Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH
AND DEVELOPMENT

| RESEARCH ARTICLE

Auditing AI Access to Electronic Health Records: HIPAA Compliance, Challenges, Solutions, and Future Directions

Venkata Naga Mahesh Kumar Vankayala
Oracle, USA
Corresponding author: Venkata Naga Mahesh Kumar Vankayala. **Email:** venkatanagamaheshkumar@gmail.com

| ABSTRACT

The integration of artificial intelligence (AI) into healthcare, especially within Electronic Health Records (EHRs), is transforming clinical workflows and data management. However, this evolution introduces new complexities for regulatory compliance, particularly under the Health Insurance Portability and Accountability Act (HIPAA). Traditional EHR audits focus on human users, but as AI agents increasingly access sensitive patient data, audit frameworks must evolve to ensure accountability, transparency, and compliance. This article explores the regulatory requirements, technical challenges, and practical solutions for auditing AI access to EHRs, illustrated by recent real-world case studies.

| KEYWORDS

AI auditing, HIPAA compliance, Electronic Health Records, healthcare data security, regulatory frameworks

| ARTICLE INFORMATION

ACCEPTED: 12 July 2025 **PUBLISHED:** 04 August 2025 **DOI:** 10.32996/jcsts.2025.7.8.51

1. Introduction

1.1 Electronic Health Records and Traditional Auditing

Electronic Health Records are foundational to modern healthcare, supporting clinical decision-making, research, and operational efficiency. Regulatory frameworks such as HIPAA mandate strict auditing of access to patient data (U.S. Department of Health & Human Services, 2013). Traditionally, audits track human users including clinicians, administrators, and support staff by logging who accessed which records, when, and for what purpose.

1.2 The Rise of AI in Healthcare Data Management

With the rapid adoption of AI in healthcare, autonomous or semi-autonomous software agents now access, process, and sometimes modify EHR data. These systems, ranging from clinical decision support tools to natural language processing engines and predictive analytics platforms, operate at scales and speeds beyond human capability. The emergence of agentic AI systems in healthcare environments presents unique compliance challenges that require novel approaches to regulatory adherence [1].

1.3 Critical Questions in AI Auditing

This technological shift raises critical questions about how AI interactions with EHRs should be audited for HIPAA compliance, what the regulatory and ethical implications of AI access are, and which technical solutions can ensure accountability and transparency. The intersection of AI ethics and regulatory compliance has become increasingly complex, with practitioners and lawmakers holding varying perspectives on the appropriate frameworks for AI governance in sensitive domains like healthcare [2].

1.4 The Need for Robust AI Auditing

As agentic AI systems become more prevalent in clinical settings, establishing robust auditing mechanisms becomes essential not only for regulatory compliance but also for maintaining trust in AI-driven healthcare technologies. The traditional audit frameworks designed for human users must evolve to accommodate the unique characteristics and challenges posed by AI agents operating within healthcare environments.

2. HIPAA Regulatory Overview and the Need for Audit Logs

2.1 HIPAA Audit Log Requirements

The HIPAA Security Rule requires covered entities and business associates to implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Architectural requirements for HIPAA compliance have evolved to address modern audit program challenges, particularly in response to regulatory scrutiny [3]. Key requirements include recording access with all access to ePHI being logged, including user identification, date and time, and the nature of the activity such as view, modify, or delete operations.

Requirement Category	Traditional Human Access	AI Agent Access	Technical Implementation
User Identification	Employee ID, Role	Unique AI Agent ID	Service Account Registry
Access Timestamp	Login/Logout Times	API Call Timestamps	Millisecond Precision Logging
Activity Type	View, Edit, Delete	Query, Process, Modify	Enhanced Action Categorization
Data Scope	Record-level Access	Multi-record Batch Access	Granular Data Element Tracking
Purpose Documentation	Clinical Notes	Algorithmic Rationale	XAI Integration Required

Table 1: HIPAA Audit Log Requirements for AI Systems [3, 4]

2.2 Regular Review and Retention Standards

Logs must be reviewed to detect unauthorized access or suspicious activity, with retention requirements typically extending for a minimum period of six years. Modern approaches to healthcare data access incorporate robust authentication mechanisms that leverage advanced technologies to ensure audit trail integrity [4]. These systems must support incident response capabilities, enabling logs to facilitate investigations into potential breaches or unauthorized disclosures.

