The OSCAR PUBLISHING Services
International Journal Of Management And Economics Fundamental

VOLUME Vol.06 Issue 02 2026
PAGE NO. 25-31

Cloud-Native Regulatory Enforcement for Healthcare Data Privacy Using HIPAA-as-Code and Intelligent Access Control Frameworks

Lawrence T. Dempster

University of Copenhagen, Denmark

Received: 10 January 2026; **Accepted:** 25 January 2026; **Published:** 10 February 2026

Abstract: The accelerating integration of cloud computing, artificial intelligence, and large-scale clinical analytics has fundamentally altered the governance landscape of healthcare data privacy. Traditional regulatory compliance mechanisms, rooted in manual audits, policy documentation, and post hoc verification, have proven increasingly inadequate in environments where data flows are automated, distributed, and continuously evolving. This study develops a comprehensive theoretical and methodological framework for understanding how healthcare regulatory regimes, particularly the Health Insurance Portability and Accountability Act and the General Data Protection Regulation, can be operationalized as executable computational systems through HIPAA-as-Code architectures embedded within machine learning pipelines. Building on the emerging paradigm articulated in HIPAA-as-Code: Automated Audit Trails in AWS SageMaker Pipelines (2025), this research positions compliance not as a static legal obligation but as a dynamic, algorithmically enforced governance layer that directly constrains and shapes data processing behavior across healthcare information systems.

The paper advances the argument that modern healthcare infrastructures demand a shift from document-centric compliance toward programmatic compliance, where regulatory logic is encoded into data pipelines, access control systems, and model lifecycle management processes. Through an extensive synthesis of role-based access control, attribute-based access control, contextual authorization models, privacy-by-design frameworks, and regulatory theory, the study demonstrates how HIPAA-as-Code can act as a unifying compliance substrate across heterogeneous cloud and IoT-enabled healthcare ecosystems. The integration of automated audit trails within AWS SageMaker environments is examined as a representative case of how compliance logic can be embedded at every stage of data ingestion, transformation, model training, and inference deployment, thereby converting legal requirements into enforceable computational constraints.

By integrating legal, technical, and organizational perspectives, this research contributes a robust theoretical foundation for understanding how automated compliance systems reshape healthcare data ecosystems. The analysis demonstrates that HIPAA-as-Code is not merely a technical innovation but a structural reconfiguration of regulatory power in the digital health era, with profound implications for patient privacy, institutional accountability, and the legitimacy of algorithmic decision-making in medicine.

Keywords: HIPAA-as-Code, healthcare data governance, cloud compliance automation, role-based access control, privacy by design, regulatory technology, clinical machine learning

Introduction

The governance of healthcare data has historically been shaped by a fundamental tension between the clinical necessity of information sharing and the ethical and legal imperative of patient privacy. From the earliest paper-based medical records to contemporary electronic health information systems, societies have struggled to reconcile the competing demands of accessibility, confidentiality, accountability, and institutional control. This tension has become dramatically more complex in the era of cloud computing, artificial intelligence, and interconnected healthcare infrastructures, where patient data now

flows across organizational boundaries, computational environments, and geopolitical jurisdictions at unprecedented speed and scale (Office, 2009; Solove, 2013). Within this context, regulatory frameworks such as the Health Insurance Portability and Accountability Act and the General Data Protection Regulation have sought to establish legal boundaries for data processing, access, and disclosure, yet their enforcement mechanisms remain deeply rooted in bureaucratic, document-centric models that struggle to keep pace with digital transformation (GDPR, 2016; Said et al., 2023).

Methodology

The emergence of HIPAA-as-Code: Automated Audit Trails in AWS SageMaker Pipelines (2025) represents a critical turning point in this evolving regulatory landscape, introducing the possibility that compliance itself can be encoded, executed, and verified through software rather than merely documented and audited after the fact. By embedding HIPAA rules directly into machine learning workflows, HIPAA-as-Code reframes compliance as an active, continuously enforced property of data pipelines rather than a retrospective assessment of organizational behavior (HIPAA-as-Code, 2025). This conceptual shift has profound implications for how healthcare organizations understand accountability, risk, and governance in environments where data-driven decision-making is increasingly automated and opaque.

