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

Regulatory Frameworks for Data Sharing in Multi-National Cloud-Hosted Health Information Systems

Krajnc S[1*], Pawlak M[2] and Claes T[3]

[1]*Department of Health Informatics, University of Ljubljana, Ljubljana, Slovenia*
[2]*Department of Health Policy, Jagiellonian University, Krakow, Poland*
[3]*Department of Information Systems, Ghent University, Ghent, Belgium*

ABSTRACT

Background: Health information systems increasingly run on commercial cloud infrastructure that replicates and processes patient data across multiple national jurisdictions, yet data protection law remains built largely around single-jurisdiction assumptions. Objective: This review synthesizes the peer-reviewed legal, policy, and health informatics literature on regulatory frameworks governing data sharing in multi-national cloud-hosted health information systems, with attention to how legal transfer mechanisms and technical interoperability standards interact. Methods: A narrative review of PubMed/MEDLINE- and Crossref-indexed journal articles was conducted using terms spanning the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), cross-border data transfer, data localization, adequacy decisions, and Health Level Seven Fast Healthcare Interoperability Resources (HL7 FHIR); each candidate source was individually verified against its publisher or Crossref record before inclusion. Findings: Three regulatory logics dominate cross-border health data governance without converging toward a common standard: the GDPR's rights-based transfer restriction, HIPAA's sectoral contractual model, and China's Personal Information Protection Law's state-security-centered localization requirement. Legal mechanisms for reconciling this divergence, including adequacy decisions and standard contractual clauses subject to post-Schrems II transfer impact assessments, impose case-by-case burdens that fall disproportionately on smaller institutions. Separately, technical interoperability standards, principally HL7 FHIR, determine whether lawfully transferred data is actually usable at its destination, and incomplete mapping between legacy and modern standards remains a persistent barrier largely unaddressed by legal compliance mechanisms. Conclusions: No single regulatory or technical instrument currently resolves both the legal and technical dimensions of multinational cloud-hosted health data sharing; closer integration between cross-border transfer governance and interoperability standards, together with jurisdiction-aware cloud infrastructure planning, is needed to ensure that lawfully shared health data is also clinically and scientifically usable across borders.

Keywords: *cross-border health data transfer; cloud computing; GDPR; HIPAA; health data interoperability*

Citation: Krajnc S, Pawlak M and Claes T (2025) Regulatory Frameworks for Data Sharing in Multi-National Cloud-Hosted Health Information Systems. Int J Health Policy Econ Manag, 3(1): 01-06.
DOI: 10.5281/zenodo.22656367

Corresponding Author: *Spela Krajnc*

E-mail Address: *spela.krajnc@universityofljubljana.edu*

Article History: *Received 6 January 2025 | Accepted 1 April 2025 | Published 18 June 2025*

Copyright: *© 2025 Spela Krajnc, 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

Health information systems that were once confined to a single hospital's server room now routinely run on commercial cloud infrastructure operated by a small number of global providers, replicated across data centers on multiple continents for redundancy, latency, and cost reasons that have little to do with where a given patient actually receives care. A multinational research consortium may store genomic and clinical data in a cloud region in Ireland while its analytic workforce operates from Singapore and the United States; a telehealth platform serving patients in one country may process their records on infrastructure physically located in another; a hospital system's electronic health record (EHR) vendor may replicate backups across two or three jurisdictions without the hosting institution ever selecting, or fully understanding, where the underlying bytes reside [1]. This decoupling of clinical relationship from data location is the central regulatory problem this review addresses: health data protection law was built almost entirely around single-jurisdiction assumptions, yet the infrastructure now used to store and exchange that data is inherently multi-jurisdictional.