2.3 The Purpose and Importance of Audit Logs

Audit logs serve multiple critical functions in healthcare environments. They provide accountability by identifying who accessed or modified patient records, enhance security through detection and response to unauthorized access or breaches, demonstrate compliance with HIPAA requirements during audits or investigations, and enable forensic analysis in the event of security incidents.

2.4 Consequences of Inadequate Audit Logging

Failure to maintain adequate audit logs can result in significant consequences including regulatory penalties where HIPAA violations can incur substantial civil and potential criminal penalties. Inadequate logs may delay detection and notification of breaches, leading to reputation damage through publicized breaches or regulatory actions that erode trust. The operational impact includes impaired incident investigation and remediation capabilities when proper logs are not maintained.

3. Challenges in Auditing AI Access

3.1 Lack of Human Identity

AI processes often run under generic service accounts, making it difficult to attribute actions to a responsible party and undermining non-repudiation. Current AI accountability infrastructure faces significant gaps in establishing clear chains of responsibility, particularly when automated systems operate without direct human oversight [6]. This challenge becomes more pronounced as AI systems become increasingly autonomous in their decision-making processes.

3.2 Volume and Complexity

AI can access thousands of records in seconds, generating voluminous logs that are challenging to interpret. The sheer scale of AI operations creates unprecedented audit trail volumes that traditional review processes cannot effectively handle. This complexity is compounded by the need to understand not just what data was accessed, but why the AI system deemed that access necessary.

3.3 Transparency and Explainability

Many AI models are considered opaque systems where understanding why an AI accessed a particular record is often non-trivial. The application of explainable artificial intelligence principles becomes crucial in healthcare contexts where audit transparency is mandatory [5]. Without proper explainability mechanisms, audit logs may capture the technical details of access but fail to provide the clinical or operational rationale behind AI decisions.

3.4 Regulatory Ambiguity

While HIPAA requires all access to be logged, it does not provide explicit guidance for AI agents, creating uncertainty for compliance officers. This regulatory gap leaves healthcare organizations to interpret traditional compliance frameworks for emerging AI technologies. The absence of clear standards for AI audit requirements creates inconsistent approaches across the industry.

3.5 Chain of Custody

Tracking the full lifecycle of data as it is accessed and processed by AI agents is essential for accountability. Establishing comprehensive audit tooling that can effectively monitor and document AI behavior throughout the entire data processing pipeline remains a significant challenge [6]. This includes understanding how data flows through different AI components and ensuring that each step in the process is properly documented and traceable.

Challenge Category	Complexity Level	Impact on Compliance	Current Solutions Available
Identity Attribution	High	Critical	Service Account Management
Log Volume Management	Very High	High	ML-based Log Analysis
Explainability	High	Critical	XAI Framework Integration
Regulatory Clarity	Medium	High	Industry Best Practices
Data Provenance	Very High	Critical	Blockchain Implementation

Table 2: AI Auditing Challenges and Impact Assessment [5, 6]

4. Technical Solutions for HIPAA-Compliant AI Auditing

4.1 Enhanced Audit Trails

AI Identity Management involves assigning unique, traceable identities to each AI agent or process to establish clear accountability chains. Granular Logging requires recording access events, purpose, context, and outcome, including model version and input parameters to provide comprehensive audit documentation. Metadata Enrichment includes triggering clinical events and user context to create meaningful audit trails that support both compliance and operational understanding.