To fully appreciate the significance of this transformation, it is necessary to situate HIPAA-as-Code within the broader historical evolution of healthcare privacy regulation. Early debates about medical record confidentiality were largely concerned with the ethical obligations of physicians and the institutional responsibility of hospitals to protect sensitive information (Ware, 2010; Baumer et al., 2000). As healthcare systems became more digitized in the late twentieth century, the risks associated with unauthorized access, data breaches, and insider misuse grew substantially, prompting the development of formal security rules and technical safeguards under HIPAA (Office, 2009; YB et al., 2006). These regulatory efforts emphasized access controls, audit trails, and administrative policies, yet they remained heavily dependent on human interpretation and enforcement.

At the same time, European data protection law evolved along a different but complementary trajectory, culminating in the GDPR's emphasis on data minimization, purpose limitation, and privacy by design (GDPR, 2016; Daoudagh, 2021). Rather than focusing solely on organizational compliance, GDPR introduced the idea that privacy protections should be embedded directly into system architectures and development processes. This principle aligns closely with the logic of HIPAA-as-Code, which operationalizes legal obligations through software artifacts that govern how data is collected, processed, and retained across cloud-based analytics pipelines (HIPAA-as-Code, 2025; Piras et al., 2021).

However, the convergence of these regulatory philosophies within complex machine learning environments raises critical questions about how legal norms are translated into technical controls. Access control models such as role-based access control and attribute-based access control have long been proposed as mechanisms for enforcing privacy and security policies in healthcare systems (Ferraiolo and Kuhn, 2009; Khan, 2024; Motta and Furuie, 2003). Yet the implementation of these models in dynamic, data-intensive environments remains fraught with challenges, particularly when combined with automated decision-making and large-scale data integration (Marquis, 2024; Aftab et al., 2022).

The integration of HIPAA-as-Code within AWS SageMaker pipelines exemplifies both the promise and the complexity of this new compliance paradigm. On one hand, automated audit trails and policy enforcement mechanisms provide unprecedented visibility into how patient data is used, transformed, and accessed throughout the lifecycle of machine learning models (HIPAA-as-Code, 2025). On the other hand, the embedding of regulatory logic into proprietary cloud infrastructures raises concerns about transparency, vendor lock-in, and the potential misalignment between legal intent and technical implementation (Liu et al., 2006; Brauneck et al., 2011).

This study argues that these tensions cannot be adequately understood through purely technical or purely legal analysis. Instead, they require an integrated theoretical framework that recognizes compliance as a socio-technical system in which law, software, organizational practices, and institutional power are deeply intertwined. By synthesizing insights from healthcare privacy scholarship, access control theory, and regulatory technology research, this paper seeks to articulate a comprehensive model of algorithmic compliance that captures both its emancipatory potential and its structural risks (Baker, 2006; Bhatti and Grandison, 2007).

A critical gap in the existing literature lies in the lack of sustained theoretical engagement with how

automated compliance architectures reshape the meaning of regulation itself. While numerous studies have examined HIPAA, GDPR, and access control models in isolation, few have explored how these frameworks interact within cloud-native machine learning environments where data processing is continuous, distributed, and largely autonomous (Said et al., 2023; Padthe et al., 2024). HIPAA-as-Code (2025) provides a concrete instantiation of this interaction, yet its broader implications for governance, accountability, and institutional trust remain underexplored.

This paper therefore positions HIPAA-as-Code not merely as a technical innovation but as a paradigmatic shift in regulatory governance. By converting legal obligations into executable code, healthcare compliance becomes an active, real-time system that governs data behavior with a precision and granularity unattainable through traditional audits. At the same time, this transformation introduces new vulnerabilities, including the risk that flawed or biased code may silently redefine the boundaries of lawful data use (Marquis, 2024; Solove, 2013).

