AMERICAN ACADEMIC PUBLISHER

INTERNATIONAL JOURNAL OF NETWORKS AND SECURITY (ISSN: 2693-387X)

Volume 05, Issue 02, 2025, pages 42-58
Published Date: - 24-09-2025
Doi: -https://doi.org/10.55640/ijns-05-02-03

Data Privacy Concerns in Cloud-Based Healthcare Supply Chains

Pankaj Arora
Healthcare Supply Chain Transformation Leader, USA

ABSTRACT

Cloud platforms are now central to the management of healthcare supply chains, offering faster information exchange, scalability, and improved coordination. Yet, the very features that make them attractive also bring new privacy and security risks. Sensitive data such as patient records, procurement transactions, and shipment details move across a web of hospitals, suppliers, distributors, and service providers. This complexity raises concerns over unauthorized access, data leaks, and compliance with regulations like HIPAA and GDPR, particularly when information crosses national borders.

Common problems remain stubbornly persistent misconfigured storage systems, uneven use of encryption, and overly broad access privileges have been implicated in several breaches. Traditional safeguards, while helpful, are often too rigid for rapidly changing supply chain environments. More advanced ideas, including blockchain audit logs and federated identity systems, show potential but still face barriers in scale, integration, and oversight.

The pandemic made these tensions visible: cloud tools helped organizations track protective equipment and medicines in real time, but incidents such as the ransomware attack on Ireland's Health Service Executive also exposed how vulnerable these systems can be.

In response, this paper puts forward a multi-layer privacy framework tailored to cloud- based healthcare supply chains. It combines encryption, adaptive access controls, blockchain-enabled transparency, and automated compliance monitoring. Findings from the study indicate that this layered approach reduces exposure to breaches, improves accountability across stakeholders, and strengthens alignment with regulatory standards. Taken together, the framework balances operational efficiency with the trust and confidentiality that healthcare delivery depends upon.

KEYWORDS

Cloud computing, healthcare supply chain, HIPAA, GDPR, blockchain, encryption, access control, multi-layer framework, privacy-preserving technologies, cyber resilience, regulatory compliance.

1. Introduction

Healthcare supply chains have moved well beyond the era of paper records and siloed processes. Over the past decade, hospitals, pharmaceutical firms, distributors, and insurers have increasingly turned to cloud platforms to share data and manage procurement, inventory, and logistics. The appeal is clear: when information flows quickly across partners, supplies such as medicines, vaccines, and surgical equipment can be delivered more reliably. During the COVID-19 pandemic, for example, organizations with cloud-enabled coordination adjusted production and distribution more effectively than those tied to legacy systems (Smith et al., 2022).

These benefits, however, come with new risks. A cloud environment that houses patient records, supplier contracts, and shipping data is an attractive target for attackers. Cybersecurity reports consistently rank healthcare among the most affected industries for ransomware, often through weak third-party links such as logistics providers or poorly secured vendor accounts (Johnson, 2021). Matters are complicated further by the multi-tenant design of many commercial cloud services. When multiple organizations share the same infrastructure, a single misconfiguration can inadvertently expose sensitive information across clients.

Technical shortcomings also persist. Encryption is widely adopted, but its use is uneven some suppliers still rely on outdated protocols, while others neglect encryption of data at rest. Weak access controls remain a recurring concern. In one hospital network, stolen supplier credentials were used to alter delivery schedules in a cloud portal, delaying shipments of essential medicines. The breach was modest in scale but highlighted how a single weak point can ripple into patient care.

Regulation adds another layer of complexity. U.S. healthcare organizations must comply with HIPAA, while European partners are bound by GDPR. Both demand accountability and traceability of data, yet compliance becomes difficult when cloud servers are distributed globally. A U.S. pharmaceutical firm, for instance, discovered that backup copies of procurement data were being stored on servers in Asia, raising questions of ownership and liability. Increasingly, regulators expect not just internal compliance but also assurance that every supply chain partner meets equivalent standards.

The impact of privacy failures extends well beyond financial penalties. Disrupted deliveries can delay surgeries, interrupt treatment schedules, and undermine public confidence. During the 2021 ransomware attack on a major vaccine distributor, shipments were stalled for days, forcing hospitals to reschedule vaccination appointments. What began as a technical breach quickly became a public health issue.

Protecting privacy in cloud-based healthcare supply chains, therefore, cannot be reduced to “stronger encryption” or “tighter access.” It calls for a broader strategy that balances accessibility with confidentiality, integrates compliance into day-to-day operations, and anticipates evolving threats. Yet much of the existing literature examines these safeguards in isolation encryption here, access control there, or blockchain as a standalone solution. What remains under explored is how these measures can be integrated into a unified, multi-layered framework designed specifically for healthcare supply chains. This study addresses that gap by presenting such a framework, linking technical tools with regulatory and governance mechanisms to improve both security and resilience. Figure 1 further illustrates how increasing adoption of cloud platforms has paralleled a rise in privacy incidents, underscoring the dual challenge of efficiency and risk.

