THE JOURNAL OF TELEMEDICINE

Ghaemi et al., Health data control, Winter 2026 3(1), 42-55

REVIEWS

An Analytical Review of Methods and Models for Health Data Control

Mohammad Mehdi Ghaemi, Zahra Pourmand*

ABSTRACT

The rapid digital transformation of healthcare has increased the generation, storage, and exchange of electronic health data, creating challenges related to security, privacy, interoperability, and access control. This structured narrative review examines contemporary approaches to healthcare data control based on peer-reviewed studies published between 2018 and 2026. The literature was synthesized into six thematic categories: access-control models, cryptographic techniques, blockchain-based frameworks, anonymization methods, artificial intelligence and machine learning approaches, and hybrid security architectures. The findings show that traditional access-control mechanisms alone are insufficient for modern healthcare environments. Emerging technologies such as homomorphic encryption, blockchain, federated learning, and artificial

Received 18/05/2026
Accepted for publication 15/06/2026
Published 21/06/2026

* ***Correspondence to****: Zahra Pourmand, Department of Health Information Sciences, Faculty of Management and Medical Information Sciences, Kerman University of Medical Sciences, Kerman, Iran Email: z.pourmand@kmu.ac.ir*

About the authors:

Mohammad Mehdi Ghaemi; MD, PhD in Medical Informatics, Associate Professor, Department of Health Information Sciences, School of Management and Medical Information Sciences, Kerman University of Medical Sciences, Kerman, Iran.

Head of Medical Informatics Research Center, Institute for Futures Studies in Health, Kerman University of Medical Sciences, Kerman, Iran.

Zahra Pourmand; PhD Candidate in Medical Informatics, Department of Health Information Sciences, Faculty of Management and Medical Information Sciences, Kerman University of Medical Sciences, Kerman, Iran.

intelligence improve confidentiality, privacy protection, and threat detection. However, their adoption remains constrained by challenges including computational complexity, scalability, interoperability, and implementation barriers. The review also highlights the importance of interoperability standards, particularly HL7 FHIR, and patient-centered data governance for secure information exchange. Overall, the evidence suggests that hybrid and multilayered architectures that combine complementary security technologies provide the most effective approach to controlling healthcare data. Future research should focus on enhancing interoperability, developing scalable privacy-preserving solutions, strengthening governance frameworks, and facilitating real-world implementation.

Keywords: Electronic Health Records, Privacy, Computer Security, Blockchain, Machine Learning, Medical Informatics, Online Systems

INTRODUCTION

Healthcare data includes information about individuals' physical, psychological, and social conditions that is collected, processed, and exchanged across healthcare systems. The rapid digitalization of healthcare through electronic health records (EHRs), telemedicine platforms, wearable devices, mobile health applications, and the Internet of Medical Things (IoMT) has significantly increased the volume and value of health information. Consequently, healthcare organizations have become increasingly dependent on digital infrastructures for clinical, administrative, and research activities (1,2).

Although digital transformation offers substantial benefits for healthcare delivery and decision-making, it has also introduced significant security and privacy concerns. Healthcare data are among the most sensitive categories of personal information, and unauthorized disclosure may result in financial, social, and psychological harm to patients. In addition, healthcare organizations have become frequent targets of cyberattacks because of the high value of medical information and the complexity of interconnected healthcare systems (2,3).

Recent studies have identified multiple vulnerabilities across healthcare ecosystems, including weaknesses in healthcare data, medical devices, healthcare networks, and cloud-based infrastructure (2). Traditional healthcare data management systems are also challenged by issues such as centralized architectures, limited auditability, and potential misuse of access privileges by authorized users (4). These limitations have increased the need for advanced approaches to ensure secure data access, preserve privacy, and enable trustworthy information exchange.

To address these challenges, a wide range of healthcare data control mechanisms has been developed, including access-control models, cryptographic techniques, blockchain-based frameworks, anonymization methods, artificial intelligence (AI)-driven security solutions, and privacy-preserving machine learning approaches (4–6). Emerging technologies such as federated learning and homomorphic encryption have further expanded opportunities for secure analytics while reducing the exposure of sensitive patient information (6,15).

At the same time, regulatory and governance frameworks play an essential role in healthcare data protection. International regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) have established important principles for privacy protection, secure data processing, and patient rights (4,5). Furthermore, interoperability standards such as Health Level Seven (HL7) and Fast Healthcare Interoperability Resources (FHIR) have become increasingly important for enabling secure and standardized health information exchange across heterogeneous healthcare environments (4,20).

