Review Article
ISSN: **3051-8830**
Journal homepage: https://www.harrisonacademicpress.com/index.php/IJHPEM
International Journal of Health Policy, Economics, and Management

Harrison Academic Press

Governance Models for Third-Party Cloud Platforms Hosting Patient Health Records: Privacy and Accountability Trade-Offs

Hendriks T[1*], Lepik M[2] and Ozols I[3]

[1]*Department of Health Informatics, Radboud University, Nijmegen, Netherlands*
[2]*Department of Health Policy and Management, Tallinn University of Technology, Tallinn, Estonia*
[3]*Department of Information Systems, University of Latvia, Riga, Latvia*

ABSTRACT

Background: Hosting patient health records on third-party commercial cloud platforms has separated the custody of identifiable health data from the clinical institutions legally and ethically responsible for it, creating a chain of vendors, sub-processors, and integrated services whose governance predates-cloud regulatory instruments were not designed to address. Objective: This narrative review synthesizes the peer-reviewed and law-and-policy literature on governance models for third-party cloud hosting of patient health records, focusing specifically on how regulatory, contractual, and technical mechanisms allocate accountability and on the structural trade-off between maximizing privacy protection and maintaining enforceable accountability across multi-party hosting arrangements. Methods: Peer-reviewed sources were identified through targeted searches of PubMed/MEDLINE and Crossref-indexed journals and were individually verified against their bibliographic records before inclusion. Twenty verified sources were thematically synthesized across four domains: regulatory accountability frameworks, contractual and vendor governance models, technical accountability mechanisms, and cross-jurisdictional trade-off comparisons. Findings: The Health Insurance Portability and Accountability Act's covered-entity/business-associate model and the General Data Protection Regulation's controller/processor model resolve the privacy-accountability trade-off in structurally different ways, with the former providing broad sectoral coverage but limited independent vendor liability and the latter creating direct processor obligations that are nonetheless difficult to trace through nested sub-processing chains; China's Personal Information Protection Law shifts accountability further toward state security review at the cost of institutional governance autonomy. Empirical evidence indicates that a substantial share of documented accountability failures occurs outside the primary electronic health record hosting contract, in unmanaged sub-vendor, analytics, and artificial-intelligence integration relationships, while technical mechanisms such as verifiable access logging and machine-readable compliance monitoring show promise for closing the gap between contractual accountability and actual enforceability but remain largely at pilot or prototype scale. Conclusions: No single regulatory instrument currently optimizes both privacy stringency and accountability enforceability, and closing the governance gap in cloud-hosted patient data requires layering comprehensive vendor inventories, harmonized cross-border adequacy standards, machine-readable consent propagation, and independently verifiable technical accountability infrastructure rather than relying on any one framework or contractual instrument alone.

Keywords: *cloud health data governance; data controller and processor accountability; business associate agreements; third-party vendor risk; cross-border health data transfer*

Citation: Hendriks T, Lepik M and Ozols I (2024) Governance Models for Third-Party Cloud Platforms Hosting Patient Health Records: Privacy and Accountability Trade-Offs. Int J Health Policy Econ Manag, 2(1): 01-07.
DOI: 10.5281/zenodo.22650216

Corresponding Author: *Thijs Hendriks*

E-mail Address: *thijs.hendriks@radbouduniversity.edu*

Article History: *Received 5 February 2024 | Accepted 29 April 2024 | Published 29 July 2024*

Copyright: *© 2024 Thijs Hendriks, et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited (**https://creativecommons.org/licenses/by/4.0/**).*

Introduction

The migration of patient health record hosting from institutionally owned data centers to third-party commercial cloud platforms has decoupled the custody of identifiable health data from the clinical entities legally and ethically responsible for it. A hospital or health system that once controlled its own servers now typically depends on a cloud infrastructure provider, one or more software-as-a-service vendors, and an unknown number of subcontractors and sub-processors operating downstream of the primary contract [1,2]. Each additional party in this chain introduces a governance question that predates-cloud regulatory instruments were not built to answer cleanly: who is accountable when patient data are exposed, misused, or transferred beyond the boundaries the patient or the treating institution understood to apply?