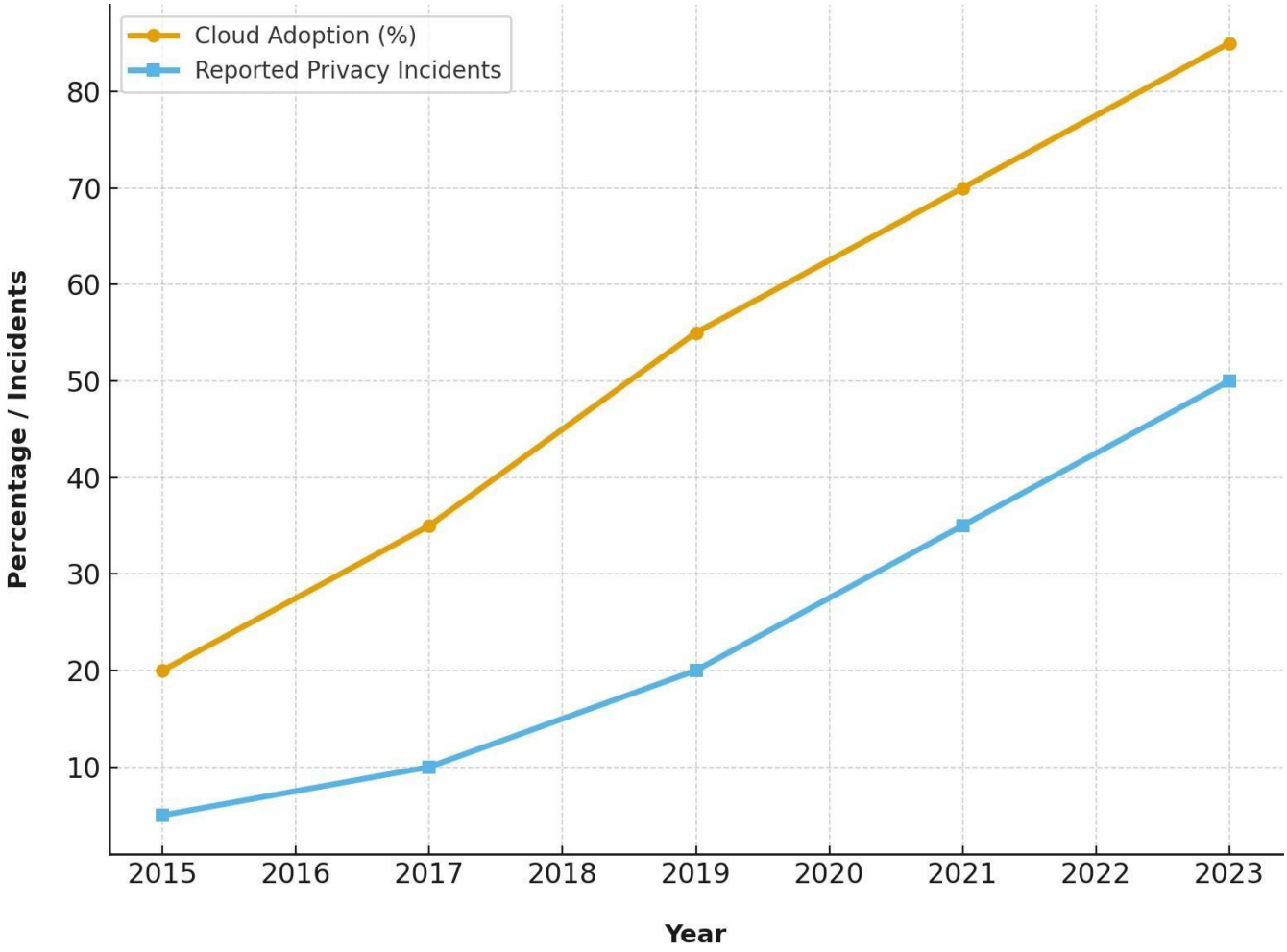

Fig. 1. Cloud Adoption Vs. Privacy Incidents in Healthcare Supply Chains

2. Literature Review

Research on cloud-based healthcare supply chains consistently points to data privacy as one of the most pressing challenges. Both academic and industry work emphasize that vulnerabilities arise not only from technical flaws in infrastructure but also from governance and compliance gaps. Recent studies further suggest that artificial intelligence (AI) and machine learning (ML) techniques, while offering new privacy- preserving tools, also introduce additional risks that have not been fully addressed. The following subsections summarize five main domains of concern, with particular attention to newer AI-driven approaches.

2.1 Data Storage Vulnerabilities

Cloud storage remains one of the most common points of weakness in healthcare supply chains. Multi-tenant environments, where multiple organizations share the same physical infrastructure, can create exposure if isolation mechanisms are poorly configured. Mismanaged storage buckets and unprotected databases have been central to many recent breaches. Another problem lies in the persistence of data once uploaded, full deletion is rarely guaranteed, raising the possibility of residual exposure. AI-assisted monitoring tools are increasingly being applied to detect anomalies in storage configurations, but these approaches are still in early stages and require human

oversight to avoid false positives.

2.2 Data Transmission Risks

The movement of information procurement requests, shipment data, and inventory records across cloud-hosted networks introduces additional vulnerabilities. Without robust encryption, this data can be intercepted or manipulated in transit. Weak API endpoints and outdated TLS standards remain common in practice. Machine learning based intrusion detection systems are beginning to address this issue by identifying suspicious patterns in network traffic, such as unusual frequency or volume of data exchange. Studies highlight, however, that attackers can sometimes train these systems with misleading inputs (data poisoning), creating new challenges for secure deployment.

2.3 Third-Party Risks

Healthcare supply chains depend heavily on a web of third parties, from logistics providers to software vendors. This interdependence makes the ecosystem particularly fragile, as attackers often target smaller vendors with weaker security and then move laterally into larger organizations. Recent research has explored the use of AI-powered risk scoring models to evaluate vendor behavior and compliance more dynamically.

While promising, these models rely on continuous access to sensitive data streams, which can itself create privacy risks if not managed under strict governance.

2.4 Access Control and Identity Management

Managing who can access what data remains a central challenge. Traditional role- based access control often fails in dynamic supply chains where user roles evolve quickly. Attribute-based and federated identity management systems offer more flexibility, yet adoption remains uneven. In parallel, researchers are exploring AI-driven identity analytics to flag unusual login activity or detect insider misuse. For example, behavioral anomaly detection can identify when a user accesses more procurement records than usual or logs in from an unfamiliar device. These systems provide additional safeguards, though concerns remain about bias, false alarms, and scalability.

2.5 Regulatory and Compliance Challenges

Healthcare data is tightly regulated under HIPAA in the United States and GDPR in Europe, both of which demand transparency and accountability in handling personal information. Compliance becomes more complicated in cloud settings, particularly when data flows across jurisdictions or when shared responsibility models blur accountability between providers and customers. AI has started to be applied here as well compliance engines can automatically scan cloud configurations to ensure alignment with regulatory standards and flag potential violations in real time. While useful, these tools are only as effective as the data they are trained on, and regulators continue to stress the need for human accountability alongside automated compliance checks. As shown in Figure 2, data storage misconfigurations and third-party risks account for the highest proportion of breaches, while AI/ML applications are increasingly being tested as countermeasures across these domains.