To provide a comprehensive overview of contemporary healthcare data control approaches, a targeted literature search was conducted in PubMed, Scopus, Web of Science, IEEE Xplore, SID, and Magiran for studies published between 2018 and 2026. Eligible peer-reviewed articles and conference papers addressing healthcare data security, privacy protection, and access management mechanisms were reviewed and organized into six thematic domains: access control models, cryptographic techniques, blockchain frameworks, anonymization methods, artificial intelligence and machine learning approaches, and hybrid security architectures.

Objectives

This study presents a structured narrative review of current methods and models for healthcare data control. The review critically examines their strengths, limitations, implementation challenges, and future directions, with particular emphasis on secure healthcare data governance, privacy preservation, interoperability, and emerging intelligent security architectures.

1. Healthcare Data Control Models

Healthcare data control encompasses a wide range of technologies and frameworks designed to protect the confidentiality, integrity, availability, and privacy of health information. Based on the reviewed literature, the major approaches can be categorized into six broad groups: traditional access control models, cryptography-based approaches, blockchain-based frameworks, anonymization techniques, artificial intelligence and machine learning-based methods, and hybrid security architectures. Each category addresses different aspects of healthcare cybersecurity and presents unique strengths and limitations.

1.1Traditional Access Control Models

Access control is considered the first security layer in healthcare information systems and determines which users are authorized to access, modify, or manage healthcare data.

1.1.1 Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) was originally introduced by Sandhu in 1996 and remains one of the most widely implemented access-control mechanisms in healthcare systems. In RBAC, permissions are assigned according to predefined organizational roles such as physicians, nurses, laboratory personnel, and healthcare administrators (4, 10).

RBAC offers simple authorization management, centralized administration, and high scalability in structured healthcare environments. However, its predefined role structure limits flexibility in dynamic clinical situations where temporary or emergency access to patient information may be required (4, 5, 10).

1.1.2 Attribute-Based Access Control (ABAC)

Attribute-Based Access Control (ABAC) was proposed as a more flexible alternative to RBAC.

ABAC extends traditional access control by evaluating requests using contextual attributes such as user role, location, access time, patient status, and data sensitivity. This approach provides greater flexibility and fine-grained authorization in distributed healthcare environments, although it increases policy-management complexity and computational requirements (4).

1.1.3 Critical Analysis of Traditional Access-Control Models

Although RBAC and ABAC remain essential security mechanisms, access control alone cannot adequately address modern healthcare cybersecurity threats and should be complemented by encryption, auditing, and intelligent monitoring technologies (5,6,11).

1.2 Cryptography-Based Healthcare Data Protection

Cryptography is one of the most fundamental approaches to protecting the confidentiality of healthcare information. The reviewed studies investigated four major cryptographic approaches: Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), Ciphertext-Policy Attribute-Based Encryption (CP-ABE), and Homomorphic Encryption (HE) (2, 6, 10, 16).

AES and RSA remain the most widely adopted cryptographic mechanisms in healthcare systems (Table 1). AES provides efficient protection for large-scale healthcare data because of its low computational overhead, whereas RSA is primarily used for authentication and secure key exchange. Several recent healthcare frameworks have combined AES-256 encryption with RSA-based key distribution to improve confidentiality and secure information sharing across distributed environments (5,6). Despite their widespread use, challenges related to key management and scalability persist in large healthcare ecosystems (5, 16).

1.2.1 Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

CP-ABE enables fine-grained and decentralized access control by embedding authorization policies directly into encrypted data. This approach facilitates secure healthcare information sharing across distributed environments, although computational complexity and attribute management overhead remain significant implementation challenges (2, 4, 6).

1.2.2 Homomorphic Encryption (HE)

Homomorphic encryption supports privacy-preserving analytics by enabling computations on encrypted healthcare data without revealing sensitive information. Despite its strong privacy guarantees, high computational cost, and scalability limitations currently restrict routine clinical deployment (6). Additional details are provided in Table 1.

1.3 Blockchain-Based Healthcare Security Frameworks

Blockchain has emerged as an important technology in healthcare cybersecurity because of its decentralized architecture, immutability, transparency, and distributed trust mechanisms. By maintaining tamper-resistant records and verifiable transaction histories, blockchain can improve data integrity, traceability, and accountability in healthcare information systems (4–6).