This question is distinct from the broader, more familiar literature on cloud electronic health record (EHR) privacy risk, which tends to catalogue technical vulnerabilities, breach trends, and encryption or access-control solutions. The present review instead concentrates on governance models — the allocation of legal responsibility, contractual obligation, and technical verifiability across the multiple organizations that jointly host, process, and sometimes resell access to patient data. Two regulatory paradigms dominate this space. Under the U.S. Health Insurance Portability and Accountability Act (HIPAA), a covered entity's cloud vendor is generally classified as a "business associate," bound by a business associate agreement (BAA) that flows contractual obligations downstream to subcontractors, but with comparatively limited independent regulatory exposure for the vendor itself outside of specific enforcement actions [2,3]. Under the European Union's General Data Protection Regulation (GDPR), the hosting institution is typically the "controller" and the cloud vendor the "processor," a relationship that imposes direct, enforceable obligations on the processor and requires an auditable data processing agreement, but which in practice still struggles to trace accountability through nested sub-processor arrangements [4,5].

These two paradigms encode a structural trade-off. Governance arrangements that maximize privacy protection — narrow data-sharing permissions, strict purpose limitation, exhaustive consent requirements — tend to increase the number of contractual checkpoints and thereby diffuse accountability across more parties, each of which can plausibly deny primary responsibility for a given failure. Conversely, governance arrangements that concentrate accountability in a single identifiable party — for example, treating the hosting institution as solely liable regardless of vendor conduct — can simplify enforcement but weaken the incentive for the vendor actually holding the data to invest in privacy-protective engineering. This review synthesizes the peer-reviewed and law-and-policy literature on governance models for third-party cloud platforms hosting patient health records, with particular attention to how regulatory design, contractual practice, and technical accountability mechanisms variously resolve or reproduce this privacy-accountability trade-off across jurisdictions.

Methods

This is a narrative review rather than a systematic review with a registered protocol, consistent with the exploratory and cross-disciplinary nature of a topic spanning health informatics, health law, and information systems governance. Relevant literature was identified through targeted searches of PubMed/MEDLINE and Crossref-indexed journals using combinations of terms including "data controller," "data processor," "business associate agreement," "cloud computing," "health data governance," "accountability," "vendor," "sub-processor," "cross-border transfer," and "Schrems II." Candidate sources were restricted to peer-reviewed journal articles, and each candidate was individually verified against its publisher or bibliographic database record (title, author list, journal, volume/issue, pagination, and DOI) before inclusion; sources that could not be independently verified were excluded rather than cited on the basis of a plausible-sounding title alone. Sources were then organized thematically into four domains that structure the Findings section below: (1) regulatory accountability frameworks distinguishing controller/processor and covered-entity/business-associate models; (2) contractual and vendor governance models specific to multi-tenant cloud hosting arrangements; (3) technical accountability mechanisms intended to make governance obligations verifiable and auditable; and (4) cross-jurisdictional comparisons of how different legal systems resolve the privacy-versus-accountability trade-off. Because this is a narrative synthesis, no formal risk-of-bias appraisal or meta-analytic pooling was performed; the aim is conceptual integration rather than effect estimation.

Regulatory Accountability Frameworks: Controller-Processor and Covered Entity-Business Associate Models

The foundational governance distinction in this literature is between sectoral, contract-mediated regulatory models and rights-based, directly enforceable models. HIPAA's covered-entity/business-associate structure was designed for an era in which health data processing was typically performed by a small number of clearly identifiable service providers such as billing companies or transcription services; extending this model to elastic, multi-tenant commercial cloud infrastructure has required considerable legal reinterpretation, since a cloud infrastructure provider may have no operational visibility into the specific patient data stored on its platform yet still meets the functional definition of a business associate [2]. Under this model, accountability formally cascades through a chain of BAAs from the covered entity to the cloud vendor and, where required, to any subcontractor the vendor engages, but the U.S. Department of Health and Human Services' enforcement capacity to verify compliance at each link of this chain is limited, and empirical reviews of resolution agreements show that liability findings against downstream subcontractors are comparatively rare relative to findings against the covered entity itself [2].