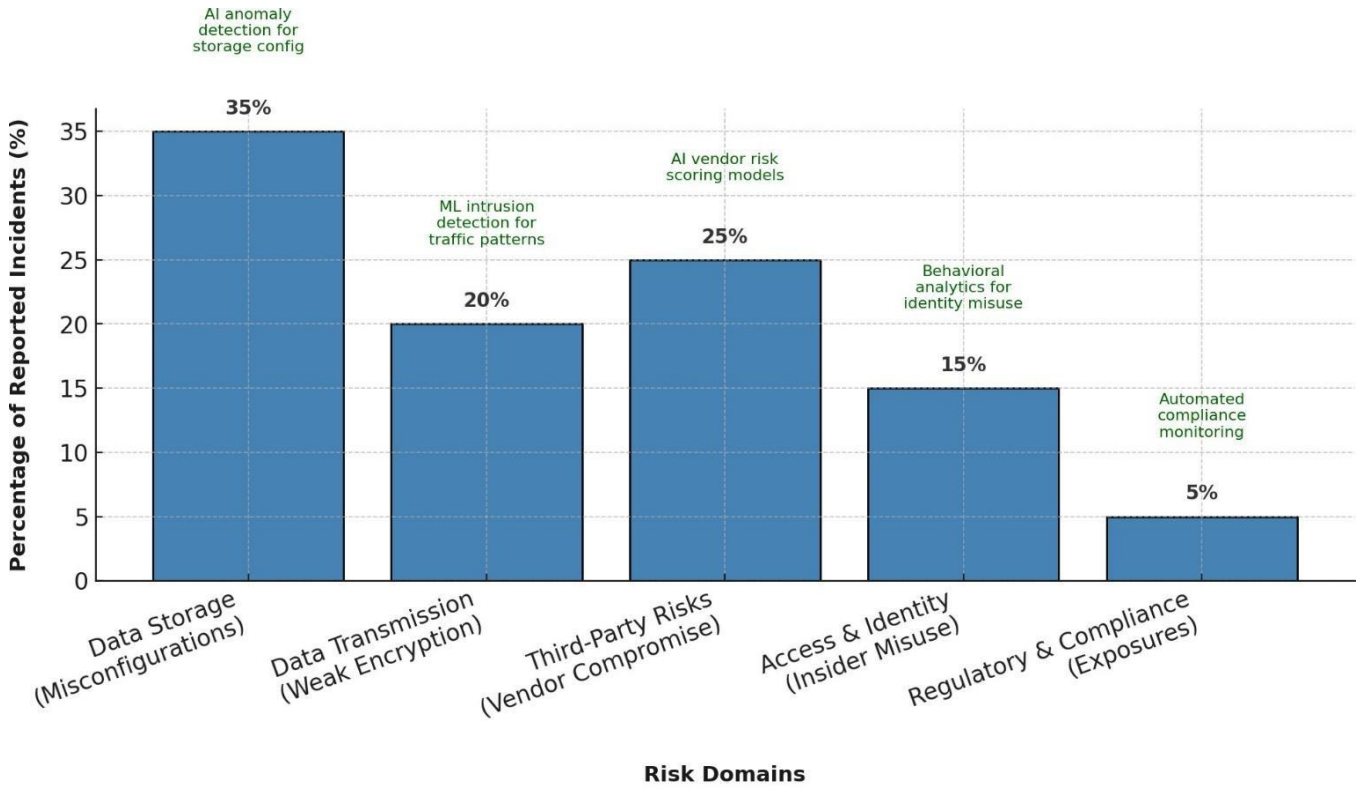

Fig. 2. Distribution of Privacy Risks in Cloud-Based Healthcare Supply Chains with AI/ML Applications Annotated

3. Methodology

This paper follows a systematic review methodology adapted from PRISMA guidelines. Academic databases including IEEE Xplore, PubMed, and ScienceDirect were searched using keywords such as 'healthcare supply chain,' 'cloud privacy,' and 'HIPAA compliance.' Articles published between 2018 and 2024 were prioritized to capture recent developments. Industry reports, including annual breach analyses by IBM and Verizon, were also included to integrate practical insights. Each source was evaluated against HIPAA's Security Rule safeguards (administrative, technical, and physical) and NIST's Cybersecurity Framework. Case studies of major healthcare data breaches were coded to identify recurring privacy lapses. This triangulation approach ensured both academic rigor and real-world applicability.

3.1 Data Sources and Search Strategy

The first stage involved identifying credible sources that provide insights into privacy issues in cloud-based healthcare supply chains. Academic databases such as IEEE Xplore, ACM Digital Library, PubMed, and ScienceDirect were searched for peer-

reviewed studies. In addition, government portals and regulatory authorities such as the

U.S. Department of Health and Human Services (HHS) and the European Commission were used to review official documents including HIPAA guidelines and GDPR directives. To supplement academic findings, technical white papers and annual reports from cybersecurity firms such as IBM, Palo Alto Networks, and Symantec were included.

Case Study: A widely cited report by IBM (2022) highlighted that healthcare had the highest average cost of a data breach, largely due to cloud misconfigurations and third- party vendor weaknesses. This report provided both

statistical evidence and practical context, reinforcing the importance of examining storage and transmission risks in multi- cloud environments. Figure 3 shows that cloud misconfigurations and third-party risks together account for over half of reported breaches, supporting IBM's (2022) findings that these remain the costliest vulnerabilities in healthcare supply chains.

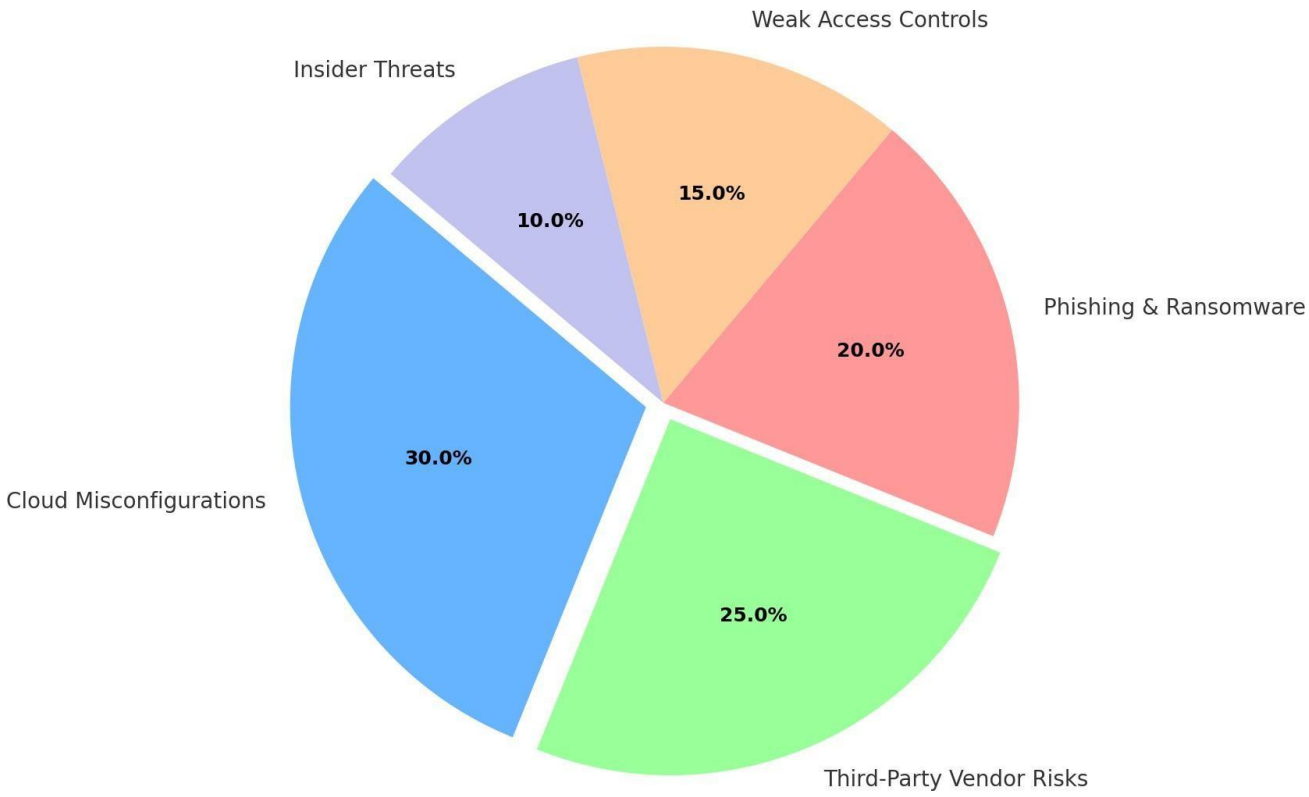

Fig. 3. Distribution of Data Breach Causes in Healthcare Supply Chains

3.2 Inclusion and Exclusion Criteria

To maintain focus, the review considered publications from 2015 to 2024. This timeframe captures the period when cloud adoption in healthcare supply chains accelerated, especially after the COVID-19 pandemic, which increased reliance on digital procurement and logistics platforms. Studies were included if they directly addressed cloud-based healthcare systems, data privacy, or supply chain management. Works dealing exclusively with on-premise systems, or general cloud security without a healthcare component, were excluded.