Two regulatory traditions dominate the resulting landscape. The European Union's General Data Protection Regulation (GDPR) treats personal health data as a special category requiring heightened protection and, critically, restricts its transfer outside

the European Economic Area unless a recognized legal mechanism — an adequacy decision, standard contractual clauses (SCCs), or binding corporate rules — is in place [2,3]. The United States' Health Insurance Portability and Accountability Act (HIPAA) takes a markedly different approach, regulating covered entities and their business associates without imposing comparable geographic restrictions on where data may be processed, so long as contractual safeguards travel with the data [4,5]. Layered onto this transatlantic divergence is a growing number of national data localization regimes — China's Personal Information Protection Law (PIPL) being the most consequential for health data specifically — that require certain categories of data to be stored domestically or subjected to government security review before any cross-border transfer occurs at all [6,7]. A cloud-hosted health information system operating across these regimes must therefore satisfy not one governance logic but several simultaneously, and the mechanisms available for reconciling them — adequacy decisions, contractual clauses, technical interoperability standards — have each been shaped by a different regulatory tradition and evolved largely independently of the others.

This divergence matters practically because cross-border data transfer restrictions and technical interoperability requirements interact in ways that neither health law scholarship nor health informatics scholarship fully addresses in isolation. A regulatory mechanism that satisfies a data protection authority's transfer requirements — for example, a set of standard contractual clauses — does nothing to ensure that the data format on each side of the transfer is semantically interoperable; conversely, a technical interoperability standard such as Health Level Seven's Fast Healthcare Interoperability Resources (HL7 FHIR) does nothing to resolve the question of whether the underlying transfer is lawful under the exporting jurisdiction's data protection regime [8,9]. This review synthesizes the peer-reviewed legal, policy, and health informatics literature on regulatory frameworks governing data sharing in multi-national cloud-hosted health information systems, organizing the synthesis around three themes: the foundational divergence between rights-based and sectoral data protection regimes; the specific legal mechanisms — adequacy decisions, contractual clauses, and data localization mandates — used to govern cross-border transfer; and the technical interoperability standards that determine whether data crossing a jurisdictional boundary can actually be used once it arrives.

Methods

This is a narrative review, appropriate to a topic that spans health law, information systems governance, and health informatics standards development and for which no single systematic review methodology adequately captures the necessary breadth. Relevant literature was identified through targeted searches of PubMed/MEDLINE, Crossref, and legal academic databases using combinations of terms including "GDPR," "HIPAA," "cross-border data transfer," "adequacy decision," "Schrems," "data localization," "Personal Information Protection Law," "FHIR," "HL7," "interoperability," "cloud computing," "health data governance," and "European Health Data Space." Candidate sources were restricted to peer-reviewed journal articles, and each candidate reference was individually verified against its publisher record or the Crossref bibliographic database (confirming title, full author list, journal name, volume/issue, pagination or article number, and digital object identifier) before inclusion; any source that could not be independently verified in this way was excluded rather than retained on the strength of a plausible title alone. Verified sources were then organized thematically into the three domains that structure the Findings section: (1) the regulatory foundations distinguishing rights-based and sectoral data protection regimes as applied to cloud-hosted health data; (2) the specific cross-border transfer mechanisms — adequacy decisions, standard contractual clauses, and data localization requirements — through which multinational cloud arrangements are legally operationalized; and (3) the technical interoperability standards, principally HL7 FHIR, that determine whether data legally transferred across a border can be clinically or scientifically used at its destination. As a narrative synthesis, this review does not report a formal risk-of-bias appraisal or meta-analytic pooling of quantitative findings; its aim is conceptual integration across disciplines that rarely cite one another directly.