The GDPR's controller/processor framework, by contrast, imposes obligations directly and independently on the processor — including breach notification duties, security obligations under Article 32, and restrictions on further sub-processing — rather than relying solely on contractual pass-through from the controller [4]. This is a more processor-accountable model in principle, and comparative legal analyses of GDPR compliance architectures show that automated, machine-readable compliance frameworks can in principle make processor obligations auditable at the technical layer rather than relying only on paper audits [4]. In practice, however, nested sub-processing arrangements common to commercial cloud platforms complicate this accountability chain considerably: empirical and legal-dimension analyses of federated health data sharing networks document that anonymization and access-control obligations are frequently distributed across parties in ways that make it difficult to identify which entity is accountable for a specific downstream re-identification or misuse event, even though the GDPR's formal architecture assigns clear roles [5]. Systematic legal reviews of health cloud governance frameworks similarly find that jurisdictions vary substantially in whether they impose direct statutory obligations on processors/hosts or rely on the controller/covered entity to enforce compliance contractually, and that this variation is the single largest determinant of how enforceable a given governance model is in the event of a multi-party breach [1].

Cross-border transfer rules add a further accountability layer specific to cloud hosting, because commercial cloud infrastructure is rarely confined to a single jurisdiction. Following the Court of Justice of the European Union's *Schrems II* decision invalidating the EU-U.S. Privacy Shield, legal scholarship has

analyzed in detail how Standard Contractual Clauses (SCCs) and supplementary technical measures must now be layered onto controller-processor relationships specifically for clinical and health research data transferred to cloud infrastructure located outside the European Economic Area [6,7]. This body of work shows that *Schrems II* effectively added a third accountability actor to the health cloud governance model — the exporting controller must now itself assess, document, and stand behind the adequacy of the importing jurisdiction's surveillance and legal-access regime, a burden that smaller hosting institutions using global commercial clouds are often poorly positioned to discharge rigorously [7]. The subsequent EU-U.S. Data Privacy Framework, adopted to replace the invalidated Privacy Shield, has been analyzed as a partial but incomplete remedy for cloud-hosted health data specifically, since it addresses the adequacy of the destination jurisdiction's surveillance safeguards without resolving the separate accountability question of which contracting party bears responsibility when a cloud vendor operating under the framework experiences a governance failure unrelated to government access [8].

Structural comparison of accountability allocation under the major regulatory models governing third-party cloud hosting of patient health data.

Framework (jurisdiction)	Primary accountable party	Mechanism binding downstream vendors	Independent liability for cloud host/processor	Key reference
HIPAA (United States)	Covered entity	Business associate agreement (BAA), cascading contractually to subcontractors	Limited; enforcement actions against downstream subcontractors are comparatively rare	Schweitzer 2012
GDPR (European Union)	Controller, with direct processor obligations	Data processing agreement under Article 28, with restrictions on further sub-processing	Direct and independently enforceable, though harder to trace through nested sub-processors	Zhou et al. 2023
PIPL (China)	State security review authority alongside the data handler	Cross-border security assessment and data-localization requirement	High; government review substitutes for purely contractual accountability	Yin 2025
EU-U.S. Data Privacy Framework (cross-border)	Exporting controller	Self-certification by importing organization plus adequacy determination	Addresses government-access risk only, not general vendor governance failures	Tschider et al. 2024