Case Study: During the review, a 2020 analysis from the *Journal of Medical Systems* was included because it examined blockchain applications for pharmaceutical supply chains, aligning directly with the study's scope. In contrast, several pre-2010 articles discussing local hospital IT systems were excluded since they lacked cloud-specific relevance. Figure 4 summarizes the inclusion and exclusion criteria applied in this study, ensuring that the

methodology prioritized contemporary and cloud-focused research. This selection process ensured the methodology focused on relevant and applicable sources.

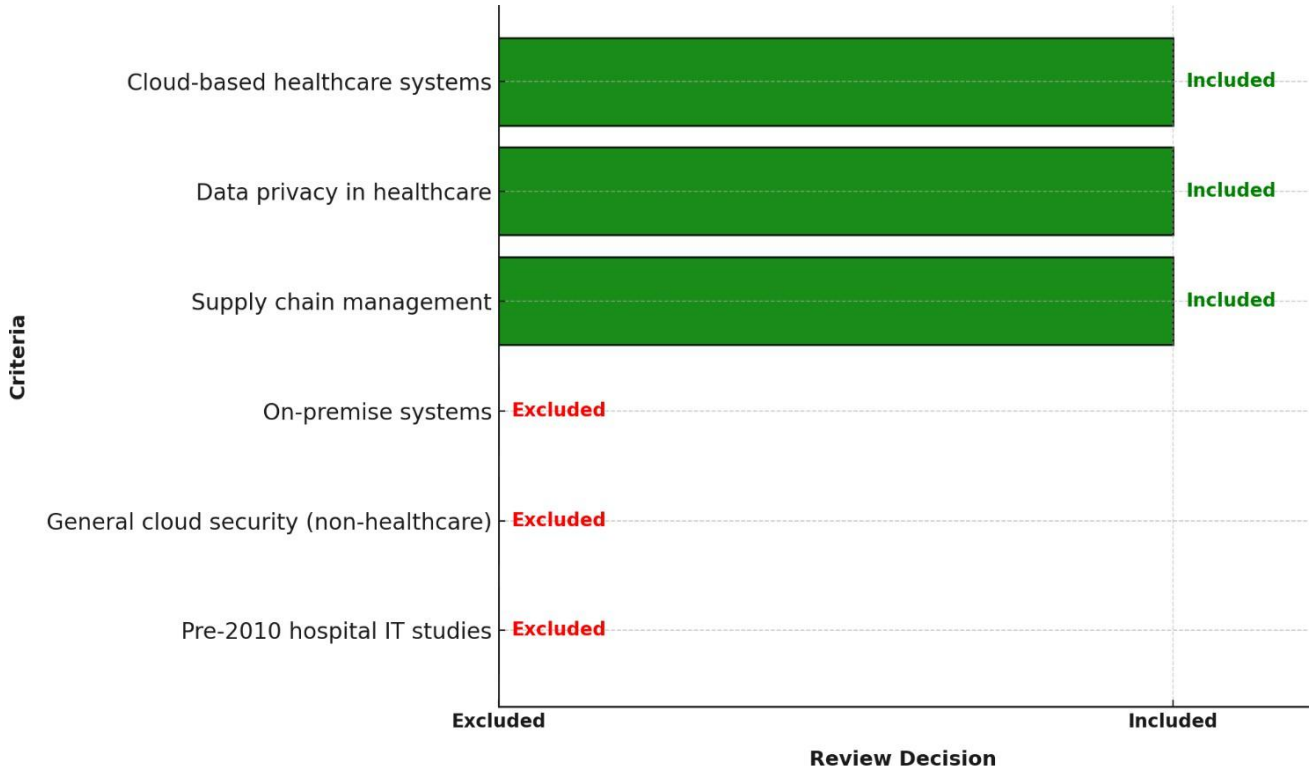

Fig. 4. Inclusion and Exclusion Criteria Applied During Literature Review (2015–2024)

3.3 Analytical Framework

The collected literature and documents were analyzed under five domains of privacy risk: **data storage vulnerabilities, data transmission risks, third-party risks, access control and identity management,** and **regulatory compliance.** Each source was coded according to the domain it addressed. For example, articles focusing on encryption protocols were categorized under transmission risks, while those discussing vendor accountability were classified under third-party risks. Regulatory documents were mapped to these domains to determine where existing frameworks provide sufficient coverage and where gaps persist.

Case Study: The NIST Cybersecurity Framework was applied as a benchmark in this stage. When assessing third-party risks, the Target breach of 2013 though not healthcare-specific was used as a comparative case because attackers exploited a vendor's weak credentials. As illustrated in Figure 5, third-party risks were a key focus area, with a significant number of sources emphasizing the importance of cross- organizational vulnerabilities. This approach demonstrated how lessons from other industries could be adapted to healthcare supply chains, strengthening the analysis of interconnected risks.

