,97]

Discussion

Integration Between AI and Blockchain: Opportunities and Security Challenges

The findings from this review confirm that the central theme is not simply identifying the potential of AI and blockchain in healthcare, but also fully understanding how these technologies interact with each other and the real implications for data security, clinical risk management, and operational sustainability. While artificial intelligence has introduced undeniable advantages in terms of predictive capacity, diagnostic automation, and decision support, it has also opened up vulnerability scenarios that no longer fit into traditional categories. For example, the continuous adaptability of algorithms that modify behavior based on data, thus shifting the very concept of informed consent from a static act to a dynamic process. Then there are the risks deriving from the presence of interconnected IoMT devices that can become targets for ransomware and DoS attacks with immediate impacts on patient safety.

All this, not to mention the systemic risks associated with obsolete or unevenly protected hospital infrastructure, where a single flaw can compromise the entire digital ecosystem with dramatic consequences. In this context, blockchain presents itself as a technology that, at least in theory, appears to offer solid solutions because it introduces immutability, traceability, and distributed consensus mechanisms that guarantee integrity and transparency, as well as the possibility of integrating smart contracts to automate authorizations and secure sharing of clinical data. However, all this works in models and pilot projects, while the reality of a national healthcare system with millions of transactions per day requires a serious approach to scalability and interoperability. It’s unthinkable to write every clinical event on the main chain without saturating the system. Solutions like Layer 2, which allow large transaction volumes to be moved off the main chain with periodic on-chain anchors, or the use of models derived from the Lightning Network, become indispensable. Although originally developed for Bitcoin micropayments, it demonstrates how payment channels can be adapted for

https://doi.org/10.2147/RMHP.S544523

microtransactions linked to the IoMT. Reducing latency and costs and ensuring operational continuity, while on the consensus front, energy-intensive and slow algorithms like Proof-of-Work cannot be used, but permissioned protocols like Raft or BFT are needed to ensure rapid finality, high throughput, and resilience, as demonstrated by the experience of Hyperledger Fabric with Raft or Tendermint in decentralized EHR systems. If the consensus algorithm slows down the network, clinical security is jeopardized rather than improved. Therefore, the key message emerging from this analysis is that blockchain can truly be a mitigation strategy for the risks introduced by AI, but only if architectures are designed based on privacy-by-design, with scalable models and protocols suited to clinical flows, accompanied by regulatory updates and significant infrastructure investments. Without these, the promise of security risks remaining confined to white papers and not becoming a concrete reality in hospital settings.

Integration of AI and Blockchain: Potential and Regulatory Challenges

The use of innovative technologies such as AI and blockchain in healthcare represents a radical change in healthcare paradigms to improve care and operational efficiency. The integration of these two technologies offers enormous potential to improve the healthcare sector, in particular, AI with its ability to analyze large amounts of data and identify complex correlative patterns, can improve the functionality of blockchain. For example, machine learning algorithms can be used to optimize smart contracts, computer programs that are automatically executed when certain conditions are met, encoded and recorded on a blockchain. At the same time, blockchain technology can reduce the risks related to the use of AI by ensuring a safer and more transparent environment in which to operate, ensuring data integrity and traceability of algorithmic decisions. It is clear that the technical complexity of combining these two technologies is considerable, requiring high interdisciplinary skills.

However, integrating these technologies means being ready to face significant challenges, among which are risks related to privacy, cybersecurity and regulatory compliance issues. In particular, the GDPR represents a global benchmark in terms of regulations related to the protection of personal data. However, the rapid technological advancement, and at the same time the risks that derive from it, imposes the need to broaden the scope of the regulation itself. For example, the GDPR does not fully consider the complexities related to decentralized data management, a significant characteristic of blockchain. Another problem is related to the fact that in accordance with the European Regulation, personal data should be processed transparently, guaranteeing users the right to rectification and erasure of the same, these fundamental principles clash with the concept of immutability of blockchain registers in which each modification is recorded as a new block without erasing previous information.

Privacy-by-Design, GDPR Gaps and Implementation Barriers

This creates a considerable limit in the application of the GDPR which, therefore, requires a regulatory update to include specific guidelines that regulate the use of blockchain in the healthcare sector while ensuring compliance with the principle of privacy by design. This concept refers to an approach to personal data protection that integrates privacy protection as a priority from the early design stages, rather than treating it as an afterthought. The use of a blockchain is well integrated into this approach, in fact the cornerstones of the privacy-by-design system are proactivity, automated setting of the maximum level of privacy protection, integration of the data protection concept into the design plan, comprehensive functionality, avoiding unnecessary compromises, end-to-end security, ie data protection throughout the lifecycle, visibility and transparency of data processing practices, and centrality of user interests.

Another major shortcoming of the GDPR is that it does not comprehensively address the problem of re-identification of anonymous data through combination with other sources, also known as data triangulation, a growing risk in the era of big data where more and more and artificial intelligence, where multiple information can be combined to trace the identity of a subject. Another limitation of the GDPR is its difficult application in technologically advanced contexts such as hospitals, where data management is often complex and involves a variety of actors. In this sense, the use of technologies such as blockchain requires significant resources, including advanced IT facilities, a specific training plan for healthcare and technical staff, and dedicated cybersecurity teams.