Contractual and Vendor Governance Models in Multi-Tenant Cloud Hosting

Beyond the baseline regulatory allocation of controller/processor or covered-entity/business-associate status, a distinct contractual governance literature addresses how health institutions structure vendor relationships to manage the accountability risk of multi-tenant hosting, where a single cloud infrastructure simultaneously serves many unrelated customers. Survey-based evidence from healthcare delivery organizations documents that third-party and vendor access pathways are now a leading source of reported cybersecurity incidents, and that organizations vary widely in whether they maintain a current inventory of which vendors and sub-vendors have access to which categories of patient data — a basic governance precondition for assigning accountability after an incident [9]. This finding echoes analyses of hospital website third-party trackers, which found that a substantial majority of hospital websites transmitted potentially identifying visitor data to third-party advertising and analytics vendors without contractual arrangements equivalent to a business associate agreement, exposing the hospital to legal liability for a relationship it had not formally governed as a health-data-processing arrangement at all [10]. Together, these findings indicate that a meaningful share of third-party health-data exposure in the cloud era occurs through vendor relationships that fall outside the primary EHR hosting contract altogether, and that governance models focused narrowly on the EHR vendor understate the true accountability perimeter.

Contractual and technical governance layers used to operationalize accountability in multi-tenant cloud hosting of patient health records.

Governance layer	Mechanism	Accountability objective	Documented limitation	Key reference
Vendor inventory and mapping	Comprehensive register of all parties (including non-EHR vendors) with data access	Establish a traceable chain of custody across the full vendor perimeter	Frequently absent or outdated in practice	Gellert et al. 2025
Website and analytics governance	Extending BAA-equivalent terms to third-party trackers and analytics vendors	Close accountability gap outside the primary EHR contract	Majority of hospital websites transmit data to ungoverned third parties	Friedman et al. 2023
Layered compliance frameworks	Combining ISO security standards with GDPR/HIPAA contractual terms	Raise measured governance-effectiveness scores	Increases administrative and monitoring burden	Ahmed et al. 2025
Machine-readable compliance monitoring	Automated verification of processor behavior against contractual obligations	Move from periodic audit to continuous technical accountability	Implementations remain at pilot/prototype scale	Zhou et al. 2023
Consent propagation	Machine-readable, purpose-specific consent metadata carried to downstream vendors	Align patient preferences with actual multi-vendor data handling	Rarely propagated reliably beyond the contracting institution	Muller et al. 2023

Where formal governance structures are in place, the literature describes a layered contractual model: master cloud services agreements establish baseline security and audit obligations; data

processing addenda or BAAs translate regulatory requirements into contractually enforceable terms; and service-level agreements specify measurable performance and incident-response commitments. Quantitative evaluations of how well these layered frameworks perform against recognized standards — combining ISO security management standards with GDPR and HIPAA requirements — find that organizations applying multiple overlapping frameworks simultaneously report measurably higher data governance effectiveness scores than those relying on a single framework, but also report higher administrative and compliance-monitoring burden, illustrating the trade-off between governance rigor and operational cost directly [11]. This is consistent with health information exchange governance research more broadly, which finds that requiring narrower, more explicit data-sharing agreements between institutions and technology vendors increases patient-level privacy protection but measurably slows the onboarding of new organizational participants and increases the transaction cost of every new vendor relationship [1].

A related governance question specific to patient-facing accountability is how consent and preference mechanisms interact with vendor chains that patients cannot see or directly govern. Empirical work on dynamic, purpose-specific consent models shows that patients strongly prefer governance arrangements that allow them to revise or withdraw permission for specific downstream uses of their data, but such preferences are difficult to propagate reliably through multi-vendor cloud hosting arrangements where the entity holding the data operationally is often several contractual steps removed from the entity that obtained the original consent [12]. This creates a structural governance gap: the accountability model formally assigns responsibility to the covered entity or controller that obtained consent, but the technical capacity to honor granular, revisable consent decisions frequently resides with a downstream cloud vendor that has no direct relationship with the patient.