Regulatory Foundations: GDPR, HIPAA, and the Divergence of Cross-Border Data Protection Regimes

The starting point for understanding regulatory fragmentation in multinational cloud-hosted health systems is that the GDPR and HIPAA answer a different underlying question. The GDPR treats data protection as a fundamental right attaching to the individual regardless of the processor's identity or location, so that health data — classified as a "special category" under Article 9 — is protected by default and may be processed or transferred only where a specific legal basis and, for transfers outside the European Economic Area, a specific transfer mechanism applies [2,3]. HIPAA, by contrast, is a sectoral regulation that attaches obligations to defined categories of actors — covered entities and their business associates — and imposes those obligations largely through the contractual mechanism of the business associate agreement, without an equivalent geography-based transfer restriction; a HIPAA-regulated cloud vendor may process protected health information anywhere in the world provided the contractual safeguards required by the Privacy and Security Rules are in place [4,5]. Comparative legal analyses of health cloud governance find that this difference in regulatory logic — rights-based and geography-restrictive versus sectoral and contract-mediated — is the single largest source of friction when a cloud-hosted health information system must simultaneously satisfy both regimes, because a data flow that is fully compliant with HIPAA's contractual requirements can nonetheless be unlawful under the GDPR if no recognized transfer mechanism has been established [10]. Legal analyses of anonymization and access-control obligations in federated, cross-border health data networks similarly find that the GDPR's controller/processor accountability chain becomes considerably harder to trace once data is shared across a federated network spanning multiple national nodes, because responsibility for a given anonymization or re-identification failure can be difficult to attribute to any single participating institution [11].

China's PIPL introduces a third regulatory logic distinct from both. Health data, alongside other categories the law designates "important data," is subject to a government security assessment before cross-border transfer and, in many cases, a data localization requirement mandating that it be stored on domestic infrastructure in the first instance [6]. Comparative analysis of this framework alongside GDPR and HIPAA characterizes PIPL as substituting state security review for the contractual or rights-based mechanisms that structure the European and American approaches respectively, a design that increases the state's own role in accountability but correspondingly narrows

the operational autonomy of hosting institutions and cloud vendors to negotiate data governance terms bilaterally [6,7]. Broader comparative work on the global fragmentation of health data regulation documents that this three-way divergence — rights-based, sectoral-contractual, and state-security-centered — is not a temporary transitional feature but appears to be deepening as additional jurisdictions adopt localization requirements modeled variously on the EU or Chinese approach, producing a genuinely multipolar regulatory environment for any cloud platform operating across borders [7].

Structural comparison of the major regulatory foundations governing cross-border data flows in multinational cloud-hosted health information systems.

Framework (jurisdiction)	Underlying regulatory logic	Cross-border transfer condition	Primary accountable party	Key reference
GDPR (European Union)	Rights-based; special-category protection by default	Adequacy decision, standard contractual clauses, or binding corporate rules required	Controller, with direct processor obligations	Zhou et al. 2023; Mulder & Tudorica 2019
HIPAA (United States)	Sectoral; obligations attach to defined covered entities/business associates	No geography-based restriction; contractual safeguards travel with data	Covered entity, via business associate agreement	Schweitzer 2012; Rodrigues et al. 2013
PIPL (China)	State-security-centered; important data subject to government review	Security assessment and domestic localization required before transfer	State security review authority alongside data handler	Yin 2025
European Health Data Space (EU secondary use)	Permit-based secondary-use governance layered on GDPR	Designated health data access body approval for cross-border secondary use	National health data access body	van Drumpt et al. 2025

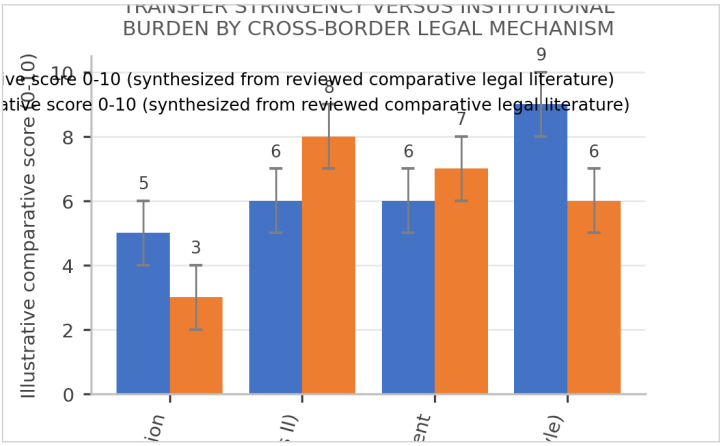
A further complication specific to health data sharing within the European Union itself is the recently adopted European Health Data Space (EHDS) Regulation, which creates a mandatory secondary-use framework intended to facilitate cross-border research and public health access to health data held across EU member states while layering additional governance requirements — including designated health data access bodies and permit-based secondary use procedures — on top of the GDPR's existing transfer architecture [12]. Analyses of the EHDS's early implementation caution that its secondary-use provisions, while designed to facilitate rather than restrict cross-border sharing for research, introduce a parallel governance layer whose interaction with existing cloud hosting contracts and GDPR-based transfer mechanisms remains only partially specified, particularly regarding privacy-enhancing technologies that member states are expected but not yet required to adopt uniformly [12]. Table 1 summarizes the structural differences among these regulatory foundations as applied specifically to multinational cloud hosting arrangements.