At the moment, the GDPR does not provide for the existence of incentives or operational guidelines that facilitate this type of compliance through an investment plan, thus leaving healthcare organizations to manage these challenges on their own. However, even in the case of regulatory compliance, GDPR compliance for healthcare facilities could be expensive. This could obviously favor the phenomenon of the digital divide, favoring larger healthcare companies, which can afford to implement advanced technological solutions, to the detriment of smaller ones, which instead risk being excluded from the benefits of innovation. Finally, the Regulation, in its current state, is not flexible enough to address emerging situations such as cyber homicide or insurance fraud. This is the case of the ransomware attack against the University Hospital of Düsseldorf in 2020, following which, due to the operational paralysis of the IT system, a woman died and was forced to be diverted in an emergency situation to another distant healthcare facility.

In fact, the GDPR does not provide specific measures for the protection of interconnected medical devices, which in the age of AI represent a highly critical point for patient safety. However, there remain a number of challenges that the healthcare system will have to address before it can systematically integrate Blockchain. First of all, one of the fundamental issues is related to the high implementation costs, since the adoption of these technologies requires significant investments in IT infrastructure, technical expertise and staff training. At first, smaller healthcare facilities may suffer the effects of this expense, however, in the long term this would be offset by a reduction in the possible costs related to data breaches and cyber-attacks.[98,99]

Furthermore, another issue is represented by the scalability problems in a context with a very high data volume such as that of the national healthcare system. As already seen, possible solutions could be represented by sharding, which divides the work on multiple nodes, or by layer 2 technologies that could improve transactions. Any interoperability problems between blockchain and the healthcare system could be overcome thanks to a close collaboration between technology developers and healthcare professionals. Finally, the last obstacle that should not be underestimated would be the acceptance of this new technology by healthcare professionals and patients. In this sense, continuous training and awareness programs would be necessary.

Implications for Clinical Risk Management and Conditions for Adoption

One aspect that is clear is that the integration of AI and blockchain is not limited to being a technological option, but becomes a structural issue for Clinical Risk Management, because CRM is no longer simply the system for detecting and managing adverse events, but must transform into a dynamic framework capable of intercepting IT vulnerabilities and algorithmic criticalities. In this sense, blockchain, with its ability to generate immutable audit trails, can become the tool that allows us to overcome one of the historical weaknesses of risk management systems: the difficulty of achieving complete and unalterable traceability of clinical operations and access authorizations. This point is not only technical but also ethical and legal, because when it comes to professional responsibility and accountability, having distributed and verifiable registers means being able to attribute every action to the authorized node without ambiguity, and this radically changes the way we conduct audits and root-cause analysis, reducing the margin of hidden errors or under-reporting.

At the same time, it's important to consider that the effectiveness of this approach depends on the stakeholders' perception and role. Patients demand transparency and control over their data. They want to know not only who uses it but also for what purposes, which requires dynamic and understandable consent dashboards. Clinicians, for their part, cannot be burdened with additional complexity, and therefore solutions must be seamlessly integrated into operational flows. This requires specific training, and it's important to understand that cybersecurity is not an IT issue but a component of patient safety. Then there's IT, which must design secure permissioned networks, implement Raft or BFT protocols, and ensure interoperability between legacy systems and new platforms. Management must evaluate costs and ROI, because blockchain infrastructures require significant investments and, without public incentives, risk widening the gap between large and small healthcare facilities. Finally, regulators must update the regulatory framework, overcoming conflicts between immutability and the right to be forgotten, between decentralization and the obligation to rectify, and introducing clear guidelines on how to apply the privacy-by-design principle. In distributed networks that never delete data but evolve it through versions.

From an operational perspective, the results of this review indicate three main gaps: the first concerns scalability, because without L2 solutions, sharding, and off-chain, blockchain cannot handle the volumes of healthcare transactions; the second is compliance, because the current GDPR was not designed for a distributed world, generating application uncertainty; the third is socio-technical acceptance, because even the best architecture fails if doctors and patients do not