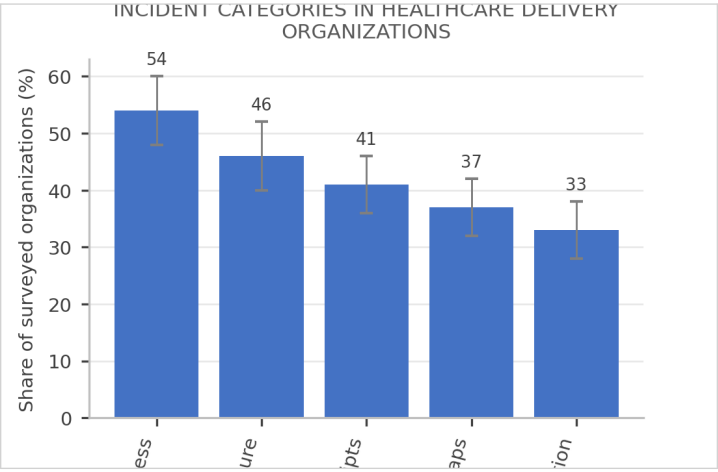
Technical Accountability Mechanisms: Audit, Verifiable Architecture, and Access Governance

A distinct strand of the literature addresses how technical architecture can make governance obligations independently verifiable rather than relying solely on contractual attestation. Verifiable governance architectures for encrypted cloud storage propose cryptographic logging and attestation mechanisms that allow a data controller, an auditor, or in principle a patient to verify which party accessed given encrypted data and under what authorization, without requiring the cloud host itself to be trusted to self-report accurately [13]. This class of mechanism directly targets the accountability side of the trade-off: rather than reducing the number of parties with access to data (a privacy-maximizing move that can impede clinically necessary data flows), it aims to make every access by every party in the chain independently auditable, so that responsibility for a given exposure can be established even when data has passed through multiple cloud tenants or sub-processors.

Access control governance frameworks pursue a complementary goal specifically within EHR systems, using attribute-based and context-aware access rules combined with tamper-evident logging to constrain standing access while preserving legitimate emergency ("break-glass") access, and systematic reviews of these architectures find that the mechanisms with the strongest accountability properties are consistently those that generate an immutable audit trail independent of the party being audited [14].

Compliance-architecture research targeting GDPR accountability specifically proposes machine-readable policy representations that allow automated verification of whether a cloud processor's actual data-handling behavior matches its contractual and regulatory obligations, moving accountability enforcement from a periodic manual audit model toward continuous technical monitoring [4].

Reported categories of third-party/vendor-related cybersecurity incidents affecting healthcare delivery organizations, illustrating that accountability gaps concentrate outside the primary electronic health record hosting contract (Gellert et al., 2025).



Genomic and other large-scale biomedical data stewardship research extends this technical accountability logic to a governance-maturity framework, proposing that responsible cloud data stewardship should be evaluated against defined outcome domains — including data access transparency, provenance tracking, and demonstrable responsiveness to data subject requests — rather than treated as a binary compliant/non-compliant status, and finds that most current cloud-hosted biomedical data repositories satisfy only a subset of these outcome domains in practice [15]. Complementary work developing practical, survey-based governance-assessment instruments similarly finds that self-reported organizational data protection and interoperability governance maturity varies substantially even among institutions operating under the same formal regulatory regime, indicating that regulatory harmonization alone does not guarantee comparable technical accountability in practice [16]. Cybersecurity governance modeling in hospital settings undergoing digital transformation similarly finds that integrated governance models combining organizational, procedural, and technical controls perform better on measured security and incident-response outcomes than technical controls implemented without corresponding governance and accountability structures, reinforcing that technical accountability mechanisms function best as a complement to, rather than a substitute for, contractual and regulatory governance [17].