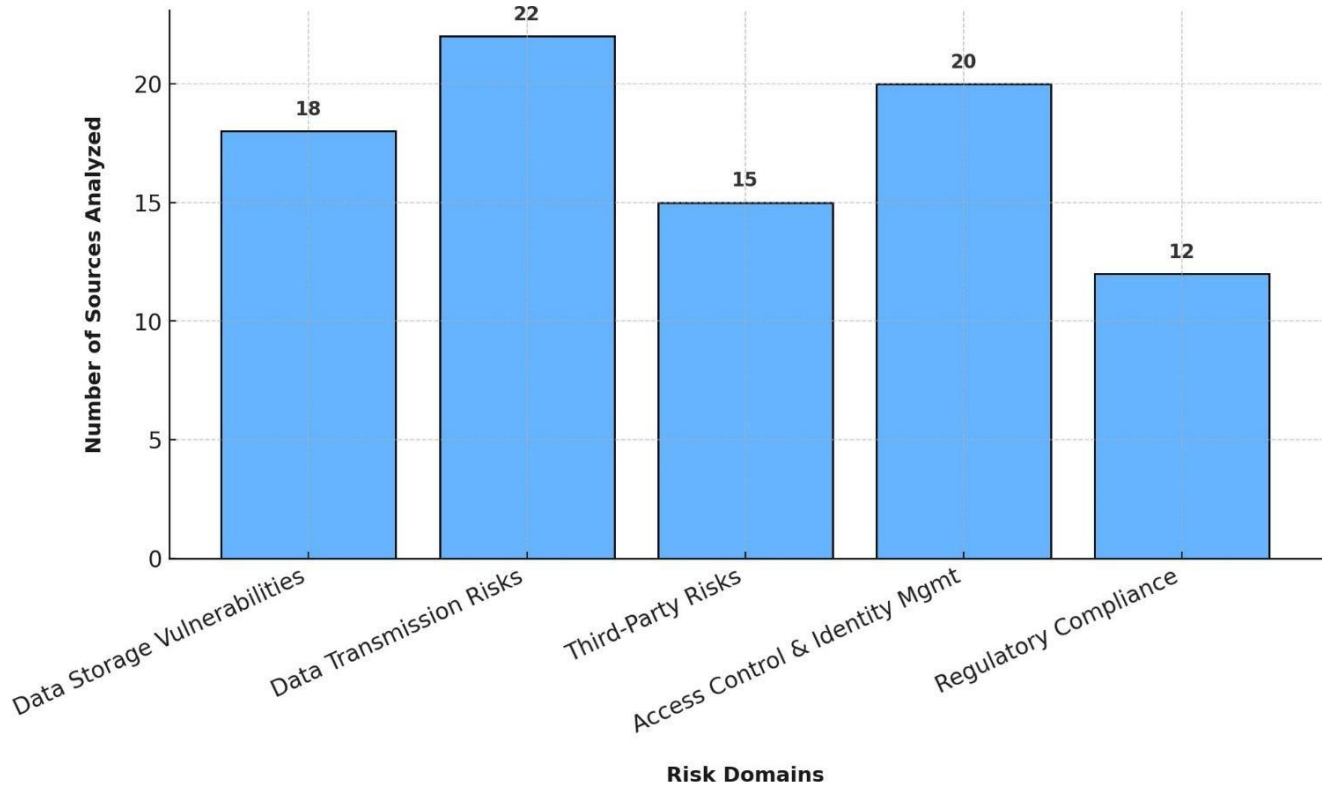

Fig. 5. Analytical Framework: Privacy Risk Domains

3.4 Breach Report Validation

The final stage involved validating literature findings with real-world data breaches. Publicly available records from the HHS Breach Portal were reviewed to identify recurring attack patterns. For instance, several 2021–2023 incidents revealed that misconfigured cloud storage buckets exposed thousands of patient records. These real cases confirmed academic observations that storage mismanagement remains one of the most common vulnerabilities in healthcare supply chains.

Case Study: In 2021, a U.S. healthcare provider experienced a breach where an unsecured cloud database exposed over 3 million patient records, including procurement orders for critical drugs. Investigation revealed that the storage service had been deployed without encryption or proper access controls. As illustrated in Figure 6, misconfigured storage, weak access controls, and lack of encryption consistently appear among the most frequently reported vulnerabilities, reinforcing their identification as foundational risks in the literature. This incident validated the emphasis on encryption and access control as essential safeguards for supply chain privacy.

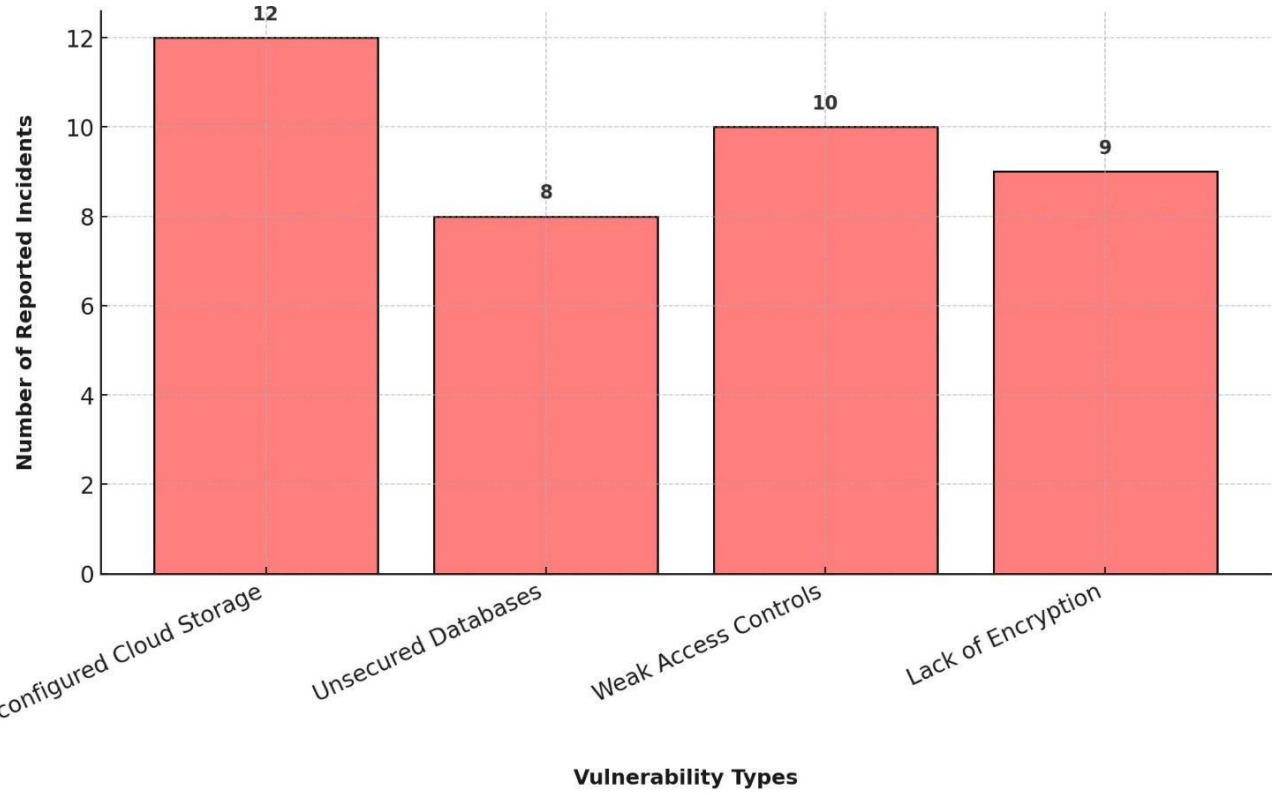

Fig. 6. Breach Report Validation of Common Vulnerabilities in Healthcare Supply Chains (2021–2023)

4. Privacy Concerns in Cloud-Based Healthcare Supply Chains

The adoption of cloud platforms within healthcare supply chains has improved efficiency, scalability, and real-time collaboration across stakeholders. However, the migration of sensitive healthcare data into distributed, multi-stakeholder environments has created serious privacy concerns. These risks are multi-dimensional, involving regulatory, technical, and organizational challenges. Based on existing literature, regulatory frameworks, and breach reports, six key areas emerge: **regulatory compliance, data breaches and cyberattacks, lack of standardization, third-party access risks, insider threats, data ownership and accountability.**

4.1 Regulatory Compliance

Healthcare organizations must comply with strict privacy regulations, most notably the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe. Both frameworks impose rigorous requirements on how data is stored, transmitted, and shared. Cloud environments complicate compliance because patient records may be stored in data centers located across multiple jurisdictions. This raises legal questions about sovereignty, lawful access requests, and enforcement authority.

Real-World Example: In 2020, the U.S. Department of Health and Human Services fined Athens Orthopedic Clinic $1.5 million for HIPAA violations after a breach exposed over 200,000 patient records. Investigations revealed that the clinic had failed to implement proper business associate agreements with its IT vendors. This case illustrates how regulatory non-compliance in cloud or vendor-managed environments can lead to both financial penalties and reputational damage.

4.2 Data Breaches and Cyberattacks

Healthcare records are among the most lucrative assets on the black market because they include medical history, demographic details, and financial information. Cloud adoption expands the attack surface by introducing APIs, web portals, and distributed data storage. Ransomware campaigns and phishing remain common entry points, while misconfigured storage buckets are frequently exploited.