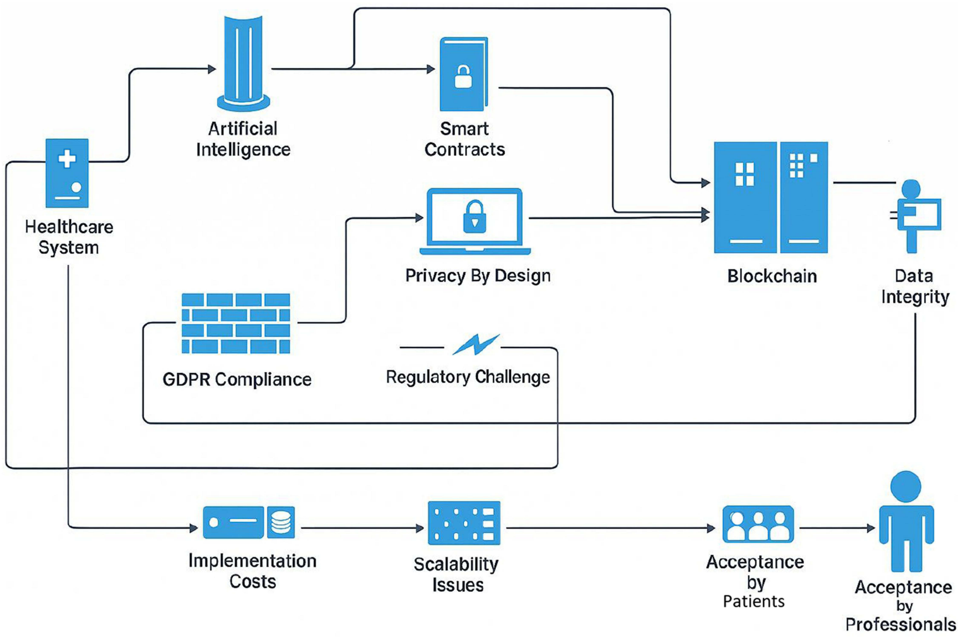

Figure 2 Interactions between AI, blockchain and the healthcare system, highlighting benefits (security and data traceability) and challenges (cost, compliance and professional acceptance).

adopt it. This requires an integrated approach that combines technology, training, governance, and incentives. In other words, it's not enough to say that blockchain and AI can coexist to increase security; we must create the conditions for this to happen in practice. This means adopting modular, interoperable, and economically sustainable models, and above all, governed by clear and shared policies. Without governance, technology remains merely a theoretical exercise (Figure 2).

Conclusion

Final Considerations

The integration of advanced technology such as Blockchain in the healthcare sector is one of the epochal challenges that will arise in the near future. However, the increasingly widespread use of intelligent systems in the healthcare sector requires the use of futuristic technologies in order to prevent new emerging risks. In any case, to strategically address these challenges, it is necessary to maximize their positive impact. The use of blockchain can ensure security, transparency and traceability of healthcare data, however, it seems necessary to comply with operational recommendations such as providing economic incentives to finance its use, an update of the regulatory framework, specifically the GDPR, and the promotion of a training program for healthcare and non-healthcare personnel. From a future-oriented perspective, it is essential for the healthcare sector to adopt a proactive, ethical and patient-centric approach, the introduction of technologies such as blockchain can help ensure a safer and more resilient healthcare system. The success of this process will depend on the ability to integrate emerging technologies into an increasingly systemic and dynamic risk management framework. A central element that emerges from this review is the concrete contribution that can derive from the integration between blockchain and artificial intelligence to the strengthening of Clinical Risk Management practices. In this context, the integration between blockchain and artificial intelligence does not only represent a technological opportunity, but a structural evolution of Clinical Risk Management, in particular, blockchain with its ability to generate immutable audit trails, automate processes through smart contracts and ensure the traceability of algorithmic decisions, makes it possible to address historical CRM critical issues such as data fragmentation and the difficulty in attributing responsibility. These tools, when applied systemically, enable proactive management of clinical risks, improve transparency and professional accountability, and strengthen patient safety in digitized settings. In this scenario, CRM is no longer just a reactive system but evolves into a dynamic and predictive framework, capable of intercepting technological and behavioral vulnerabilities in real time. To translate this potential into concrete applications, it is necessary to promote pilot tests in hospital environments, in the light of the evidence that has emerged, it seems strategic to promote the launch of blockchain-based pilot projects within hospital contexts, projects that should focus on areas with high clinical impact such as the secure management of health data, the monitoring of IoMT devices, the automation of adverse event reporting processes and interoperability with legacy systems. It is essential that these trials are always accompanied by multidisciplinary assessments, bringing together clinical, technical, ethical and legal expertise, and by public incentives aimed at supporting adoption, especially in smaller facilities. Only through controlled tests will it be possible to verify the effectiveness, sustainability and acceptability of these technologies in the real context, transforming what today remains a theoretical promise into a real operational value for the health system.

Limitations of the Study and Future Prospects

The present work has been developed as a narrative revision because this methodological choice has proved to be the most consistent with the complex and constantly evolving nature of the topic addressed. In fact, this approach has been particularly suitable for dealing with topics that are not yet consolidated and that involve multiple disciplinary areas, as is the case with the interaction between artificial intelligence, blockchain and clinical risk management. To maintain an adequate level of methodological rigor, the SANRA scale was used, which serves to assess the quality of narrative reviews on the basis of six fundamental parameters which are the justification of the theme, the clarity of the objectives, the description of the bibliographic sources, the presentation of the data, the scientific discussion and the clinical relevance. The methodology has been described in such a way as to make clear the application of these criteria.