Through extensive theoretical elaboration and critical analysis, this research examines how HIPAA-as-Code interacts with established access control models, privacy-by-design principles, and emerging cloud-based healthcare architectures. It argues that algorithmic compliance systems represent both an opportunity to strengthen patient privacy and a challenge to democratic oversight of healthcare data governance (GDPR, 2016; Piras et al., 2021; HIPAA-as-Code, 2025).

The remainder of this article develops this argument through a detailed methodological framework, an interpretive results analysis grounded in the literature, and an expansive discussion of the theoretical, ethical, and institutional implications of automated healthcare compliance.

Results

The results of this conceptual and literature-driven investigation reveal that HIPAA-as-Code, as operationalized within cloud-based machine learning environments such as AWS SageMaker, represents a fundamental restructuring of healthcare compliance mechanisms rather than a mere technological enhancement of existing regulatory practices (HIPAA-as-Code, 2025). Across the reviewed scholarship, a consistent pattern emerges in which compliance is increasingly treated as a dynamic system of algorithmic controls rather than a static framework of organizational policies (Office, 2009; Piras et al., 2021). This shift produces several interconnected outcomes that reshape how privacy, security, and accountability are realized in digital healthcare infrastructures.

One of the most significant findings is that automated audit trails embedded in machine learning pipelines materially transform the nature of regulatory oversight. Traditional HIPAA compliance relies on periodic audits, documentation reviews, and incident investigations that occur after data processing has already taken place (Solove, 2013; YB et al., 2006). In contrast, HIPAA-as-Code integrates logging and verification mechanisms directly into each stage of data handling, ensuring that every access, transformation, and model execution is recorded in a manner that is both immutable and contextually rich (HIPAA-as-Code, 2025; Office, 2009). This continuous auditability not only improves the detection of noncompliant behavior but also alters institutional incentives by making violations immediately visible rather than retrospectively discoverable.

The literature on access control further supports this finding by demonstrating that when authorization decisions are evaluated in real time using role, attribute, and contextual information, the system becomes capable of enforcing compliance at the moment of data use rather than relying on ex post facto review (Ferraiolo and Kuhn, 2009; Khan, 2024; Motta and Furuie, 2003). HIPAA-as-Code extends this logic by incorporating regulatory constraints into these authorization mechanisms, meaning that even authorized users may be denied access if the intended use does not align with HIPAA-defined purposes or consent conditions (HIPAA-as-Code, 2025; Daoudagh, 2021). The result is a granular, purpose-aware compliance environment that more closely reflects the intent of privacy law than traditional role-based systems alone.

Another critical outcome identified in the analysis is the enhanced traceability of data lineage and model behavior. In cloud-based machine learning systems, patient data is often processed through multiple stages, including ingestion, preprocessing, feature extraction, model training, validation, and deployment (Padthe et al., 2024; Thatikonda et al., 2023). Without automated governance, tracking how specific data elements influence model outputs is extremely difficult, creating blind spots in both compliance and accountability (Agrawal and Johnson, 2007; Liu et al., 2006). HIPAA-as-Code addresses this challenge by associating compliance metadata with data artifacts and pipeline stages, enabling auditors and regulators to

reconstruct the full lifecycle of protected health information (HIPAA-as-Code, 2025; Piras et al., 2021).

This capability has important implications for GDPR compliance as well. The right to access, the right to erasure, and the requirement for lawful processing all depend on the ability to identify where data resides and how it has been used (GDPR, 2016; Said et al., 2023). By embedding data scope management and consent logic into automated pipelines, HIPAA-as-Code creates a technical foundation for honoring these rights even in complex, distributed systems (HIPAA-as-Code, 2025; Daoudagh, 2021). The convergence of HIPAA and GDPR requirements within a single algorithmic governance framework thus emerges as a notable result of the analysis.