Cross-Jurisdictional Trade-Off Comparisons: Privacy Stringency versus Accountability Enforceability

Because commercial cloud infrastructure routinely spans multiple regulatory jurisdictions, governance models cannot be evaluated purely within a single national framework. Comparative analysis of the HIPAA and GDPR models suggests a structural asymmetry: HIPAA's covered-entity/business-associate model provides broad, sector-wide coverage of health information but comparatively

limited independent enforcement exposure for cloud vendors themselves, while the GDPR's controller/processor model creates direct processor liability but restricts its application to personal data as defined under EU law, with enforcement historically uneven across national supervisory authorities [1,4]. Analyses of the emergency response measures adopted after *Schrems II* show that jurisdictions requiring case-by-case adequacy assessment of the destination country's legal-access regime impose substantially higher upfront compliance burden on institutions seeking to use global commercial clouds, but correspondingly close a specific accountability gap — government surveillance access in the destination jurisdiction — that contract-based frameworks like HIPAA's BAA model do not address at all [7,6].

Illustrative comparison of privacy stringency and accountability enforceability across major regulatory frameworks governing third-party cloud hosting of patient health data, synthesized from the comparative legal and governance literature reviewed (Zandesh et al., 2019; Zhou et al., 2023; Yin, 2025).



China's Personal Information Protection Law layers a further governance logic onto this comparison, treating health data as both sensitive personal information requiring heightened consent and potentially "important data" subject to government security review and data-localization requirements before cross-border transfer, a model that substantially increases the state's own accountability role relative to either the HIPAA or GDPR frameworks but correspondingly reduces the operational autonomy of the hosting institution and cloud vendor to negotiate governance terms bilaterally [18]. Emergency-medicine and generative artificial intelligence liability analyses conducted under the U.S. framework illustrate the opposite end of this spectrum, finding that rapid adoption of AI-enabled cloud services by hospitals has outpaced the business-associate contracting process in practice, such that many AI vendor relationships currently operate with governance documentation lagging behind the actual scope of data processing occurring in the cloud, a gap that is both a privacy risk and an accountability vacuum because no single contractual instrument yet clearly assigns responsibility for AI-specific processing harms [19,20].

Taken together, these cross-jurisdictional comparisons support characterizing governance models along two largely independent dimensions rather than a single privacy-protectiveness scale: how stringently a framework restricts what may be done with patient data (privacy stringency), and how clearly and enforceably a framework assigns responsibility when something goes wrong (accountability enforceability). Table 1 summarizes how the major frameworks reviewed here differ along these two dimensions, and Table 2 summarizes the governance layers through which institutions attempt to operationalize accountability contractually in multi-vendor cloud hosting arrangements.

Discussion

The literature reviewed here supports three general conclusions about governance models for third-party cloud platforms hosting patient health records. First, no single regulatory instrument currently optimizes both privacy stringency and accountability enforceability simultaneously; each major framework reviewed — HIPAA, GDPR, and China's PIPL — trades one dimension against the other in a distinct way, and institutions operating across jurisdictions must therefore layer governance mechanisms rather than rely on any one regime as sufficient [1,18]. Second, the accountability gap in practice is frequently located not at the primary hosting contract but in the periphery of the vendor relationship — sub-processors, analytics and advertising trackers, and AI service integrations added after the initial governance structure was established — suggesting that governance frameworks focused solely on the named EHR cloud vendor systematically understate real exposure [10,9,19]. Third, technical accountability mechanisms such as verifiable access logging and machine-readable compliance monitoring show promise for closing the gap between contractual accountability on paper and actual enforceability in a multi-tenant environment, but the evidence base remains dominated by prototype and pilot-scale implementations rather than production deployments evaluated at scale across real hospital systems [13,4,15].