The main limitation of the study is related to the fact that the technologies under analysis, in particular artificial intelligence and blockchain, evolve at an extremely high speed. In fact, innovations in this field proceed so rapidly that some sources and even some solutions that have been discussed here have been outdated in a short time. For this reason, it is essential to constantly update both the literature and the proposed mitigation strategies, so as to ensure that the contents maintain real practical applicability in the clinical setting.

On the basis of the evidence that has emerged, it seems appropriate that future studies focus on some lines of in-depth study that can consolidate and strengthen the integration of emerging technologies in the health context. First of all, it would be useful to systematically compare the effectiveness of the different blockchain solutions that have already been tested in the clinical field to understand which of these are the most suitable to ensure security, interoperability and sustainability. Another point that deserves attention is the impact of artificial intelligence on the quality of clinical decisions and also on the informed consent process because the growing autonomy of algorithms requires ethical and methodological reflection on how to ensure transparency and comprehensibility towards patients.

At the same time, it will be necessary to think of regulatory models that are more flexible and more suitable for the decentralized management of health data, overcoming current rigidities and arriving at a regulation that truly accompanies technological innovation. Technological risk assessment also requires the use of interdisciplinary frameworks that combine clinical, IT, legal and ethical skills, in order to address new vulnerabilities with a systemic approach. Finally, an aspect that is often underestimated but which is of fundamental importance concerns the perception and acceptance of these technologies by professionals and patients. Understanding what the resistances, expectations and training needs are will be essential to encourage an adoption that is conscious and shared. All these lines of research can contribute to building a safer and more sustainable healthcare ecosystem, capable of integrating technological innovations while always maintaining an ethical vision that puts the person at the center.

Acknowledgments

Thanks to the National Ph.D. in Artificial Intelligence, XL cycle, a course on Health and Life Sciences, organized by University Campus Bio-Medico of Rome, to which Gianmarco Di Palma is enrolled as a Ph.D. student.

Disclosure

The authors report no conflicts of interest in this work.