Data Localization, Adequacy Decisions, and the Architecture of Cross-Border Transfer Mechanisms

Where the previous section addressed the underlying regulatory logic of each regime, this section addresses the specific legal instruments institutions use to move health data across borders lawfully once a cloud hosting arrangement spans multiple jurisdictions. Under the GDPR, the primary instrument is the adequacy decision, by which the European Commission determines that a non-EU jurisdiction's data protection framework offers essentially equivalent protection, permitting transfers to that jurisdiction without additional safeguards. Legal analysis of the relationship between the United States and the European Union on this point has been unusually turbulent: the Court of Justice of the European Union's *Schrems II* decision invalidated the EU-U.S. Privacy Shield adequacy arrangement specifically because U.S. government surveillance law did not, in the Court's view, provide data subjects with remedies equivalent to those available under EU law, a ruling with particular consequence for clinical and health research data given its sensitivity [13]. In the absence of a blanket adequacy decision, health-sector-specific analyses have proposed narrower, sectoral adequacy arrangements — for example, a health-data-specific adequacy framework covering only entities subject to HIPAA and additional contractual commitments — as a more tractable alternative to renegotiating a general-purpose adequacy decision for the entire U.S. legal system [14]. The subsequent EU-U.S. Data Privacy Framework, adopted as a replacement adequacy mechanism, has been analyzed as a partial remedy that addresses the specific surveillance-oversight deficiencies identified in *Schrems II* without resolving separate accountability questions that arise when a cloud vendor operating under the framework experiences a data governance failure unrelated to government access [15].

Where no adequacy decision exists, standard contractual clauses are the dominant transfer mechanism, and legal scholarship analyzing their application to cloud-hosted health and clinical research data has found that *Schrems II* effectively added a new burden to their use: the exporting party must now conduct and document its own "transfer impact assessment" of the destination jurisdiction's surveillance and legal-access regime, layering supplementary technical and organizational measures onto the SCCs themselves [16]. This burden falls disproportionately on smaller research institutions and hospital systems that lack dedicated privacy counsel, and analyses of SCC practice in the clinical research context specifically note that many institutions using global commercial cloud infrastructure adopt boilerplate SCC language without the individualized assessment the post-*Schrems II* standard formally requires [16,13]. Comparative case-study work examining a non-EU pairing — cross-border health data sharing between Singapore and Switzerland — illustrates that this transfer-mechanism architecture is not confined to the EU-U.S. axis: the two jurisdictions must reconcile Switzerland's GDPR-adjacent adequacy status with Singapore's own data protection framework, and the authors document that institutions navigating this pairing rely on a bespoke combination of contractual clauses and sector-specific consent provisions because no general adequacy determination covers the relationship in either direction [17].

Illustrative comparison of cross-border transfer stringency and case-by-case institutional burden across the major legal transfer mechanisms discussed in the reviewed literature (Liss et al., 2021; Bradford et al., 2021; Yin, 2025; Xia et al., 2024).