TABLE I. COMPARISON OF ENCRYPTION METHODS IN HEALTHCARE DATA CONTROL APPLICATIONS

Encryption Method	*Key Structure*	*Encryption/Decryption Speed*	*Computational Overhead*	*Computation on Encrypted Data*	*Primary Healthcare Application*
AES (Symmetric)	Single key	Very high	Very low	No	Large-scale healthcare data encryption
RSA (Asymmetric)	Public/private keys	Low	Moderate	No	Secure key distribution
CP-ABE	Public/private + master key	Moderate	Moderate to high	No	Fine-grained secure data sharing
Homomorphic Encryption	Two-key structure	Very low	Very high	Yes	Privacy-preserving medical analytics

1.3.1 Types of Blockchain

Blockchain platforms can be categorized into public and permissioned systems. Public blockchains allow unrestricted participation but often face privacy, latency, and energy-consumption concerns. Permissioned blockchains restrict participation to authorized users and are generally considered more suitable for healthcare environments due to their stronger privacy and access control capabilities (5, 6).

1.3.2 Hyperledger Fabric

Hyperledger Fabric is the most frequently reported permissioned blockchain platform in healthcare applications. Through distributed ledgers, smart contracts, and identity-management mechanisms, it supports secure data sharing, traceability, and patient-centered access management. Nevertheless, implementation complexity, infrastructure requirements, and interoperability challenges continue to limit large-scale adoption (5, 6).

The reviewed studies suggest that Hyperledger Fabric improves auditability, traceability, and trust management, although implementation complexity, interoperability issues, infrastructure costs, and scalability challenges remain important barriers to adoption (5, 6).

1.3.3 Challenges of Blockchain in Healthcare

Despite its advantages, blockchain implementation in healthcare remains constrained by transaction latency, scalability limitations, infrastructure costs, regulatory requirements, and integration challenges with legacy systems (4–6).

The reviewed studies also emphasized the importance of interoperability standards such as HL7 FHIR for secure data exchange. Overall, blockchain should be viewed as a component

of broader multilayered healthcare security architectures rather than a standalone solution (4–6).

1.3.4 Emerging Trends: Blockchain and Cloud Integration

Emerging healthcare architectures increasingly combine blockchain with cloud computing, federated learning, and advanced cryptographic techniques. Recent studies suggest that integrating these technologies may enhance privacy-preserving analytics, secure data sharing, and distributed healthcare intelligence while maintaining patient confidentiality (7, 16).

1.3.5 Interoperability and Patient-Centered Data Control

Interoperability remains a critical challenge in healthcare data control because many healthcare information systems continue to rely on heterogeneous legacy infrastructures. Standards such as HL7 and FHIR facilitate secure health information exchange through standardized data formats, application programming interfaces, and access-management mechanisms (4,20). In parallel, patient-centered approaches have gained increasing attention. Dynamic consent models enable patients to manage authorization for sharing their health information and provide greater transparency in data governance (19). Emerging blockchain-based smart contracts may further automate consent management and authorization processes while improving traceability and accountability (5,6). However, interoperability constraints, regulatory requirements, identity-management issues, and workflow integration challenges continue to limit large-scale implementation (4,19,20).

1.4 Anonymization and Privacy-Preserving Techniques

Anonymization techniques reduce the risk of patient re-identification while enabling the use of healthcare data for research, analytics, and information sharing. Common approaches include data masking, suppression, generalization, and perturbation, as well as anonymization models such as k-anonymity, l-diversity, and t-closeness, which provide progressively stronger protection for sensitive attributes (2,4,10). Although these methods enhance privacy protection, increasing levels of anonymization may reduce data utility and analytical precision (10).

Although these methods are computationally efficient, they remain vulnerable to correlation and re-identification attacks. Abouelmhedi et al. (2018) demonstrated that anonymized healthcare records could still be re-identified using auxiliary metadata such as browser User-Agent information (10). Therefore, the reviewed studies consistently concluded that anonymization alone is insufficient in modern healthcare environments and should be integrated with encryption, access control mechanisms, and other privacy-preserving technologies (4, 10).