References

1. Vincent C, Neale G, Woloshynowych M. Adverse events in British hospitals: preliminary retrospective record review. *BMJ*. 2001;322 (7285):517–519.PMID: 11230064; PMCID: PMC26554. doi:10.1136/bmj.322.7285.517
2. Reason J. (1990). Human error. Cambridge University Press.
3. Brunsveld-Reinders AH, Arbous MS, De Vos R, De Jonge E. Incident and error reporting systems in intensive care: a systematic review of the literature. *Int J Qual Health Care*. 2016;28(1):2–13.Epub 2015 Dec 10. PMID: 26660441. doi:10.1093/intqhc/mzv100
4. Shah F, Falconer EA, Cimiotti JP. Does root cause analysis improve patient safety? a systematic review at the department of veterans affairs. *Qual Manag Health Care*. 2022;31(4):231–241.Epub 2022 Feb 14. PMID: 35170581. doi:10.1097/QMH.0000000000000344
5. De Micco F, Di Palma G, Ferorelli D, et al. Artificial intelligence in healthcare: transforming patient safety with intelligent systems-A systematic review. *Front Med*.
6. Institute of Medicine (US).*Committee on Quality of Health Care in America. To Err Is Human: Building a Safer Health System*.Kohn LT, Corrigan JM, Donaldson MS: editors.;Washington (DC);National Academies Press (US).2000.PMID: 25077248
7. Verman S, Anjankar A. A narrative review of adverse event detection, monitoring, and prevention in indian hospitals. *Cureus*. 2022;14(9):e29162. PMID: 36258971; PMCID: PMC9564564. doi:10.7759/cureus.29162
8. Shaqdan K, Aran S, Daftari Besheli L, Abujudeh H. Root-cause analysis and health failure mode and effect analysis: two leading techniques in health care quality assessment. *J Am Coll Radiol*. 2014;11(6):572–579.Epub 2014 Feb 4. PMID: 24507549. doi:10.1016/j.jacr.2013.10.024
9. Khatri N, Brown GD, Hicks LL. From a blame culture to a just culture in health care. *Health Care Manage Rev*. 2009;34(4):312–322.PMID: 19858916. doi:10.1097/HMR.0b013e3181a3b709
10. Parker J, Davies B. No blame no gain? from a no blame culture to a responsibility culture in medicine. *J Appl Philos*. 2020;37(4):646–660.PMID: 33362325; PMCID: PMC7750815. doi:10.1111/japp.12433
11. Rodziewicz TL, Houseman B, Vaqar S, Hipskind JE.Medical Error Reduction and Prevention.2024.(FL);StatPearls Publishing;Jan.PMID: 29763131
12. Wu AW. Medical error: the second victim. The doctor who makes the mistake needs help too. *BMJ*. 2000;320(7237):726–727.PMID: 10720336; PMCID: PMC1117748. doi:10.1136/bmj.320.7237.726
13. White AA, Gallagher TH. Medical error and disclosure. *Handb Clin Neurol*. 2013;118:107–117. PMID: 24182370. doi:10.1016/B978-0-444-53501-6.00008-1
14. Puch EA, Nowak-Jaroszyk M, Swora-Cwynar E. Błąd medyczny w teorii i praktyce – przegląd najważniejszych zagadnień [Medical error in theory and practice - a review of the most important issues]. *Med Pr*. 2020;71(5):613–630.Epub 2020 Sep 15. PMID: 32969411. doi:10.13075/mp.5893.00988
15. Gu X, Deng M. Medical error disclosure: developing evidence-based guidelines for Chinese hospitals. *J Patient Saf*. 2021;17(8):e738–e744.PMID: 32740131. doi:10.1097/PTS.0000000000000760
16. Edrees H, Federico F. Supporting clinicians after medical error. *BMJ*. 2015;350:h1982. PMID: 25877670. doi:10.1136/bmj.h1982
17. Grober ED, Bohnen JM. Defining medical error. *Can J Surg*. 2005;48(1):39–44. PMID: 15757035; PMCID: PMC3211566.