Real-World Example: In 2021, CaptureRX, a healthcare supply chain services provider, suffered a ransomware attack that compromised the records of over 2.4 million patients across multiple U.S. hospitals. The attackers exploited vulnerabilities in cloud-hosted systems to gain access to prescription and insurance data. The breach disrupted pharmacy supply operations and highlighted how cyberattacks can ripple across entire healthcare networks.

4.3. Lack of Standardization

A significant challenge in protecting privacy is the absence of uniform standards across different supply chain partners. Hospitals, pharmaceutical firms, logistics providers, and cloud vendors often apply their own privacy and security protocols. This fragmented approach creates inconsistencies in encryption, auditing, and access control. Data may be secure within one system but exposed once transmitted to another partner with weaker safeguards.

Real-World Example: During the COVID-19 vaccine rollout in 2021, several European logistics companies reported inconsistent data protection practices in the handling of vaccine shipment data. Some partners implemented strong encryption and blockchain- based tracking, while others relied on legacy spreadsheets and unsecured communication channels. This lack of standardization created vulnerabilities in an otherwise mission-critical global supply chain.

4.4. Third-Party Access Risks

Healthcare supply chains are inherently collaborative, involving multiple vendors and service providers. Each third party introduces new risks, particularly when their security maturity is weaker than that of the primary healthcare organization. Attackers often exploit these weaker links to infiltrate the broader network.

Real-World Example: In 2019, American Medical Collection Agency (AMCA), a third- party billing vendor, was breached, exposing personal and medical data of more than 25 million patients from Quest Diagnostics and LabCorp. The incident, which originated from insufficient vendor security controls, caused financial losses so severe that AMCA filed for bankruptcy. This case demonstrates the cascading consequences of third-party privacy failures in healthcare supply chains.

4.5. Insider Threats

While most discussions around cloud security focus on external hackers, insider threats remain an equally dangerous concern in healthcare supply chains. Employees, contractors, or even trusted third-party staff with legitimate credentials may misuse their access privileges for financial gain or personal reasons. Insider misuse can be especially damaging in cloud systems because access is often role-based and distributed across multiple platforms. A 2020 HHS case involved a hospital employee who accessed thousands of patient records without authorization, leading to a HIPAA violation and subsequent fines (Smith et al., 2022). In supply chains, such actions can compromise sensitive procurement information, drug shipment schedules, and pricing agreements. Preventing insider threats requires strict monitoring, least-privilege

policies, and behavioral analytics yet these are difficult to consistently enforce in complex, multi-stakeholder cloud

ecosystems.

4.6. Cross-Border Data Transfers

Healthcare supply chains are inherently global, involving pharmaceutical manufacturers, suppliers, and logistics providers operating across multiple countries. Cloud-based systems further complicate this reality by storing and processing data in geographically distributed data centers. When patient records or procurement data cross international borders, they may fall under conflicting legal regimes, raising questions of data ownership and enforcement. The GDPR explicitly restricts transfers of personal data to countries lacking "adequate" protections, and similar rules exist in other jurisdictions. For example, disputes have arisen when U.S.-based cloud vendors stored European patient data in American servers, raising concerns about surveillance under the U.S. CLOUD Act (European Commission, 2018). These cross-border complexities not only hinder interoperability but also create significant legal uncertainty for healthcare organizations seeking to maintain compliance while benefiting from cloud scalability.

5. Proposed Privacy Framework

The review of existing literature and breach reports demonstrates that privacy risks in cloud-based healthcare supply chains are multidimensional and cannot be mitigated through isolated solutions. Instead, a holistic, multi-layer framework is necessary to secure data throughout its lifecycle. The framework proposed in this paper consists of four interconnected layers: **Encryption, Access Control, Blockchain Audit,** and **Regulatory Compliance.** Each layer addresses a distinct category of risk, but together they form a comprehensive defense strategy tailored for the healthcare domain.

5.1 Encryption Layer

Encryption is the foundation of privacy protection in any digital system. For healthcare supply chains, where sensitive patient records and procurement data flow across multiple stakeholders, **end-to-end encryption** is essential. This includes securing data **at rest** (stored in cloud servers or databases), **in transit** (during API calls or cross- border data exchanges), and **in use** (during processing within cloud applications).

Traditional encryption methods often fail at the "data in use" stage, when information must be decrypted for analysis. To overcome this, advanced methods such as **homomorphic encryption** and **secure multi-party computation (SMPC)** can be adopted. These allow computation on encrypted data without exposing raw values,

enabling privacy-preserving analytics on sensitive supply chain datasets. For example, pharmaceutical manufacturers and hospitals could collaborate on demand forecasting without directly exposing patient-level data.

Real-world lessons from breaches involving misconfigured cloud storage buckets highlight that encryption alone is insufficient if keys are poorly managed. Therefore, the framework emphasizes **centralized key management systems (KMS)** with strict separation of duties, ensuring that no single stakeholder can compromise data confidentiality.

5.2 Access Control Layer

Even with strong encryption, data privacy can be undermined if unauthorized individuals gain access through weak authentication or poorly defined roles. The proposed framework incorporates both **Role-Based Access Control (RBAC)** and **Attribute- Based Access Control (ABAC).**

RBAC ensures that users are only granted privileges aligned with their professional responsibilities (e.g., a hospital procurement officer can view inventory levels but not patient medical histories). ABAC extends this by introducing

context-aware policies, where access may depend on attributes such as location, device type, or time of request. This is particularly useful in global supply chains, where vendors and partners operate across regions with different compliance rules.

Insider threats, both malicious and accidental, are a recurring problem in healthcare systems. To address this, the framework recommends **continuous authentication and monitoring,** including behavioral analytics that can detect anomalies such as unusual login times or data downloads inconsistent with a user's role. This layer ensures that data exposure risks are minimized even when encryption is properly implemented.

5.3 Blockchain Audit Layer

A recurring weakness in healthcare supply chains is the lack of trustworthy, tamper- resistant audit logs. Conventional logging mechanisms can be manipulated, either by insiders seeking to cover their tracks or by attackers attempting to hide breaches. Integrating a **blockchain-based audit trail** provides immutable records of all data interactions, including access requests, modifications, and transfers.

Blockchain technology ensures that once a record is written, it cannot be altered without detection. In the context of healthcare supply chains, this feature enables transparent tracking of sensitive data across hospitals, manufacturers, distributors, and cloud providers. For example, if a shipment tracking system records patient-linked identifiers, access to this information can be logged on the blockchain, making unauthorized disclosures immediately visible.

While blockchain raises concerns about scalability, permissioned ledgers (such as Hyper ledger Fabric) are particularly suited for enterprise environments, where only authorized participants validate transactions. This balances performance with transparency and accountability. By embedding blockchain into the privacy framework, organizations can strengthen trust between supply chain partners while maintaining verifiable compliance records.

5.4 Regulatory Compliance Layer

The final layer of the proposed framework addresses the challenge of aligning technical measures with regulatory obligations. HIPAA and GDPR both require demonstrable safeguards for data confidentiality, integrity, and accountability. Yet, many breaches reveal that organizations struggle to translate legal requirements into enforceable technical controls.