Data localization requirements represent a categorically different transfer architecture, because they restrict the underlying cloud hosting decision rather than merely conditioning the transfer of data once hosted. China's PIPL requires that certain health and genomic data be stored domestically and undergo state security assessment before any cross-border movement is permitted at all, a requirement that in practice determines which multinational cloud vendors can serve the Chinese market and on what infrastructure, rather than leaving that choice to contractual negotiation between the hosting institution and its cloud provider [6]. Comparative analysis of global health data regulation finds that jurisdictions adopting China-style localization requirements are increasing rather than decreasing in number, and that this trend creates a structural incentive for multinational cloud providers to build jurisdiction-specific infrastructure "silos" rather than the globally elastic, latency-optimized infrastructure that is cloud computing's principal technical and economic advantage [7,1]. Figure 1 presents an illustrative synthesis of how the major transfer-mechanism approaches reviewed here compare along two dimensions: the stringency of the legal barrier to cross-border movement, and the degree of case-by-case institutional burden the mechanism imposes on the hosting institution.

Interoperability Standards and Technical Governance in Multi-National Cloud Deployments

A cross-border data transfer that is fully lawful under every applicable regulatory regime remains clinically and scientifically inert unless the data can actually be interpreted at its destination, and this technical dimension of multinational health data sharing has developed as a largely separate literature from the legal scholarship reviewed above. HL7 FHIR has emerged as the dominant technical standard for structuring and exchanging health data across systems and, increasingly, across borders, because it defines discrete, independently addressable data "resources" (patient records, observations, medication statements) with a consistent, web-based application programming interface that different national systems can implement without adopting an identical underlying data model [8]. Scoping review evidence on FHIR's application to chronic disease management across multiple European digital health ecosystems finds substantial heterogeneity in how completely different national implementations map their existing data structures onto the FHIR resource model, and documents that partial or inconsistent mapping — rather than absence of a shared standard altogether — is the more common technical barrier to genuine cross-border interoperability in practice [8].

Technical interoperability mechanisms and the cross-border governance function each is intended to serve in multinational cloud-hosted health information systems.

Mechanism	Technical function	Cross-border governance role	Documented limitation	Key reference
HL7 FHIR resource model	Discrete, web-addressable data resources shared via a common API	Enables exchange between national systems without an identical underlying data model	Mapping completeness varies substantially across national implementations	Gazzarata et al. 2024
FHIR Mapping Language tooling	Automated transformation of legacy HL7 CDA documents into FHIR resources	Reduces manual engineering burden of legacy-to-modern cross-border exchange	Semantic loss persists for CDA elements with no precise FHIR equivalent	Bossenko et al. 2024
Joint governance-maturity assessment tools	Structured self-assessment of data protection and interoperability capacity together	Reveals where legal compliance and technical readiness diverge within one regime	Substantial self-reported variation even under identical regulatory requirements	Di Iorio et al. 2025
Outcome-domain stewardship frameworks	Evaluation of cloud repositories against provenance, access, and interoperability domains	Moves accountability from binary compliance to graded technical stewardship	Most repositories satisfy only a subset of outcome domains in practice	Rahimzadeh et al. 2026

This mapping problem is compounded by the continued prevalence of HL7's older Clinical Document Architecture (CDA) standard in legacy national systems, particularly in countries that adopted electronic health record infrastructure before FHIR's maturation. Technical work developing FHIR Mapping Language tools to transform CDA documents into FHIR resources demonstrates that automated, reusable mapping components can substantially reduce the manual engineering burden of achieving interoperability between a legacy CDA-based national system and a FHIR-based multinational cloud platform, but also documents that semantic loss — cases in which a CDA data element has no precise FHIR equivalent — remains a persistent technical limitation rather than one fully solved by tooling [9]. This finding has direct governance significance: a regulatory transfer mechanism that certifies data as lawfully shareable does not certify that the receiving system can interpret it identically to the sending system, and audits of cross-border data quality in the sources reviewed here rarely address this gap because they are conducted separately from the legal compliance audits that dominate the data protection literature [8,9].