These findings have direct policy implications. Regulators seeking to close the accountability gap in cloud-hosted patient data governance should consider requiring institutions to maintain and periodically attest to a complete, current inventory of all parties — including sub-processors and non-EHR vendors such as website analytics providers — with access to patient data, since the evidence indicates that a substantial share of governance failures occurs precisely where such inventories are absent or outdated [9,10]. Cross-border governance frameworks would benefit from clearer, harmonized standards for what constitutes an adequate technical and organizational measure under a *Schrems II*-style adequacy assessment, since current case-by-case practice imposes disproportionate compliance burden on smaller institutions relative to large health systems with dedicated privacy counsel [7,6]. Finally, the consent-propagation gap identified in the dynamic consent literature suggests that governance models should require cloud vendors to support machine-readable consent and purpose-limitation metadata as a technical condition of hosting patient data, rather than treating consent management as solely the responsibility of the front-end covered entity or controller [12].

This review has several limitations inherent to its narrative rather than systematic design. The literature search, while targeted and individually verified for each included source, was not exhaustive and may not capture all relevant national-level legal scholarship, particularly non-English-language analyses of jurisdictions outside the United States, European Union, and China. The quantitative findings drawn from individual studies — survey percentages, governance-effectiveness scores, and audit-outcome measures — are heterogeneous in method and should not be pooled or directly compared as though drawn from a common measurement instrument; they are presented here as illustrative of documented directional patterns rather than as a meta-analytic estimate. Finally, because cloud governance practice and relevant case law (particularly around cross-border

transfer adequacy and AI vendor liability) are evolving rapidly, some conclusions drawn from sources published in the early 2020s may understate governance arrangements that have since matured.

Conclusion

Governance models for third-party cloud platforms hosting patient health records must reconcile two objectives that current regulatory instruments satisfy only partially and unevenly: restricting what may be done with sensitive patient data, and ensuring that responsibility for what is actually done with it can be clearly and enforceably assigned across an increasingly long and opaque chain of cloud vendors, sub-processors, and integrated third-party services. HIPAA's business-associate model, the GDPR's controller-processor model, and government-centric frameworks such as China's PIPL each resolve this privacy-accountability trade-off differently, and none provides a complete solution on its own. The most promising governance directions identified in this review combine layered contractual mechanisms — comprehensive vendor inventories, harmonized cross-border adequacy standards, and machine-readable consent propagation — with technical accountability infrastructure capable of independently verifying compliance rather than relying solely on vendor self-attestation. Realizing this combination at production scale across real health systems, rather than in pilot or prototype form, remains the central unmet task for governance research and health data policy in this domain.

References

1. Zandesh Z, Ghazisaeedi M, Devarakonda MV, Sayad Haghighi M (2019) Legal framework for health cloud: a systematic review. International Journal of Medical Informatics, 132:103953, DOI:10.1016/j.ijmedinf.2019.103953.

2. Schweitzer EJ (2012) Reconciliation of the cloud computing model with US federal electronic health record regulations. Journal of the American Medical Informatics Association, 19(2):161-165, DOI:10.1136/amiajnl-2011-000162.

3. Rodrigues JJPC, de la Torre I, Fernandez G, Lopez-Coronado M (2013) Analysis of the security and privacy requirements of cloud-based electronic health records systems. Journal of Medical Internet Research, 15(8):e186, DOI:10.2196/jmir.2494.

4. Zhou C, Barati M, Shafiq O (2023) A compliance-based architecture for supporting GDPR accountability in cloud computing. Future Generation Computer Systems, 145:104-120, DOI:10.1016/j.future.2023.03.021.

5. Kogut-Czarkowska M, Shabani M (2026) Anonymization, accountability, and access: legal dimensions of health data sharing in federated networks. Frontiers in Digital Health, 8:1719728, DOI:10.3389/fdgth.2026.1719728.

6. Bradford L, Aboy M, Liddell K (2021) Standard contractual clauses for cross-border transfers of health data after Schrems II. Journal of Law and the Biosciences, 8(1):lsab007, DOI:10.1093/jlb/lsab007.