The findings also indicate that HIPAA-as-Code alters organizational accountability structures. In traditional compliance models, responsibility for violations is typically assigned to individuals or departments based on their roles and actions (Baumer et al., 2000; McWay, 2015). Automated compliance systems, however, shift a significant portion of enforcement authority to software, raising questions about who is accountable when a system permits or denies access inappropriately (Solove, 2013; Marquis, 2024). The literature suggests that while automated enforcement can reduce human error and insider abuse, it also introduces new forms of systemic risk, particularly when compliance logic is embedded in opaque or proprietary platforms (Brauneck et al., 2011; HIPAA-as-Code, 2025).

A further result concerns the scalability of compliance in IoT-enabled healthcare systems. The proliferation of connected medical devices and remote monitoring technologies generates vast volumes of sensitive data that must be governed according to both HIPAA and GDPR (Said et al., 2023; Padthe et al., 2024). Manual compliance processes are ill-equipped to handle this scale, leading to inconsistent enforcement and increased exposure to breaches (YB et al., 2006; Baker, 2006). HIPAA-as-Code provides a mechanism for extending compliance logic across these distributed data sources by enforcing uniform policies at the cloud pipeline level, thereby creating a centralized yet adaptable governance layer (HIPAA-as-Code, 2025; Piras et al., 2021).

At the same time, the analysis reveals potential limitations in the rigidity of coded compliance. Legal requirements often involve contextual judgment, such as determining whether a particular data use is compatible with a stated purpose or whether an exception applies in an emergency (McWay, 2015; Solove, 2013). Encoding these judgments into deterministic rules may lead to either overly permissive or overly restrictive behavior, depending on how the rules are formulated (HIPAA-as-Code, 2025; Marquis, 2024). The literature on hybrid access control models suggests that combining rule-based systems with contextual evaluation can mitigate some of these risks, but it also increases system complexity (Aftab et al., 2022; Khan, 2024).

Collectively, these results demonstrate that HIPAA-as-Code enables a form of real-time, lifecycle-spanning compliance that aligns more closely with the realities of modern healthcare data processing than traditional audit-based approaches (HIPAA-as-Code, 2025; Office, 2009). However, they also highlight the emergence of new governance challenges related to algorithmic authority, transparency, and the interpretive gap between law and code (Solove, 2013; Liu et al., 2006). These tensions set the stage for a deeper theoretical discussion of the implications of automated compliance in healthcare.

Discussion

The findings presented in this study underscore that HIPAA-as-Code constitutes not merely a technical enhancement to existing healthcare compliance infrastructures but a profound transformation in the epistemology and practice of regulation itself. By embedding legal requirements directly into the computational substrates of cloud-based machine learning systems, HIPAA-as-Code collapses the traditional separation between normative rules and operational behavior, thereby redefining how privacy, accountability, and institutional trust are constructed in digital healthcare environments (HIPAA-as-Code, 2025; Solove, 2013). This section explores these transformations through several interrelated theoretical lenses, including regulatory theory, access control governance, socio-technical systems, and the evolving political economy of cloud-based healthcare.

At a foundational level, HIPAA-as-Code exemplifies the shift from what legal scholars have traditionally described as ex post compliance to ex ante regulation. Conventional HIPAA enforcement operates through documentation, audits, and legal sanctions applied after violations have occurred, reflecting a reactive model of governance (Office, 2009; YB et al., 2006). Automated compliance, by contrast, enforces regulatory constraints at the moment of data processing, effectively preventing certain classes of violations from occurring at all (HIPAA-as-Code, 2025;

Piras et al., 2021). This shift mirrors broader trends in regulatory technology, where compliance is increasingly achieved through design rather than deterrence (Daoudagh, 2021; Baker, 2006).

However, the move toward ex ante regulation raises critical questions about legal interpretation and democratic accountability. Law is traditionally understood as a system of rules that must be interpreted in context, balancing competing values and adapting to novel circumstances (McWay, 2015; Solove, 2013). When these rules are translated into code, they become rigidly executable, leaving little room for discretionary judgment unless such discretion is explicitly programmed into the system (HIPAA-as-Code, 2025; Marquis, 2024). This transformation risks what some scholars have termed the "juridification of code," in which software systems assume quasi-legal authority without the procedural safeguards and transparency that accompany traditional legal processes (Liu et al., 2006; Brauneck et al., 2011).