18. Kachalia A, Hemmelgarn C, Gallagher TH. Communication after medical error: the need to measure the patient experience. *Jt Comm J Qual Patient Saf*. 2024;50(9):618–619.Epub 2024 Jun 28. PMID: 39013757. doi:10.1016/j.jcjq.2024.06.006
19. Ahsani-Estahbanati E, Sergeevich Gordeev V, Doshmangir L. Interventions to reduce the incidence of medical error and its financial burden in health care systems: a systematic review of systematic reviews. *Front Med*. 2022;9:875426. PMID: 35966854; PMCID: PMC9363709. doi:10.3389/fmed.2022.875426
20. Galante N, Cotroneo R, Furci D, Lodetti G, Casali MB. Applications of artificial intelligence in forensic sciences: current potential benefits, limitations and perspectives. *Int J Legal Med*. 2023;137(2):445–458.Epub **2022** Dec 12. PMID: 36507961. doi:10.1007/s00414-022-02928-5
21. Reason J. Understanding adverse events: human factors. *Qual Health Care*. 1995;4(2):80–89.PMID: 10151618; PMCID: PMC1055294. doi:10.1136/qshc.4.2.80
22. Aronson JK. Medication errors: definitions and classification. *Br J Clin Pharmacol*. 2009;67(6):599–604.PMID: 19594526; PMCID: PMC2723196. doi:10.1111/j.1365-2125.2009.03415.x
23. Ribeiro Gda S, Silva RC, Ferreira Mde A, Silva GR. Slips, lapses and mistakes in the use of equipment by nurses in an intensive care unit. *Rev Esc Enferm USP*. 2016;50(3):419–426.PMID: 27556712. doi:10.1590/S0080-623420160000400007
24. Thomas B, Paudyal V, MacLure K, et al. Medication errors in hospitals in the Middle East: a systematic review of prevalence, nature, severity and contributory factors. *Eur J Clin Pharmacol*. 2019;75(9):1269–1282.Epub 2019 May 24. PMID: 31127338. doi:10.1007/s00228-019-02689-y
25. Lenharo M. An AI revolution is brewing in medicine. What will it look like? *Nature*. 2023;622(7984):686–688. doi:10.1038/d41586-023-03302-0.
26. Regulation. EU - 2024/1689 - EN -. EUR–Lex.
27. Hamet P, Tremblay J. Artificial intelligence in medicine. *Metabolism*. 2017:69S:S36–S40. PMID: 28126242. doi:10.1016/j.metabol.2017.01.011
28. Ramesh AN, Kambhampati C, Monson JR, Drew PJ. Artificial intelligence in medicine. *Ann R Coll Surg Engl*. 2004;86(5):334–338.PMID: 15333167; PMCID: PMC1964229. doi:10.1308/147870804290
29. Liu PR, Lu L, Zhang JY, Huo TT, Liu SX, Ye ZW. Application of artificial intelligence in medicine: an overview. *Curr Med Sci*. 2021;41 (6):1105–1115.PMID: 34874486; PMCID: PMC8648557. doi:10.1007/s11596-021-2474-3
30. Bellini V, Valente M, Gaddi AV, Pelosi P, Bignami E. Artificial intelligence and telemedicine in anesthesia: potential and problems. *Minerva Anestesiol*. 2022;88(9):729–734.PMID: 35164492. doi:10.23736/S0375-9393.21.16241-8
31. Nazer LH, Zatarah R, Waldrip S, et al. Bias in artificial intelligence algorithms and recommendations for mitigation. *PLOS Digit Health*. 2023;2(6): e0000278.PMID: 37347721; PMCID: PMC10287014. doi:10.1371/journal.pdig.0000278
32. Sallam M, Al-Mahzoum K, Sallam M. generative artificial intelligence and cybersecurity risks: implications for healthcare security based on real-life incidents. *Mesopotamian J Artificial Intelligence Healthcare*. 2024;2024:184–203. doi:10.58496/MJAIH/2024/019
33. Buttazzo G. Rise of artificial general intelligence: risks and opportunities. *Front Artif Intell*. 2023;6:1226990. PMID: 37693010; PMCID: PMC10485377. doi:10.3389/frai.2023.1226990
34. Kiener M. Artificial intelligence in medicine and the disclosure of risks. *AI Soc*. 2021;36(3):705–713.PMID: 33110296; PMCID: PMC7580986. doi:10.1007/s00146-020-01085-w