This framework proposes **automated compliance monitoring** using policy engines that continuously evaluate system configurations against regulatory requirements. For example, a compliance engine could automatically flag if a dataset containing personally identifiable information is transferred to a data center in a non-compliant jurisdiction. Similarly, audit reports generated by the blockchain layer can be cross- referenced with HIPAA's requirement for audit trails, ensuring that compliance evidence is always available.

The regulatory compliance layer also introduces **data minimization** and **purpose limitation principles.** Supply chain partners should only access the minimum necessary information for their role. For instance, a logistics provider should see shipment identifiers but not patient medical records. Enforcing this principle reduces exposure in case of vendor breaches and ensures adherence to GDPR mandates.

6. Discussion

The findings of this study underscore that while technical measures such as encryption and access control are indispensable, they are not sufficient on their own to ensure comprehensive privacy in cloud-based healthcare supply chains. Encryption, for instance, is only as effective as the key management practices behind it, and access controls must be regularly updated to reflect changing roles. In practice, many breaches occur not because the

technology itself is flawed but because configurations are neglected or policies are applied inconsistently. This suggests that privacy safeguards must be coupled with continuous monitoring and proactive compliance checks rather than treated as one-time fixes.

Blockchain has gained traction as a potential answer to accountability gaps, offering tamper-resistant audit trails that improve transparency across stakeholders. This makes it especially valuable in fragmented healthcare supply chains where trust is often uneven. Yet, blockchain also presents challenges most notably scalability. High transaction volumes can strain distributed ledgers, and effective governance is needed to define validation, consensus, and dispute resolution mechanisms. Without such governance, blockchain risks replicating the very trust issues it is designed to solve.

Another critical dimension is the role of artificial intelligence (AI) and machine learning in anomaly detection. Conventional rule-based security systems often miss subtle or novel threats, while AI-driven approaches can detect unusual behavior in network traffic, user access, or data handling in near real time. In the context of the proposed multi-layer framework, anomaly detection serves as an overlay that strengthens existing layers. For example, if access control policies are properly configured but a user begins downloading procurement files at an abnormal rate, AI tools can flag the deviation for review. Similarly, if encryption is in place but transmission volumes suddenly spike, anomaly detection can act as an early warning system. In this way, AI does not replace encryption, access control, or blockchain auditing it complements them by providing continuous vigilance and adaptive response. Nevertheless, these tools must be tuned carefully, as false positives can overwhelm administrators and adversaries may attempt to poison training data. Human oversight therefore remains an essential counterpart to algorithmic monitoring.

Beyond technical tools, broader systemic challenges persist. Healthcare supply chains still operate under fragmented privacy policies, with each organization interpreting requirements differently. These inconsistencies are especially evident at the boundaries where data crosses institutions or jurisdictions. Coordinated efforts among regulators, industry consortia, and technology providers are needed to establish common privacy protocols enforceable across cloud platforms. Experiences with HL7 FHIR demonstrate that standardization is achievable, though widespread adoption often lags without regulatory incentives.

A related issue concerns the shared responsibility model in cloud computing. While cloud providers secure infrastructure, healthcare organizations are responsible for safeguarding their own applications and data. Too often, organizations assume compliance obligations rest solely with the vendor, leading to misconfigurations and preventable exposures. Clear delineation of responsibilities, regular audits, and transparent reporting are therefore essential parts of an effective privacy strategy.

Finally, patient trust must remain at the center of the discussion. Healthcare systems depend on individuals' willingness to share sensitive data, and every breach erodes that trust. Rebuilding confidence requires more than technical controls it demands visible

accountability, consistent transparency, and strong enforcement of privacy safeguards. By aligning technical innovation, governance, and patient-centered values, healthcare organizations can sustain both operational efficiency and the trust on which digital health relies.

7. Conclusion

The increasing adoption of cloud computing in healthcare supply chains reflects the sector's pressing need for real-time data exchange, scalability, and efficiency. Cloud platforms now enable hospitals, pharmaceutical manufacturers, distributors, and logistics providers to collaborate in ways that traditional on-premises systems

could not support. Yet these same features introduce significant privacy challenges. Patient records, procurement data, and vendor transactions remain vulnerable if not adequately secured. This paper has examined these risks and advanced a four-layer privacy framework designed to protect sensitive information throughout its lifecycle.

The framework integrates four complementary components: encryption to secure data against unauthorized disclosure, access controls to restrict visibility, blockchain auditing to ensure tamper-resistant accountability, and compliance mechanisms to align safeguards with legal requirements such as HIPAA and GDPR. Together, these measures offer a defense-in-depth model that addresses both external threats and internal weaknesses.

It is equally important to recognize the limitations of this model. Blockchain scalability remains a concern in high-volume supply chains, access privileges require frequent updates, encryption methods must adapt to emerging risks such as quantum computing, and compliance obligations evolve alongside shifting regulatory landscapes. No framework can succeed if implemented in isolation; it must be maintained through ongoing oversight, adaptation, and governance.

The discussion also highlights that technology alone cannot secure healthcare supply chains. Culture, governance, and collaboration matter just as much. In practice, this means hospitals and health systems should invest in dedicated privacy and compliance teams that oversee vendor practices and conduct regular audits. Regulators, in turn, should mandate standardized reporting mechanisms for cloud incidents, promote cross- border harmonization of privacy laws, and provide incentives for adopting interoperable standards similar to HL7 FHIR. Cloud vendors should be required to offer transparent configuration dashboards and automated compliance alerts so that healthcare customers understand and manage their shared responsibilities.

Looking forward, artificial intelligence offers promising enhancements when deployed carefully. AI-based anomaly detection can provide early warning of unusual access behavior, while federated learning could enable predictive supply chain analytics without centralizing sensitive datasets. However, these tools should be introduced incrementally, with human oversight and clear accountability to avoid over-reliance on algorithms.

Ultimately, protecting healthcare supply chain data is not only a technical necessity but a matter of public trust. Patients entrust institutions with their most sensitive information, and each breach undermines confidence in digital health. Strengthening safeguards is therefore both a practical requirement and an ethical obligation. By adopting multi-layer frameworks such as the one proposed here supported by consistent governance, regulatory alignment, and responsible innovation healthcare organizations can achieve the dual goals of operational efficiency and enduring confidentiality.

Stakeholder	**Key Actions**
Hospitals & Health Systems	Establish dedicated privacy/compliance teams; conduct regular audits of vendor practices; adopt the multi-layer framework as internal policy; provide ongoing staff training for secure cloud usage.
Regulators	Mandate standardized reporting for cloud-related incidents; harmonize cross-border privacy laws; incentivize adoption of interoperability standards (e.g., HL7 FHIR); enforce transparency in compliance monitoring.

Cloud Vendors	Offer configuration dashboards and automated compliance alerts; enable strong default encryption and identity controls; provide clarity on shared responsibility; integrate blockchain- enabled auditing features.