1.5 Artificial Intelligence and Machine Learning-Based Security Models

Artificial intelligence (AI) and machine learning (ML) are increasingly used to enhance healthcare cybersecurity through anomaly detection, intrusion prevention, behavioral analysis, and adaptive threat monitoring (11,12). Anomaly detection aims to identify abnormal behaviors, suspicious access requests, or unusual network activities that may indicate security threats. Previous studies have shown that traditional rule-based approaches often struggle with the complexity and scale of modern healthcare systems, resulting in high false-positive and false-negative rates (11).

Anomaly-detection methods can be broadly categorized into threshold-based, regression-based, clustering-based, and deep learning approaches (11). Among these, deep learning techniques have demonstrated particularly promising performance in complex healthcare environments. Autoencoders, LSTM networks, and transformer-based models have been successfully applied to detect anomalous patterns in electronic health records and other healthcare datasets (8,13,14,17). Isolation Forest has also been reported as an effective unsupervised anomaly-detection method (11).

Overall, the reviewed studies suggest that AI-based approaches can improve the detection of unauthorized access, insider threats, and abnormal system behaviors. However, their effectiveness remains dependent on the availability of high-quality datasets and is constrained by challenges related to interpretability, generalizability, and real-world implementation (11–14,17).

1.5.1 Practical Applications of Anomaly Detection in Healthcare Data Control

The reviewed studies demonstrated that AI-based anomaly-detection systems can support healthcare cybersecurity by identifying unauthorized access, insider threats, and network intrusions (11,12). Several studies have also proposed integrating anomaly-detection models with privacy-preserving technologies, such as homomorphic encryption, to enable secure analysis of healthcare data while maintaining patient confidentiality (6). These findings suggest that AI-driven security frameworks can strengthen healthcare data protection through intelligent and adaptive threat detection mechanisms (6,11,12).

1.5.2 Challenges of Machine Learning-Based Security Models

Table 2 presents the major limitations of machine learning-based healthcare cybersecurity systems, as categorized by Bhanja et al. (2026) (11).

TABLE III. MAJOR CHALLENGES OF MACHINE LEARNING METHODS IN HEALTHCARE SECURITY

Challenge	***Description***
Data Limitations	Deep learning methods require large, high-quality datasets. Rare diseases and limited clinical samples may reduce effectiveness.
Lack of Interpretability	Many deep learning models function as “black-box” systems, making clinical interpretation difficult.
Uncertainty and Generalizability	Models trained in one hospital environment may perform poorly in other institutions.
EHR-Specific Challenges	EHR datasets are often heterogeneous, incomplete, and irregularly recorded over time.

Although artificial intelligence is expected to play a major role in the future of healthcare cybersecurity, the reviewed studies emphasized that most current AI-based healthcare

security frameworks remain experimental and have not yet been comprehensively validated in large-scale real-world hospital environments (11, 12).

1.5.3 Privacy-Preserving Learning and Data Protection Approaches

In addition to machine-learning frameworks, several complementary privacy-preserving approaches have been proposed to support secure healthcare analytics. Federated learning has emerged as an important privacy-preserving framework that enables healthcare organizations to collaboratively train machine-learning models without sharing raw patient data (15). Instead, only model updates or aggregated results are exchanged, reducing privacy risks while supporting distributed analytics. Tomášik et al. demonstrated that data-quality assessment can be performed across federated healthcare networks without exposing sensitive patient information (15).

Differential privacy provides an additional layer of protection by introducing carefully calibrated statistical noise into data or analytical outputs, thereby reducing the risk of patient re-identification while preserving overall data utility (18). To address the challenge of balancing privacy protection and analytical accuracy, Kuang et al. proposed the Flexible Differential Privacy based on Evolutionary Learning (FDPEL) framework, which generates privacy–utility trade-off solutions for different operational requirements (18). Together, federated learning and differential privacy support privacy-preserving healthcare analytics while reducing the need for direct sharing of sensitive patient information (15,18).

1.6 Hybrid Healthcare Security Models

The reviewed studies consistently demonstrated that hybrid and multilayered architectures provide the most comprehensive healthcare data protection frameworks (4-6).

Rather than relying on a single protection mechanism, hybrid models integrate blockchain, encryption frameworks, access-control systems, artificial intelligence, anonymization methods, and distributed learning approaches into unified security architectures.

Taloba and Rayan (2025) proposed one of the most advanced hybrid healthcare cybersecurity frameworks combining three major technologies (6):

1. Permissioned Blockchain (Hyperledger Fabric): Used for decentralized transaction logging, immutable auditing, and smart-contract execution.
2. Encrypted RBAC: Access-control roles and permissions are encrypted using AES-256 before storage on the blockchain.
3. Homomorphic Encryption (Paillier): Enables privacy-preserving computations directly on encrypted healthcare data.