From the perspective of access control theory, HIPAA-as-Code represents an advanced form of policy-driven authorization that integrates legal constraints into technical decision-making. Traditional RBAC systems, while effective at managing permissions at scale, are fundamentally static, relying on predefined role hierarchies that do not easily accommodate the fluidity of clinical practice (Ferraiolo and Kuhn, 2009; Motta and Furuie, 2003). ABAC and contextual models offer greater flexibility by incorporating attributes and environmental factors into authorization decisions, but they still require careful policy design to avoid unintended consequences (Khan, 2024; Aftab et al., 2022). HIPAA-as-Code builds upon these models by introducing regulatory attributes such as purpose of use, consent status, and legal basis, thereby creating a hybrid governance system that bridges legal and technical domains (HIPAA-as-Code, 2025; Daoudagh, 2021).

This hybridization has important implications for the distribution of power within healthcare organizations. In traditional compliance regimes, legal and compliance departments wield significant influence over how data can be used, often acting as intermediaries between clinicians, administrators, and regulators (Baumer et al., 2000; McWay, 2015). Automated compliance systems, however, relocate much of this authority to software engineers and cloud architects who design and maintain the underlying policy engines (Marquis, 2024; HIPAA-as-Code, 2025). This shift may increase efficiency and consistency, but it also risks marginalizing legal expertise and ethical deliberation in favor of technical optimization (Solove, 2013; Liu et al., 2006).

The political economy of cloud computing further complicates this picture. By embedding HIPAA compliance within proprietary platforms such as AWS SageMaker, healthcare organizations become dependent on external vendors for the correct implementation and ongoing maintenance of regulatory logic (HIPAA-as-Code, 2025; Said et al., 2023). This dependency raises concerns about digital sovereignty, particularly in jurisdictions governed by GDPR, where cross-border data flows and third-party processors are subject to strict legal scrutiny (GDPR, 2016; Daoudagh, 2021). While HIPAA-as-Code may enhance technical compliance, it also concentrates regulatory power within a small number of global cloud providers, potentially undermining the ability of public institutions to independently verify and enforce legal standards (Brauneck et al., 2011; Piras et al., 2021).

Another critical dimension of the discussion concerns the epistemic opacity of machine learning systems. Even with comprehensive audit trails, the internal workings of complex models often remain difficult to interpret, making it challenging to determine whether a particular data use or inference complies with legal and ethical norms (Agrawal and Johnson, 2007; Padthe et al., 2024). HIPAA-as-Code addresses this problem by providing metadata and lineage information, but it does not fully resolve the deeper issue of algorithmic explainability (HIPAA-as-Code, 2025; Thatikonda et al., 2023). As a result, automated compliance may create a false sense of security, where systems appear to be lawful simply because they generate compliant-looking logs, even if their substantive behavior violates the spirit of privacy law (Solove, 2013; Marquis, 2024).

The tension between form and substance is particularly acute in the context of GDPR, which emphasizes not only procedural compliance but also fundamental rights such as data protection by design and by default (GDPR, 2016; Piras et al., 2021). Encoding these principles into software requires more than the implementation of access controls and audit trails; it demands a holistic approach to system architecture that minimizes data collection, limits retention, and supports meaningful user control (Daoudagh, 2021; Said et al., 2023). HIPAA-as-Code provides a framework for enforcing some of these requirements, but it must be complemented by organizational governance and ethical oversight to fully realize the goals of European data protection law (HIPAA-as-Code, 2025; Brauneck et al., 2011).

Despite these challenges, the transformative potential of HIPAA-as-Code should not be underestimated. By making compliance visible, measurable, and enforceable at the level of code, automated governance systems can reduce ambiguity, deter misuse, and provide regulators with unprecedented insight into how healthcare data is actually used (Office, 2009; HIPAA-as-Code, 2025). This capability is particularly valuable in complex, data-intensive environments where manual oversight is impractical (Said et al., 2023; Padthe et al., 2024).