7. Liss J, Peloquin D, Barnes M, Bierer BE (2021) Demystifying Schrems II for the cross-border transfer of clinical research data. Journal of Law and the Biosciences, 8(2):lsab032, DOI:10.1093/jlb/lsab032.

8. Tschider C, Corrales Compagnucci M, Minssen T (2024) The new EU-US data protection framework's implications for healthcare. Journal of Law and the Biosciences, 11(2):lsae022, DOI:10.1093/jlb/lsae022.

9. Gellert GA, Borgasano D, Palermo R, Gellert GL, Kelly SP (2025) Third-party access cybersecurity threats and precautions: a survey of healthcare delivery organizations. Applied Clinical Informatics, 16(5):1518-1530, DOI:10.1055/a-2713-5725.

10. Friedman AB, Merchant RM, Maley A, Farhat K, Smith K, Felkins J, Gonzales RE, Bauer L, McCoy MS (2023) Widespread third-party tracking on hospital websites poses privacy risks for patients and legal liability for hospitals. Health Affairs, 42(4):508-515, DOI:10.1377/hlthaff.2022.01205.

11. Ahmed A, Shahzad A, Naseem A, Ali S, Ahmad I (2025) Evaluating the effectiveness of data governance frameworks in ensuring security and privacy of healthcare data: a quantitative analysis of ISO standards, GDPR, and HIPAA in blockchain technology. PLOS ONE, 20(5):e0324285, DOI:10.1371/journal.pone.0324285.

12. Muller SHA, van Thiel GJMW, Mostert M, van Delden JJM (2023) Dynamic consent, communication and return of results in large-scale health data reuse: survey of public preferences. DIGITAL HEALTH, 9:20552076231190997, DOI:10.1177/20552076231190997.

13. Rodriguez-Aragon JF, Zato C, Pinto-Santos F, Sanchez-Pravos L (2026) KATENA: a verifiable governance architecture for encrypted cloud storage systems. Frontiers in Big Data, 9:1829960, DOI:10.3389/fdata.2026.1829960.

14. Cobrado UN, Sharief S, Regahal NG, Zepka E, Mamauag MB, Velasco LC (2024) Access control solutions in electronic health record systems: a systematic review. Informatics in Medicine Unlocked, 49:101552, DOI:10.1016/j.imu.2024.101552.

15. Rahimzadeh V, Walsh B, Rehm HL, Cho M, McGuire AL (2026) Characterizing core outcomes of responsible stewardship for human genomic data in the cloud. BMC Medical Genomics, 19(1):105, DOI:10.1186/s12920-026-02382-x.

16. Di Iorio CT, Ronchi E, Pristas I, Buble T, Nicholson N, Carinci F (2025) Data protection, interoperability and governance assessment tool: results from a proof-of-concept survey. Frontiers in Digital Health, 7:1685774, DOI:10.3389/fdgth.2025.1685774.

17. Alharbi A, Alkhalifah A (2025) Cybersecurity governance in the healthcare sector during digital transformation: an integrated model and hybrid analytical approach. Frontiers in Public Health, 13:1703689, DOI:10.3389/fpubh.2025.1703689.

18. Yin Q (2025) Data privacy rights in health data sharing: a government-centric paradigm in China. International Data Privacy Law, 15(3):238-255, DOI:10.1093/idpl/ipaf007.

19. Schoolcraft D, Meltzer AC, Sangal R, Terry AT, Robertson K, Buckland D, Motalib S, Genes N, Vukmir R, Waseem T (2026) Health Insurance Portability and Accountability Act liability in the age of generative artificial intelligence. JACEP Open, 7(2):100317, DOI:10.1016/j.acepjo.2025.100317.

20. Rezaeikhonakdar D (2024) AI chatbots and challenges of HIPAA compliance for AI developers and vendors. Journal of Law, Medicine & Ethics, 51(4):988-995,

DOI:10.1017/jme.2024.15.