The reviewed framework consisted of six major operational phases:

1. User registration and role assignment
2. Homomorphic encryption of healthcare records
3. Role-based access requests through smart contracts
4. Privacy-preserving statistical analysis
5. Immutable auditing and integrity verification
6. Emergency-access mechanisms for critical situations (6)

Figure 1 illustrates the conceptual architecture proposed in this review. It demonstrates how encrypted RBAC, blockchain, homomorphic encryption, off-chain storage, and audit

mechanisms can be integrated to provide secure, privacy-preserving, and traceable control over healthcare data (6).

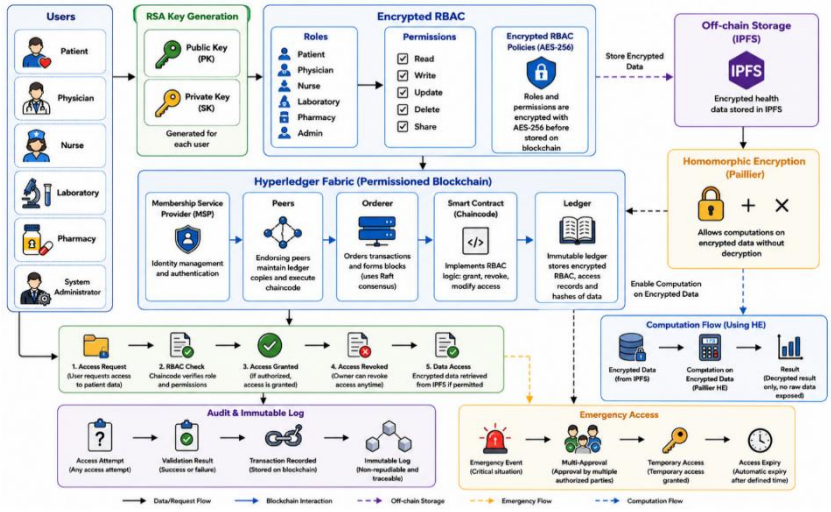

FIGURE I. Conceptual framework of the proposed healthcare data control architecture integrating encrypted role-based access control (RBAC), Hyperledger Fabric blockchain, off-chain IPFS storage, homomorphic encryption, audit logging, and emergency access management. The framework provides secure authentication and authorization, encrypted data storage, privacy-preserving computation, and traceable access control mechanisms for healthcare data (adapted from Taloba & Rayan (6)).

Despite their substantial security advantages, hybrid architectures remain associated with several implementation barriers:

- High architectural complexity
- Infrastructure and maintenance costs
- Computational overhead
- Integration difficulties with legacy hospital systems
- Limited real-time scalability in resource-constrained environments

The reviewed studies emphasized that interoperability with existing hospital systems, such as HIS, RIS, and LIS, remains one of the most significant challenges for practical deployment of advanced hybrid healthcare-security architectures (4-6).

2. Comparative Analysis of Healthcare Data Control Models

2.1 Comparative Evaluation of Healthcare Data Control Models

The comparative analysis revealed that each healthcare data control approach possesses distinct strengths and limitations depending on infrastructure requirements, scalability demands, operational complexity, and cybersecurity objectives.

Traditional RBAC frameworks provide simplicity and high scalability, but limited flexibility. ABAC improves contextual authorization management while increasing policy complexity. Encryption-based approaches provide strong confidentiality protection but may introduce substantial computational overhead. Blockchain frameworks improve transparency, integrity, and traceability but face interoperability and scalability challenges (4-6).

Artificial intelligence-based systems improve intelligent threat detection but require large, high-quality datasets and advanced computational infrastructures (11, 12, 13). Federated learning enables privacy-preserving distributed analytics without centralized data transfer, whereas differential privacy reduces re-identification risks by injecting statistical noise (15, 18).

Overall, the reviewed studies consistently demonstrated that hybrid multilayered architectures integrating blockchain, encryption, artificial intelligence, anonymization, federated learning, and dynamic access-control mechanisms provide the highest overall security performance for modern healthcare ecosystems (5, 6).