4.2 Blockchain-Based Auditing

Immutable Logs leverage blockchain technology to provide tamper-proof records of access, ensuring audit trail integrity over time. Systematic approaches to AI-blockchain integration in healthcare records management have demonstrated significant potential for enhancing security and auditability [7]. Smart Contracts can automate access controls and real-time auditing processes, creating self-executing compliance mechanisms that reduce manual oversight requirements while maintaining strict security standards.

4.3 AI-Powered Anomaly Detection

Machine learning techniques can be employed to analyze logs and flag unusual AI access patterns, providing proactive monitoring capabilities. These systems can identify deviations from established access patterns and alert compliance officers to potential security incidents or unauthorized activities before they escalate into major breaches.

4.4 Explainable AI Integration

Logging the rationale behind each AI-initiated access becomes crucial for regulatory compliance and clinical understanding. Applications of explainable artificial intelligence in healthcare contexts enable auditors and clinicians to understand not just what data was accessed but why specific decisions were made [8]. This transparency is essential for maintaining trust in AI systems and meeting regulatory requirements for accountability.

4.5 Data Provenance Tracking

Tracking the full lifecycle of data accessed and processed by AI agents ensures comprehensive accountability throughout the entire data processing pipeline. This includes documenting data transformations, intermediate processing steps, and final outcomes to create complete audit trails that support both compliance requirements and quality assurance processes.

Solution Type	Implementation Complexity	HIPAA Compliance Level	Scalability	Cost Factor
Enhanced Audit Trails	Medium	High	High	Low
Blockchain Integration	High	Very High	Medium	High
AI Anomaly Detection	High	High	Very High	Medium
XAI Integration	Very High	Very High	Medium	High
Provenance Tracking	High	Very High	High	Medium

Table 3: Technical Solutions Comparison for AI Audit Implementation [7, 8]

5. Implementation Framework

5.1 Policy Development

Define clear policies for AI access, roles, and escalation protocols that align with organizational governance structures. Effective AI governance in health systems requires comprehensive policy frameworks that address both technical implementation and organizational accountability [8]. These policies must establish clear boundaries for AI system operations while ensuring compliance with regulatory requirements and institutional standards.

5.2 Technical Architecture

Integrate identity registries, enhanced logging, blockchain ledgers, anomaly detection, and explainability modules into a cohesive technical infrastructure. Machine learning-based audit platforms can provide intelligent monitoring capabilities that enhance traditional audit processes through automated pattern recognition and anomaly detection [9]. The architecture must support scalable operations while maintaining security and performance standards across all system components.

5.3 Human Oversight

Regular review of AI access logs by compliance officers ensures that automated systems operate within acceptable parameters and regulatory boundaries. Human oversight mechanisms must be designed to complement rather than duplicate automated monitoring capabilities, focusing on strategic decision-making and exception handling rather than routine log review processes.

5.4 Integration Requirements

Ensure compatibility with existing EHR platforms and security tools to minimize disruption during implementation. The integration process must account for legacy system constraints while providing pathways for future technological evolution. Successful integration requires careful consideration of data flow patterns, system interdependencies, and user workflow impacts.

Framework Component	Primary Function	Key Stakeholders	Implementation Timeline
Policy Development	Governance Structure	Compliance Officers, Legal	Phase 1 (Months 1-2)
Technical Architecture	System Integration	IT Teams, Vendors	Phase 2 (Months 3-6)
Human Oversight	Monitoring & Review	Clinical Staff, Auditors	Phase 3 (Months 4-8)
Platform Integration	Compatibility Assurance	EHR Teams, Security	Phase 4 (Months 6-12)

Table 4: Implementation Framework Components [9, 10]

6. Case Studies: Real-World Applications of AI Agents in EHR Environments

6.1 Voice-Activated AI-Powered EHR Systems

A leading healthcare technology provider has introduced a next-generation EHR system with an integrated AI agent that allows physicians to interact with patient data using natural language voice commands. The AI agent uses advanced Natural Language Processing to convert speech into actionable queries, which are executed against the patient's records. Comprehensive surveys of artificial intelligence integration in electronic health record systems demonstrate the transformative potential of such approaches while highlighting the need for robust governance frameworks [10]. The system maintains strict patient context, ensuring queries are scoped only to the current patient.