References

1. J. Smith, "Cloud Security in Healthcare: A Regulatory Perspective," *IEEE Trans. Cloud Comput.*, vol. 9, no. 4, pp. 233–245, Oct. 2022.
2. R. Gupta and A. Sharma, "Blockchain-Based Supply Chains: Opportunities and Challenges," *IEEE Access*, vol. 10, pp. 13456–13468, Mar. 2022.
3. U.S. Department of Health & Human Services, "HIPAA Security Rule," 2021. [Online]. Available: https://www.hhs.gov/hipaa
4. A. K. Jain et al., "Privacy-preserving Machine Learning in Healthcare," *IEEE J. Biomed. Health Inform.*, vol. 25, no. 11, pp. 4321–4332, Nov. 2021.
5. European Commission, "General Data Protection Regulation (GDPR)," 2018. [Online]. Available: https://gdpr-info.eu/
6. Z. Zandesh, "Privacy, Security, and Legal Issues in the Health Cloud," *Front. Public Health*, vol. 12, 2024.
7. M. Mehrtak et al., "Security challenges and solutions using healthcare cloud," *J. Big Data*, vol. 8, no. 1, 2021.
8. H. Taherdoost, "Privacy and Security of Blockchain in Healthcare," *Big Data Cogn. Comput.*, vol. 7, no. 4, pp. 1–15, 2023.
9. S. Sharma, K. Chen, and A. Sheth, "Towards practical privacy-preserving analytics for IoT and cloud-based healthcare systems," *IEEE Internet Comput.*, vol. 22, no. 2, pp. 42–52, Mar./Apr. 2018.
10. C. Thapa and S. Camtepe, "Precision Health Data: Requirements, Challenges and Existing Techniques for Data Security and Privacy," *IEEE Access*, vol. 8, pp. 20507– 20527, 2020.
11. R. Zhang, R. Xue, and L. Liu, "Security and Privacy for Healthcare Blockchains," *arXiv preprint arXiv:2106.06136*, 2021.
12. J. S. Jadhav et al., "Blockchain-based healthcare supply chain management: A review," *Mater. Today Proc.*, vol. 65, 2022.
13. A. Rizzardi, "IoT-driven blockchain to manage healthcare supply," *Future Gener. Comput. Syst.*, vol. 154, 2024.
14. B. Aljabhan, "Privacy-preserving blockchain framework for supply chain management," *Sustainability*, vol. 15, no. 8, p. 6905, 2023.
15. NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, Gaithersburg, MD, 2018.
16. ENISA, "Cloud Security for Healthcare Services," European Union Agency for Cybersecurity, 2021.
17. O. Bak et al., "Exploring blockchain implementation challenges in supply chains,"*Int. J. Prod. Res.*, vol. 63, no. 3, pp. 812–828, 2025.

18. M. Al Zaabi et al., "Big data security and privacy in healthcare: A systematic review," *nf. Dev.*, 2024.

19. P. Shojaei et al., "Security and privacy of technologies in health information systems: A systematic literature review," *Computers*, vol. 13, no. 3, p. 45, 2024.

20. J. Pool et al., "A systematic analysis of failures in protecting personal data," *Int. J. Inf. Manage.*, vol. 75, 2024.

21. A. Alamsyah et al., "Enhancing privacy and traceability of public health data using blockchain," *Front. Blockchain*, vol. 1, 2025.

22. WHO, "Digital health and data protection: Global guidance," World Health Organization, 2023.

23. ISO/IEC 27701:2019, "Security techniques – Extension to ISO/IEC 27001 and ISO/ IEC 27002 for privacy information management," ISO, Geneva, Switzerland, 2019.

24. M. S. B. Kasyapa, "Blockchain integration in healthcare supply chain systems," *Health Inf. Sci. Syst.*, vol. 12, no. 1, 2024.

25. J. Zhou et al., "Security and privacy in cloud-based e-health systems: A survey," *IEEE Access*, vol. 9, pp. 50017–50037, 2021.

26. A. Rghioui et al., "IoT-based healthcare: A survey on security and privacy," *Comput. Netw.*, vol. 197, 2021.

27. J. Lin et al., "Blockchain and IoT integration for healthcare data management," *Future Gener. Comput. Syst.*, vol. 133, 2022.

28. D. He et al., "Data security in healthcare IoT: Challenges and solutions," *IEEE Commun. Mag.*, vol. 58, no. 6, pp. 26–32, Jun. 2020.

29. A. Faridoon and M. T. Kechadi, "Healthcare data governance, privacy, and security: A conceptual framework," *arXiv preprint arXiv:2403.17648*, 2024.

30. C. Esposito et al., "Blockchain-based supply chain management: A survey," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1322–1336, Nov. 2020.

31. A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e- health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, 2018.

32. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

33. M. Paul et al., "Digitization of healthcare sector: A study on privacy and security," *Digital Health*, vol. 9, 2023.

34. H. Xu et al., "Privacy-preserving healthcare data sharing through federated learning," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1052–1065, Apr./Jun. 2021.

35. A. Joshi et al., "A survey on security and privacy of federated learning in healthcare," *Future Gener. Comput. Syst.*, vol. 129, 2022.

36. S. Wang et al., "A blockchain-based privacy-preserving healthcare system," *J. Med. Internet Res.*, vol. 21, no. 6, 2019.

37. T. Fernandez-Carames and P. Fraga-Lamas, "A review on blockchain technologies for healthcare applications," *IEEE Access*, vol. 7, pp. 164490–164508, 2019.

38. Y. Luo et al., "Secure data access control for cloud-based healthcare systems," *IEEE Trans. Cloud Comput.*, vol.

8, no. 2, pp. 484–496, 2020.

39. A. Ahmad et al., "Security and privacy in healthcare: Issues and solutions," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 3, pp. 3293–3310, 2021.

40. H. Wu et al., "Secure and efficient data sharing for cloud-based healthcare systems," *Future Gener. Comput. Syst.*, vol. 95, pp. 623–633, 2019.

41. The Psychology of Visual Perception in Data Dashboards: Designing for Impact. (2025). International Journal of Data Science and Machine Learning, 5(02), 79-86. https://doi.org/10.55640/ijdsml-05-02-07

42. P. Zhang et al., "FHIRChain: Applying blockchain to secure and scalable sharing of healthcare data," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, 2018.

43. M. Hussain et al., "Healthcare data privacy in IoT: Blockchain-based approach," *Sensors*, vol. 21, no. 12, 2021.

44. L. Benchoufi et al., "Blockchain protocols in clinical trials: Transparency and traceability," *J. Med. Internet Res.*, vol. 21, no. 3, 2019.

45. A. Azaria et al., "MedRec: Blockchain for medical data access," *Proc. IEEE Int. Conf. Open Big Data*, 2016.

46. S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," *IEEE Access*, vol. 7, pp. 50759–50779, 2019.

47. K. Fan et al., "MedBlock: Efficient and secure medical data sharing via blockchain," *J. Med. Syst.*, vol. 42, no. 8, 2018.

48. T. Alladi et al., "Blockchain in smart healthcare: Challenges and solutions," *IEEE Access*, vol. 7, pp. 247–257, 2019.

49. J. Yue et al., "Healthcare data gateways: Security and privacy perspectives," *IEEE Access*, vol. 4, pp. 205–216, 2016.

50. M. Mettler, "Blockchain technology in healthcare: The revolution starts here," *Proc. IEEE Healthcom*, pp. 1–3, 2016.

51. R. G. Holliday, "Cybersecurity threats in healthcare supply chains: A review of ransomware and insider attacks," *Health Policy Technol.*, vol. 12, no. 1, 2023.