35. Ersoy Y. The advantages and barriers in implementing industry 4.0 and key features of industry 4.0. *J Int Scientific Res*. (2022);7:207–214. doi:10.23834/isrjournal.1122471
36. Tehci A, Ersoy Y.*(2020). Industry 4.0: New Approaches in Production Management and Marketing*.In Advanced Manufacturing.Progress, Trends and Challenges, Nova Science Publisher;ISBN: 978-1-53618-870-7
37. Firouzi F, Farahani B, Daneshmand M, et al. Harnessing the power of smart and connected health to tackle COVID-19: ioT, AI, robotics, and blockchain for a better world. *IEEE Internet Things J*. 2021;8(16):12826–12846.PMID: 35782886; PMCID: PMC8769005. doi:10.1109/JIOT.2021.3073904
38. Tagde P, Tagde S, Bhattacharya T, et al. Blockchain and artificial intelligence technology in e-Health. *Environ Sci Pollut Res Int*. 2021;28(38):52810–52831.PMID: 34476701; PMCID: PMC8412875. doi:10.1007/s11356-021-16223-0
39. Waseem HM, Islam SU, Harrison S, et al. Data-driven FMEA approach for hazard identification and risk evaluation in digital health. *Sci Rep*. 2025;15(1):26856.PMID: 40702036; PMCID: PMC12287468. doi:10.1038/s41598-025-11929-4
40. Dyrbye LN, Varkey P, Boone SL, Satele DV, Sloan JA, Shanafelt TD. Physician satisfaction and burnout at different career stages. *Mayo Clin Proc*. 2013;88(12):1358–1367.PMID: 24290109. doi:10.1016/j.mayocp.2013.07.016
41. Baethge C, Goldbeck-Wood S, Mertens S. SANRA—a scale for the quality assessment of narrative review articles. *Research*. *Integrity and Peer Rev*. 2019;4(1):5. doi:10.1186/s41073-019-0064-8
42. Mittermaier M, Raza MM, Kvedar JC. Bias in AI-based models for medical applications: challenges and mitigation strategies. *NPJ Digit Med*. 2023;6(1):113. doi:10.1038/s41746-023-00858-z
43. Malatji M, Tolah A. Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI Ethics*. doi:10.1007/s43681-024-00427-4
44. Waters M. AI meets informed consent: a new era for clinical trial communication. *JNCI Cancer Spectr*. 2025;9(2):pkaf028.PMID: 40104849; PMCID: PMC11964292. doi:10.1093/jncics/pkaf028
45. Gerke S, Minssen T, Cohen G.Ethical and legal challenges of artificial intelligence-driven healthcare. *Artif intell in healthcare*. 2020;295–336. PMCID: PMC7332220. doi:10.1016/B978-0-12-818438-7.00012-5
46. Iserson KV. Informed consent for artificial intelligence in emergency medicine: a practical guide. *Am J Emerg Med*. 2024;76:225–230. PMID: 38128163. doi:10.1016/j.ajem.2023.11.022
47. Barnes C, Aboy MR, Minssen T, et al. Enabling demonstrated consent for biobanking with blockchain and generative AI. *Am J Bioeth*. 2025;25(4):96–111.PMID: 39499856; PMCID: PMC12005476. doi:10.1080/15265161.2024.2416117
48. Ontaneda D, Ross LA, MRI HR. Big data, and artificial intelligence: rewards vs risks. *Neurology*. 2021. 97(21):975–976. **2021**. 10.1212/WNL.0000000000012883. PMID: 34607921.
49. The dark secret at the heart of AI. *MIT Technology Review*. Available from: https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/. Accessed January 16, 2025.
50. Adnan M, Kutafina E, Beyan O. Cybersecurity frameworks in healthcare data: short literature review. *Stud Health Technol Inform*. 2024;316:301–302. PMID: 39176732. doi:10.3233/SHTI240403
51. Murdoch B. Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Med Ethics*. 2021;22(1):122.PMID: 34525993; PMCID: PMC8442400. doi:10.1186/s12910-021-00687-3
52. Simon M, Looten V. Description of data breaches notifications in France and lessons learned for the healthcare stakeholders. *Stud Health Technol Inform*. 2020;275:192–196. PMID: 33227767. doi:10.3233/SHTI200721
53. Gomase VS, Ghatule AP, Sharma R, Sardana S. Cybersecurity and compliance in clinical trials: the role of artificial intelligence in secure healthcare management. *Rev Recent Clin Trials*. PMID: 40277117. doi:10.2174/0115748871366467250413070850
54. Machal ML. Risks and benefits associated with the primary functions of artificial intelligence powered autoinjectors. *Front Med Technol*. 2024;6:1331058. PMID: 38645777; PMCID: PMC11026574. doi:10.3389/fmedt.2024.1331058
55. Angehrn Z, Haldna L, Zandvliet AS, et al. Artificial Intelligence and machine learning applied at the point of care. *Front Pharmacol*. 2020;11:759. PMID: 32625083; PMCID: PMC7314939. doi:10.3389/fphar.2020.00759
56. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care*. 2017;25(1):1–10.PMID: 27689562. doi:10.3233/THC-161263
57. Carlos Ferreira J, Elvas LB, Correia R, Mascarenhas M. Enhancing Ehr interoperability and security through distributed ledger technology: a review. *Healthcare*. 2024;12(19):1967.PMID: 39408147; PMCID: PMC11477175. doi:10.3390/healthcare12191967
58. Criminal hacker hackerano l'Ospedale di Dusseldorf. Una vittima - CyberSecurity Italia.
59. Price WN 2nd, Cohen IG. Privacy in the age of medical big data. *Nat Med*. *Nature Medicine*. 2019;25(1):37–43. PMID: 30617331; PMCID: PMC6376961. doi:10.1038/s41591-018-0272-7
60. Rodgers CM, Ellingson SR, Chatterjee P. Open Data and transparency in artificial intelligence and machine learning: a new era of research. *F1000Res*. 2023;12:387. PMID: 37065505; PMCID: PMC10098385. doi:10.12688/f1000research.133019.1
61. Mazur J.Artificial Intelligence vs Data Protection: how the GDPR Can Help to Develop a Precautionary Regulatory Approach to AI?Kornilakis A, Nouskalis G, Pergantis V, Tzimas T: editors.*Artificial Intelligence and Normative Challenges: International and Comparative Legal Perspectives. Springer International Publishing;* ***2023****:215-233*.doi:10.1007/978-3-031-41081-9_12
62. La sanità è sotto attacco: soluzioni e best practice per metterla in sicurezza - Cyber Security 360.
63. Yadav N, Pandey S, Gupta A, Dudani P, Gupta S, Rangarajan K. Data privacy in healthcare: in the era of artificial intelligence. *Indian Dermatol Online J*. 2023;14(6):788–792. doi:10.4103/idoj.idoj_543_23
64. Seh AH, Zarour M, Alenezi M, et al. Healthcare data breaches: insights and implications. *Healthcare*. 2020;8(2):133. doi:10.3390/healthcare8020133
65. Rumbold JMM, Pierscionek B. The effect of the general data protection regulation on medical research. *J Med Internet Res*. 2017;19(2):e47. doi:10.2196/jmir.7108
66. Esmaeilzadeh P. Challenges and strategies for wide-scale artificial intelligence (AI) deployment in healthcare practices: a perspective for healthcare organizations. *Artif Intell Med*. 2024;151:102861. PMID: 38555850. doi:10.1016/j.artmed.2024.102861
67. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