2.1.1 Overall Synthesis of Healthcare Data Control Approaches

The reviewed evidence demonstrates a gradual shift from isolated security mechanisms to intelligent, multilayered healthcare data control architectures. Traditional access-control models such as RBAC and ABAC remain important foundations for authorization management; however, they are increasingly complemented by encryption, blockchain, artificial intelligence, and privacy-preserving learning approaches (4–6). Cryptographic techniques continue to provide strong confidentiality protection, while blockchain enhances transparency, traceability, and trust in healthcare information exchange (5,6,16). Artificial intelligence and machine-learning methods offer advanced capabilities for anomaly detection and threat monitoring, but remain constrained by challenges related to interpretability, data quality, and real-world validation (11–15,17). Overall, hybrid architectures that integrate complementary technologies appear to offer the most comprehensive approach to healthcare data control, although interoperability, scalability, and implementation complexity remain significant barriers to widespread adoption (4–6).

The approaches summarized in Table 3 were comparatively evaluated using three qualitative indicators: evidence strength, real-world validation, and maturity level. These ratings were derived from a narrative synthesis of the reviewed literature rather than a formal evidence-grading framework. Evidence strength reflects the relative consistency and frequency of supporting findings across independent studies. Real-world validation indicates the extent to which an approach has been implemented or evaluated in operational healthcare environments rather than only in simulation or laboratory settings. Maturity level represents the current stage of technological development and adoption, considering factors such as implementation experience, integration into healthcare workflows, and reported practical use. These qualitative assessments are intended to facilitate comparative interpretation and should not be regarded as standardized or quantitative evidence rankings.

2.2 Situation in Iran: Proposed Models and Patient Safety Standards

Marzban (2025) compared four major cyberattack-prevention models for healthcare information systems, emphasizing that, given current infrastructural and economic conditions in Iran, healthcare organizations should prioritize practical, cost-effective measures such as staff training, cybersecurity awareness, and regular healthcare data backups alongside advanced technological solutions (3).

TABLE III. COMPARATIVE EVALUATION OF HEALTHCARE DATA CONTROL MODELS

Model	*Major Advantage*	*Major Limitation*	*Security Level*	*Complexity*	*Scalability*	*Evidence Strength*	*Real-world Validation*	*Maturity Level*
RBAC	Simplicity and high speed	Limited flexibility	Moderate	Low	High	High	High	Mature
ABAC	Dynamic access control	Policy-management complexity	Moderate	Moderate	Moderate	Moderate	Moderate	Mature
AES/RSA	High confidentiality	Key-management challenges	High	Low to moderate	High	High	High	Mature
CP-ABE	Fine-grained access control	Computational overhead	High	High	Moderate	Moderate	Low	Emerging
Homomorphic Encryption	Computation on encrypted data	Extremely high latency	Very high	Very high	Low	Moderate	Very Low	Experimental
Blockchain	Transparency and decentralization	Cost and scalability challenges	High	High	Moderate	Moderate	Low	Emerging
Anonymization	Simplicity and low cost	Re-identification vulnerability	Low to moderate	(k-anonymity) Low (l-Diversity/t-Closeness) Moderate to high	High	High	High	Mature
Machine Learning	Detection of complex threats	False-positive alerts and interpretability limitations	High	High	Moderate	Moderate	Moderate	Emerging
Federated Learning	Privacy preservation without raw-data transfer	Coordination complexity	High	Moderate to high	High	Moderate	Low–Moderate	Developing
Differential Privacy	Reduction of re-identification risk	Reduced analytical precision	High	Moderate	High	Moderate	Low–Moderate	Emerging

Hybrid Models	Multilayered security protection	Architectural complexity	Very High	Very high	Low	Moderate	Low	Experimental

Nekoei Moghadam et al. (2021) assessed compliance with mandatory patient-safety standards across seven Iranian hospitals and reported an overall compliance rate of approximately 70% (9). The highest compliance was observed for safe-environment indicators (75%), whereas patient engagement showed the lowest compliance (47%), highlighting weaknesses in patient education, informed consent, and participation in clinical decision-making (9).

Limitations

This structured narrative review has several limitations that should be considered when interpreting its findings. First, although a targeted search was conducted across multiple international and regional databases, the literature selection process may be subject to selection bias because no formal systematic review protocol or quality assessment framework was applied. Second, the review included only English- and Persian-language publications, which may have excluded relevant studies published in other languages. Third, because this review adopted a narrative rather than a systematic approach, the methodological quality and risk of bias of the included studies were not evaluated using standardized appraisal tools. Finally, healthcare cybersecurity is a rapidly evolving field, and emerging technologies, standards, and security frameworks published after the search period may not be reflected in the present review. Despite these limitations, the review provides a comprehensive and up-to-date synthesis of major healthcare data control approaches, including their current applications, challenges, and future directions.