6.2 Technical Implementation and Audit Strategies

Behind the scenes, the AI agent accesses EHR data by making programmatic API calls. This illustrates how AI agents can directly retrieve and process sensitive patient information, often without direct human oversight. The implementation requires distinct AI identity assignment with unique, non-human user identities for all API calls and data retrievals by the AI being logged under this identity. Contextual metadata logging enriches logs with the triggering physician's identity, voice command, patient context, and purpose of access.

6.3 AI Agents for Prior Authorization Automation

Another real-world application involves AI agents automating the prior authorization process. Here, the AI agent accesses payer-specific documentation templates and coverage rules, then retrieves relevant patient data from the EHR to complete forms tailored to each payer's requirements. Legal, ethical, and technical approaches to AI auditing become particularly relevant in these automated decision-making contexts where transparency and accountability are paramount [11].

6.4 Automation Audit Implementation

The implementation strategy involves AI service accounts with dedicated service accounts for the AI agent, logging all data access and submissions under this account. Purpose and scope logging records the payer, coverage rule accessed, and scope of patient data extracted. Template and rule traceability references payer-specific rules that triggered data access, while data minimization auditing logs the exact data elements accessed to ensure compliance with regulatory standards.

7. Consequences of Non-Compliance

7.1 Regulatory Penalties and Legal Implications

Failure to implement robust audit logging for AI access can lead to substantial regulatory fines where violations can result in significant penalties. Mandatory corrective action may be required by authorities, including technology upgrades and retraining programs. Enterprise AI risk mitigation frameworks emphasize the importance of proactive compliance measures to avoid such consequences [12].

7.2 Operational and Reputational Impact

Increased liability results from inadequate logs that complicate legal defense after breaches occur. Loss of accreditation represents a serious consequence where non-compliance can jeopardize institutional accreditation or funding. Patient harm may result from untraceable inappropriate access that leads to misuse of sensitive information, undermining the fundamental trust relationship between healthcare providers and patients.

8. Future Directions

8.1 Standardization and Industry Evolution

Develop industry-wide standards for AI auditability to create consistent approaches across healthcare organizations. Comprehensive surveys of AI integration in healthcare systems indicate the urgent need for standardized audit frameworks that can accommodate diverse AI implementations [10]. Federated learning approaches enable AI training across institutions without exposing raw patient data, presenting new challenges and opportunities for audit trail management.

8.2 Technological and Regulatory Advancement

Continuous monitoring represents a shift from annual to real-time audit models that can provide immediate feedback on AI system behavior. Regulatory evolution involves collaboration with regulators to clarify AI audit requirements and establish clear guidance for compliance. Ethical governance requires establishing governance bodies for oversight of AI use and auditing that can address the complex intersection of technical capabilities and ethical responsibilities [11].

9. Discussion

9.1 Integration Opportunities and Risks

AI integration in EHRs presents both significant opportunities for enhanced clinical care and substantial risks related to data security and regulatory compliance. Assigning unique identities to AI agents, enhancing audit logs, leveraging blockchain technology, and employing AI for anomaly detection are critical technical solutions for maintaining compliance and building trust in AI-driven healthcare systems.

9.2 The Role of Human Oversight

Human oversight remains essential for interpreting audit data and ensuring continuous improvement in AI system performance and compliance. Enterprise approaches to AI risk mitigation emphasize that technological solutions must be complemented by robust human governance structures [12]. The balance between automated monitoring and human judgment represents a key challenge in developing effective AI audit frameworks.