68. Langarizadeh M, Orooji A, Sheikhtaheri A. Effectiveness of anonymization methods in preserving patients' privacy: a systematic literature review. *Stud Health Technol Inform*. 2018;248:80–87.
69. Di Pierro M. What Is the Blockchain? *Comput. Sci. Eng*. 2017;19(5):92–95. doi:10.1109/MCSE.2017.3421554
70. Belotti M, Božić N, Pujolle G, Secci S. A vademecum on blockchain technologies: when, which, and how," in IEEE communications surveys & tutorials. *Fourthquarter*. 2019;21(4):3796–3838. doi:10.1109/COMST.2019.2928178
71. Wüst K, Gervais A. *"Do You Need a Blockchain?," 2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. Zug, Switzerland;2018:45–54. doi:10.1109/CVCBT.2018.00011
72. Kewell B, Adams R, Parry G. Blockchain for good? *Strategic Change*. 2017;26:429–437.
73. Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaría V. To blockchain or not to blockchain: that is the question. *IT Professional*. 2018;20 (2):62–74. doi:10.1109/MITP.2018.021921652
74. Xu M, Chen X, Kou G. A systematic review of blockchain. *Financ Innov.* 2019;5(27). doi:10.1186/s40854-019-0147-z
75. Rodrigues U. Law and the Blockchain. *Iowa Law Review*. 2018-2019;104(3):679–719.
76. Sivasankari B, Varalakshmi P. Blockchain and iot technology in healthcare: a review. *Stud Health Technol Inform*. 2022;294:277–278. PMID: 35612074. doi:10.3233/SHTI220455
77. Fang HSA, Tan TH, Tan YFC, Tan CJM. Blockchain personal health records: systematic review. *J Med Internet Res*. 2021;23(4):e25094.PMID: 33847591; PMCID: PMC8080150. doi:10.2196/25094
78. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences-A scoping review. *Int J Med Inform*. 2020;134:104040. PMID: 31865055. doi:10.1016/j.ijmedinf.2019.104040
79. Evangelatos N, Özdemir V, Brand A. Blockchain for digital health: prospects and challenges. *OMICS*. 2020;24(5):237–240.PMID: 32316827. doi:10.1089/omi.2020.0045
80. Saeed H, Malik H, Bashir U, et al. Blockchain technology in healthcare: a systematic review. *PLoS One*. 2022;17(4):e0266462.PMID: 35404955; PMCID: PMC9000089. doi:10.1371/journal.pone.0266462
81. Kuo TT, Zavaleta Rojas H, Ohno-Machado L. Comparison of blockchain platforms: a systematic review and healthcare examples. *J Am Med Inform Assoc*. 2019;26(5):462–478.PMID: 30907419; PMCID: PMC7787359. doi:10.1093/jamia/ocy185
82. Tayebi S, Amini H. The flip side of the coin: exploring the environmental and health impacts of proof-of-work cryptocurrency mining. *Environ Res*. 2024;252(Pt 1):118798. doi:10.1016/j.envres.2024.118798.
83. Cheng M, Chong HY, Xu Y. Blockchain-smart contracts for sustainable project performance: bibliometric and content analyses. *Environ Dev Sustain*. 2023;2:1–24. PMID: 37363021; PMCID: PMC9979138. doi:10.1007/s10668-023-03063-w
84. Batchu S, Patel K, Henry OS, et al. Using ethereum smart contracts to store and share COVID-19 patient data. *Cureus*. 2022;14(1):e21378.PMID: 35198290; PMCID: PMC8853077. doi:10.7759/cureus.21378
85. Vargas C, Mira da Silva M. Case studies about smart contracts in healthcare. *Digit Health*. 2023;9:20552076231203571. PMID: 37822961; PMCID: PMC10563467. doi:10.1177/20552076231203571
86. Ullah F, He J, Zhu N, et al. Blockchain-enabled EHR access auditing: enhancing healthcare data security. *Heliyon*. 2024;10(16):e34407.PMID: 39253236; PMCID: PMC11381610. doi:10.1016/j.heliyon.2024.e34407
87. Amofa S, Xia Q, Xia H, et al. Blockchain-secure patient Digital Twin in healthcare using smart contracts. *PLoS One*. 2024;19(2):e0286120.PMID: 38422025; PMCID: PMC10903884. doi:10.1371/journal.pone.0286120
88. Chakravarthy DG, Gopi R, Murugan S, et al. Enhancing confidentiality and access control in electronic health record systems using a hybrid hashing blockchain framework. *Sci Rep*. 2025;15(30379). doi:10.1038/s41598-025-13831-5
89. Pelekoudas-Oikonomou F, Zachos G, Papaioannou M, et al. Blockchain-based security mechanisms for IoMT edge networks in iomt-based healthcare monitoring systems. *Sensors*. 2022;22(7):2449.PMID: 35408064; PMCID: PMC9003194. doi:10.3390/s22072449
90. Lakshminarayanan V, Ravikumar A, Sriraman H, Alla S, Chattu VK. Health care equity through intelligent edge computing and augmented reality/ virtual reality: a systematic review. *J Multidiscip Healthc*. 2023;16:2839–2859. PMID: 37753339; PMCID: PMC10519219. doi:10.2147/JMDH. S419923
91. Klonoff DC. Fog computing and edge computing architectures for processing data from diabetes devices connected to the medical internet of things. *J Diabetes Sci Technol*. 2017;11(4):647–652.PMID: 28745086; PMCID: PMC5588847. doi:10.1177/1932296817717007
92. P.vinayasree AMR. Advanced blockchain framework for healthcare records: hyperledger fabric with novel consensus and authentication algorithms. *Front Health Informatics*. 2024;13(3):8470–8487.
93. Available from: https://www.media.mit.edu/research/?filter=everything&page=2&tag=blockchain&utm. Accessed August 28, 2025).
94. Available from: https://patientory.com/blog/2018/04/03/birds-eye-view-patientory-software?utm. Accessed August 28, 2025).
95. FDA. MediLedger DSCSA Pilot Project. U.S. Food and Drug Administration. 2023. Available From: https://www.fda.gov/media/168283/download. Accessed August 28, 2025).
96. Abudul Kareem AB. Modelling Of Blockchain Technology. *SHIFRA*. 2024;2024:97–104. doi:10.70470/SHIFRA/2024/011
97. Integration of Artificial Intelligence. Blockchain, and quantum cryptography for securing the industrial internet of things (IIoT): recent advancements and future trends. *Applied Data Sci Analysis*. 2025;19–82. doi:10.58496/ADSA/2025/004
98. Martinazzi S, Flori A, Spelta A. The evolving topology of the Lightning Network: centralization, efficiency, robustness, synchronization, and anonymity. *PLoS One*. 2020;15(1):e0225966.PMID: 31940309; PMCID: PMC6961907. doi:10.1371/journal.pone.0225966
99. Di Palma G, Scendoni R, Tambone V, Alloni R, De Micco F. Integrating enterprise risk management to address AI-related risks in healthcare: strategies for effective risk mitigation and implementation. *J Healthc Risk Manag*. 2025;44:25–33. PMID: 39951018. doi:10.1002/jhrm.70000