Ethical Statement

As this study is based solely on previously published literature and does not involve human participants, patient information, or animal subjects, ethical approval was not required.

CONCLUSION

The rapid digital transformation of healthcare has significantly increased the volume, complexity, and sensitivity of electronic health data, making effective data control a critical requirement for modern healthcare systems. This review examined contemporary approaches to healthcare data control, including access-control models, cryptographic techniques, blockchain-based frameworks, anonymization methods, artificial intelligence and machine-learning approaches, and hybrid security architectures. The findings indicate that traditional access-control mechanisms alone are no longer sufficient to address the evolving security and privacy challenges of healthcare environments.

Among the reviewed approaches, cryptographic methods provide strong confidentiality protection, blockchain enhances transparency and traceability, anonymization techniques support privacy preservation, and artificial intelligence improves intelligent threat detection. Federated learning and differential privacy further strengthen privacy-preserving analytics by reducing the need to share sensitive patient data. However, important challenges remain, including computational overhead, scalability limitations, interoperability barriers, implementation complexity, and regulatory considerations. The

evidence consistently suggests that hybrid and multilayered architectures that integrate complementary technologies offer the most comprehensive and effective strategy for healthcare data control.

Beyond technological innovation, successful healthcare data control also requires robust governance frameworks, interoperability standards, organizational readiness, and workforce capacity. In developing healthcare systems, practical measures such as staff training, encryption, behavioral monitoring, and effective access-control policies remain essential for strengthening cybersecurity resilience. Future research should focus on scalable privacy-preserving technologies, interoperable security frameworks, explainable artificial intelligence, and practical governance models that support the real-world implementation of secure healthcare data ecosystems.

Declaration of the Use of Artificial Intelligence Tools

The authors used generative artificial intelligence tools solely to improve the language, grammar, and readability of specific sentences in this manuscript. All generated suggestions were critically reviewed, verified, and substantially edited by the authors. The authors assume full responsibility for the final content of the manuscript.

Contributorship Statement

All authors reviewed, commented on, and approved the final manuscript, as well as taking responsibility for its content.

Funding Statement

This research did not receive any specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declaration Of Conflicting Interests

The authors declare no conflicts of interest regarding the research, authorship, and publication of this article.

Data Availability Statements

No primary data were generated during this study. All information analyzed in this review was obtained from previously published literature cited in the reference list.

REFERENCES

1. Khatiwada P, Yang B, Lin J-C, Blobel B. Patient-generated health data (PGHD): understanding, requirements, challenges, and existing techniques for data security and privacy. Journal of Personalized Medicine. 2024;14(3):282. doi: https://doi.org/10.3390/jpm14030282
2. Oh S-R, Seo Y-D, Lee E, Kim Y-G. A comprehensive survey on security and privacy for electronic health data. International Journal of Environmental Research and Public Health. 2021;18(18):9668. doi: https://doi.org/10.3390/ijerph18189668
3. Marzban A. Cybersecurity models for preventing attacks on health information systems. Journal of Modern Medical Information Sciences. 2025. Persian. Available from: https://jmis.hums.ac.ir/article-1-582-fa.html
4. Shojaei P, Vlahu-Gjorgievska E, Chow Y-W. Security and privacy of technologies in health information systems: A systematic literature review. Computers. 2024;13(2):41. doi: https://doi.org/10.3390/computers13020041