Conclusion

As AI becomes integral to EHR systems, audit frameworks must evolve to address the unique challenges posed by autonomous agents accessing sensitive patient data. Robust, context-rich audit logs combined with unique AI identities and advanced monitoring technologies ensure HIPAA compliance while fostering transparency and trust in AI-driven healthcare. The integration of blockchain-based immutable logging, explainable AI principles, and intelligent anomaly detection creates comprehensive accountability mechanisms that address both regulatory requirements and ethical obligations. Healthcare organizations must proactively implement enhanced audit trails that capture not only what AI agents access but why specific decisions were made and how data flows through processing pipelines. The successful deployment of these audit frameworks requires careful coordination between policy development, technical architecture, human oversight, and system integration components. Future directions point toward standardized industry practices, real-time monitoring capabilities, and collaborative regulatory evolution that clarifies AI audit requirements. The transformation from traditional human-centered audit models to AI-inclusive frameworks represents a critical milestone in healthcare technology governance, ensuring that the benefits of artificial intelligence can be realized while maintaining the highest standards of patient data protection and regulatory compliance.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Subash Neupane, et al., "Towards a HIPAA Compliant Agentic AI System in Healthcare," IEEE Conference on Agentic AI Systems (CAIS) 2025, 6 May 2025. Available: https://arxiv.org/pdf/2504.17669v2

[2] Arif Ali Khan, et al., "AI Ethics: An Empirical Study on the Views of Practitioners and Lawmakers," IEEE Transactions on Computational Social Systems, March 2023, 6 December 2023. Available: https://ieeexplore.ieee.org/stampPDF/getPDF.jsp?arnumber=10066257

[3] Syeda Uzma Gardazi, et al., "HIPAA and QMS Based Architectural Requirements to Cope with the OCR Audit Program," 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing, June 2012, 20 September 2012. Available: https://ieeexplore.ieee.org/document/6305857/references#references

[4] Ali Shahzad, et al., "A Robust Algorithm for Authenticated Health Data Access via Blockchain and Cloud Computing," PLOS ONE, 23 September 2024. Available: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0307039

[5] Khushi Kalasampath, et al., "A Literature Review on Applications of Explainable Artificial Intelligence (XAI)," IEEE Access, 11 March 2025. Available: https://ieeexplore.ieee.org/stampPDF/getPDF.jsp?arnumber=10908240

[6] Victor Ojewale, et al., "Towards AI Accountability Infrastructure: Gaps and Opportunities in AI Audit Tooling," CHI Conference on Human Factors in Computing Systems (CHI '25), 27 February 2025, 26 April 2025. Available: https://arxiv.org/abs/2402.17861

[7] Alaa Haddad, et al., "Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems," IEEE Access, 14 September 2022. Available: https://ieeexplore.ieee.org/stampPDF/getPDF.jsp?arnumber=9868006

[8] Valerie J. Parker, et al., "AI Governance in Health Systems," Duke-Margolis Institute for Health Policy, October 2024. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://healthpolicy.duke.edu/sites/default/files/2024-10/AI%20Governance%20in%20Health%20Systems.pdf

[9] Ling Zhang, "Intelligent Internal Audit Platform Architecture Based on Machine Learning," 2023 IEEE International Conference on Artificial Intelligence and Autonomous Robot Systems (AIARS), 20 October 2023. Available: https://ieeexplore.ieee.org/document/10285286/references#references

[10] Raza Nowrozy, et al., "Artificial Intelligence in Enhancing Electronic Health Record Systems: A Comprehensive Survey," International Conference on Health Information Science (HIS 2024), Lecture Notes in Computer Science, Volume 15336, 16 May 2025. Available: https://link.springer.com/chapter/10.1007/978-981-96-5597-7_1

[11] Jakob Mökander, "Auditing of AI: Legal, Ethical and Technical Approaches," Digital Society, Volume 2, Article 49, 8 November 2023. Available: https://link.springer.com/article/10.1007/s44206-023-00074-y

[12] Usha Jagannathan, "Mitigating AI Risk in the Enterprise: Ethical and Transparent AI with IEEE CertifAIEd™," IEEE Standards Association, 7 March 2025. Available: https://standards.ieee.org/beyond-standards/mitigating-ai-risk-ieee-certifaied/