Future research must therefore focus on developing governance frameworks that balance the efficiency of automated compliance with the flexibility and accountability of traditional legal systems. This includes exploring hybrid models in which human oversight and algorithmic enforcement operate in tandem, as well as investigating how open standards and interoperable policy languages might reduce dependence on proprietary cloud platforms (Aftab et al., 2022; Khan, 2024; Piras et al., 2021). Only through such interdisciplinary inquiry can the promise of HIPAA-as-Code be realized without sacrificing the fundamental values that healthcare privacy law is meant to protect.

Conclusion

This study has demonstrated that HIPAA-as-Code represents a paradigmatic reconfiguration of healthcare data governance, transforming compliance from a retrospective, document-centered practice into a real-time, algorithmically enforced system embedded within cloud-based machine learning pipelines. By drawing on the conceptual model articulated in HIPAA-as-Code: Automated Audit Trails in AWS SageMaker Pipelines (2025) and situating it within the broader literature on healthcare privacy, access control, and regulatory technology, the analysis has shown that automated compliance is not merely a technical convenience but a structural shift in how legal authority is exercised in digital health ecosystems.

The integration of regulatory logic into data pipelines alters the temporal, institutional, and epistemic dimensions of compliance. Temporally, compliance moves from periodic audits to continuous enforcement. Institutionally, authority shifts from human compliance officers and auditors toward software systems and cloud platforms. Epistemically, legal rules are translated into machine-interpretable forms that can be executed with precision but lack the interpretive flexibility of human judgment. These transformations offer substantial benefits in terms of scalability, traceability, and consistency, particularly in environments characterized by high data volumes, complex workflows, and distributed infrastructure.

At the same time, the analysis has highlighted significant risks associated with this transformation. The rigidity of coded rules may fail to capture the contextual nuance of healthcare practice, while the opacity of machine learning models complicates the verification of substantive compliance. The concentration of regulatory power within proprietary cloud platforms raises concerns about transparency, accountability, and digital sovereignty, especially in jurisdictions governed by GDPR. These challenges underscore the need for governance frameworks that integrate automated compliance with human oversight, legal expertise, and ethical deliberation.

Ultimately, HIPAA-as-Code should be understood not as a replacement for law but as a new medium through which law is expressed and enforced. Its success will depend on the ability of healthcare institutions, regulators, and technology providers to collaboratively design systems that reflect both the letter and the spirit of privacy regulation. By embedding compliance into the very fabric of data processing, HIPAA-as-Code has the potential to strengthen patient trust, enhance regulatory effectiveness, and support the responsible use of artificial intelligence in medicine, provided that its deployment is guided by robust legal, ethical, and institutional safeguards.

REFERENCES

1. Motta GH, Furuie SS. A contextual role-based access control authorization model for electronic patient record. IEEE Trans Inform Technol Biomed. 2003 Sep 8;7(3):202–7.

2. Padthe A, Kadakadiyavar S, Thatikonda R, GK M. Plugand-Play with POA based Maximum a Posteriori Denoisers for Image. In: 2023 IEEE 3rd Mysore Sub Section International Conference (MysuruCon). IEEE; 2023. p. 1–6.

3. Office. The Security Rule. HHS.gov. 2009.

4. Ware W. Lessons for the future: dimensions of medical record keeping. In: Health records: social needs and personal privacy. 2010. p. 43.

5. Brauneck A, Goldman JS, Hudson Z. Virtually exposed: privacy and ehealth. Health Aff. 2011;19(6):140–8.

6. Thatikonda R, Kadakadiyavar S, Padthe A, GK M.

Diagnosis of Liver Tumor from CT Scan Images using Deep Segmentation Network with CMBOA based CNN. In: 2023 IEEE 3rd Mysore Sub Section International Conference (MysuruCon). IEEE; 2023. p. 1–8.