5. Jakhar AK, Singh M, Sharma R, Viriyasitavat W, Dhiman G, Goel S. A blockchain-based privacy-preserving and access-control framework for electronic health records management. Multimedia Tools Appl. 2024;83(36):84195-84229. doi: https://doi.org/10.1007/s11042-024-19156-8
6. Taloba AI, Rayan A. A privacy preserving medical data management framework using blockchain enabled encrypted role based access control. Sci Rep. 2025;15:43864. doi: https://doi.org/10.1038/s41598-025-93392-1
7. Chen S, Zhang X, Liu E, Xiong Y, Wang L, et al. Privacy-preserving cloud-based dermatological image processing for medical applications: a review. Journal of Cloud Computing. 2026;15:46. doi: https://doi.org/10.1186/s13677-026-00886-6
8. Wu X, Zhang YT, Wang AM, Shi MY, Wang HH, Liu L. MNSSp3: medical big data privacy protection platform based on Internet of things. IEEE Internet Things J. 2021;8(12):9876-90. doi: https://doi.org/10.1109/JIOT.2021.3054388
9. Moghadam MN, Ismaili MRA, Tavakoli MR. Investigating the situation of Iranian hospitals in terms of implementing mandatory patient safety standards: a systematic review. Iranian Journal of Public Health 2021;51(8):1766-78. doi: https://doi.org/10.18502/ijph.v51i8.10368
10. Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. Journal of big data. 2018;5(1):1. doi: https://doi.org/10.1186/s40537-017-0110-7
11. Bhanja SN, Niu H, Chen Y, Omitaomu OA, Laurio A, Trickey A, et al. Emerging Anomaly Detection Techniques for Electronic Health Records: A Survey. Intelligence-Based Medicine. 2026:100349. doi: https://doi.org/10.1016/j.ibmed.2026.100349
12. Jagadish S, Sharma P, Tiwari P, Kuchipudi B, Mehra A, editors. Anomaly Detection in Electronic Health Records Using Machine Learning Techniques. 2025 IEEE 1st International Conference on Smart Innovations in Systems, Infrastructure, Mechanical, Power, AI and Computing Technologies (SISIMPACT); 2025. p. 1-6. doi: https://doi.org/10.1109/SISIMPACT65195.2025.10968067
13. Niu H, Omitaomu OA, Langston MA, Olama M, Ozmen O, Klasky HB, et al. EHR-BERT: A BERT-based model for effective anomaly detection in electronic health records. Journal of Biomedical Informatics. 2024;150:104605. doi: https://doi.org/10.1016/j.jbi.2024.104605
14. Röchner P, Rothlauf F. Unsupervised anomaly detection of implausible electronic health records: a real-world evaluation in cancer registries. BMC Medical Research Methodology. 2023;23(1):125. doi: https://doi.org/10.1186/s12874-023-01952-7
15. Tomášik R, Kussel T, Dudová Z, Kacová R, Hrstka R, Lablans M, et al. Privacy-preserving data quality assessment for federated health data networks. BMC Medical Informatics and Decision Making. 2026;26:49. doi: https://doi.org/10.1186/s12911-025-03328-6
16. Bao Y, Qiu W, Tang P, Cheng X. Efficient, revocable, and privacy-preserving fine-grained data sharing with keyword search for the cloud-assisted medical IoT system. IEEE Journal of Biomedical and Health Informatics. 2022;26(5):2041-2051. doi: https://doi.org/10.1109/JBHI.2021.3100871
17. Estiri H, Murphy SN. Semi-supervised encoding for outlier detection in clinical observation data. Computer Methods and Programs in Biomedicine. 2019;181:104830. doi: https://doi.org/10.1016/j.cmpb.2019.104830
18. Kuang Y, Jiang B, Cui X, Li S, Liu Y, Song H. Flexible differential privacy for Internet of Medical Things based on evolutionary learning. IEEE Internet of Things Journal. 2024;11(9):16954-16968. doi: https://doi.org/10.1109/JIOT.2024.3366889
19. Lee AR, Koo D, Kim IK, Lee E, Kim HH, Yoo S, et al. Identifying facilitators of and barriers to the adoption of dynamic consent in digital health ecosystems: a scoping review. BMC Medical Ethics. 2023;24:107. doi: https://doi.org/10.1186/s12910-023-00988-9
20. Ayaz M, Pasha MF, Alzahrani MY, Budiarto R, Stiawan D. The Fast Health Interoperability Resources (FHIR) Standard: Systematic Literature Review of Implementations, Applications, Challenges and Opportunities. JMIR Medical Informatics. 2021;9(7):e21929. doi: https://doi.org/10.2196/21929
21. Hosseini A, Emami H, Sadat Y, Paydar S. Integrated personal health record (PHR) security: requirements and mechanisms. BMC Medical Informatics and Decision Making. 2023;23:116. doi: https://doi.org/10.1186/s12911-023-02225-0
22. Abedian S, Riazi H. E-Health: Security, Privacy, and Ethics Requirements from a National Perspective in I. R. Iran. Studies in Health Technology and Informatics. 2024. doi: https://doi.org/10.3233/SHTI240079