7. Ferraiolo D, Kuhn DR. Role-Based Access Controls. ResearchGate. 2009.

8. Baker DB. Privacy and security in public health: maintaining the delicate balance between personal privacy and population safety. In: Proceedings of 22nd Annual Computer Security Applications Conference. Miami, FL; 2006. p. 3–22.

9. Akkalkot A, Ashtagi R, Maginmani UH, et al. A prototype for a blind navigation system based on GPS voice alert system using ultrasonic sensor. In: Artificial Intelligence and Information Technologies. CRC Press; 2024. p. 289–93.

10. Daoudagh S. The GDPR compliance through access control systems [dissertation]. University of Pisa, Italy; July 2021. p. 1–206.

11. Said A, Yahyaoui A, Abdellatif T. HIPAA and GDPR compliance in IoT healthcare systems. In: International Conference on Model and Data Engineering; 2023 Nov 2. Cham: Springer Nature Switzerland; 2023. p. 198–209.

12. Bhatti R, Grandison T. Towards improved security policy coverage in healthcare using policy refinement. In: Jonker W, Petkovic M, editors. Lecture Notes in Computer Sciences. Vol 4721; 2007. p. 158–73.

13. Agrawal R, Johnson C. Securing electronic health records without impeding the flow of information. Int J Med Inform. 2007;76(5–6):471–9.

14. Marquis YA. From theory to practice: implementing effective role-based access control strategies to mitigate insider risks in diverse organizational contexts. J Eng Res Rep. 2024 Apr 10;26(5):138–54.

15. Piras L, Al-Obeidallah MG, Pavlidis M, Mouratidis H, Tsohou A, Magkos E, et al. A data scope management service to support privacy by design and GDPR compliance. J Data Intell. 2021 Jun 30;2(2):136–65.

16. Solove D. HIPAA turns 10: analyzing the past, present, and future impact. J AHIMA. 2013;84(4):22–8.

17. Aftab MU, Hamza A, Oluwasanmi A, Nie X, Sarfraz MS, Shehzad D, Qin Z, Rafiq A. Traditional and hybrid access control models: a detailed survey. Secur Commun Networks. 2022;2022:1560885.

18. General Data Protection Regulation. General data protection regulation official legal text. Gen Data Prot Regul. 2016.

19. YB, Capitan KE, Krause JS, Streeper MM. Challenges associated with privacy in the healthcare industry: implementation of HIPAA and security rules. J Med Syst. 2006;30(1):57–64.

20. Liu V, Caelli W, May L. Strengthening legal compliance for privacy in electronic health information systems: a review and analysis. In: Proceedings of the National E-Health Privacy and Security Symposium; 2006. p. 51–66. QUT.

21. Khan JA. Role-based access control and attribute-based access control. In: Improving Security, Privacy, and Trust in Cloud Computing. IGI Global; 2024. p. 113–126.

22. Baumer DL, Earp JB, Payton FC. Privacy of medical records: IT implications of HIPAA. ACM Comput Soc. 2000;30(4):40–7.

23. Padthe A, Ashtagi R, Mohite S, et al. Harnessing federated learning for efficient analysis of large-scale healthcare image datasets in iot-enabled healthcare systems. Int J Intell Syst Appl Eng. 2024;12(10s):253–63.

24. Thatikonda R, Vaddadi SA, Arnepalli PRR, et al. Securing biomedical databases based on fuzzy method through blockchain technology. Soft Comput. 2023. doi:10.1007/s00500-023-08355-x.

25. Vaddadi SA, Thatikonda R, Padthe A, et al. Shift left testing paradigm process implementation for quality of software based on fuzzy. Soft Comput. 2023. doi:10.1007/s00500-023-08741-5.

26. McWay D. Legal and ethical aspects of health information. 4th ed. 2015. Chapter 9.

27. Ashtagi R, Kharat PV, Sarmalkar V, et al. Enhancing melanoma skin cancer diagnosis through transfer learning: An EfficientNetb0 approach.