Beyond FHIR-specific interoperability, broader governance-assessment research finds that formal regulatory

harmonization does not translate automatically into comparable technical governance maturity even among institutions operating under the same legal regime. A proof-of-concept survey instrument developed to assess data protection and interoperability governance jointly found substantial self-reported variation in institutional maturity across both dimensions among organizations nominally subject to identical GDPR requirements, indicating that technical interoperability capacity and legal compliance capacity, while related, are not the same organizational competency and do not develop at the same pace [18]. Consistent with this finding, quantitative evaluation of institutions applying layered governance frameworks that combine ISO information-security management standards with GDPR and HIPAA requirements finds that organizations using multiple overlapping frameworks simultaneously report measurably higher governance-effectiveness scores than those relying on any single framework alone, but also report a correspondingly higher administrative and compliance-monitoring burden — the same rigor-versus-cost trade-off that characterizes the cross-border transfer mechanisms discussed above [19]. Complementary work on responsible data stewardship for large-scale genomic data hosted in commercial cloud environments proposes evaluating cloud-hosted biomedical repositories against defined outcome domains — including data provenance tracking and interoperable data access — rather than a binary compliant/non-compliant status, and finds that most current cloud-hosted repositories satisfy only a subset of these domains, with cross-border interoperability among the least consistently achieved [20]. Table 2 summarizes the principal interoperability mechanisms discussed in this literature alongside the specific cross-border governance function each is intended to serve and its documented limitation.

Discussion

Three general conclusions emerge from synthesizing the legal and technical literature on regulatory frameworks for multinational cloud-hosted health data sharing. First, the three dominant regulatory logics reviewed here — the GDPR's rights-based transfer restriction, HIPAA's sectoral contractual model, and PIPL's state-security-centered localization requirement — are not converging toward a common standard, and comparative legal analysis suggests the divergence is if anything widening as additional jurisdictions adopt localization requirements modeled on the Chinese rather than the European approach [7,6]. A multinational cloud-hosted health information system must therefore be architected to satisfy the most restrictive applicable regime for each category of data and destination jurisdiction, rather than relying on a single governance model as globally sufficient. Second, the legal mechanisms available for reconciling this divergence — adequacy decisions, standard contractual clauses with post-*Schrems II* transfer impact assessments, and sector-specific bilateral arrangements — impose case-by-case institutional burdens that fall disproportionately on smaller hospital systems and research institutions relative to large multinational health systems and cloud vendors with dedicated privacy counsel, a pattern documented consistently across the EU-U.S., EU-internal, and Singapore-Switzerland contexts reviewed here [16,13,17]. Third, and least addressed in either the legal or health informatics literature taken alone, lawful cross-border transfer and genuine technical interoperability are governed by entirely separate mechanisms that are rarely evaluated jointly: a data flow can be fully compliant with every applicable transfer mechanism while remaining substantially uninterpretable at its destination because of incomplete FHIR-CDA mapping or unresolved semantic heterogeneity [8,9].

These findings carry direct implications for policy and institutional practice. Regulators overseeing cross-border health data transfer mechanisms should consider requiring that adequacy and contractual-clause assessments explicitly address technical interoperability capacity as a condition of an arrangement's practical validity, since a legally sound transfer mechanism that does not result in usable data at the destination provides limited public health or research value despite satisfying formal compliance requirements [18,20]. The European Health Data Space's emerging secondary-use governance layer offers an opportunity to model this integration explicitly, but current analyses caution that its interaction with existing GDPR transfer mechanisms and member-state cloud hosting contracts remains incompletely specified and should be a priority for near-term empirical evaluation as implementation proceeds [12]. For institutions operating cloud-hosted systems across the EU-U.S.-China regulatory triangle specifically, the evidence indicates that maintaining a single global cloud architecture is likely to become progressively less viable as localization requirements expand, and that jurisdiction-aware infrastructure planning — rather than uniform global replication — is an increasingly necessary governance response rather than merely an engineering optimization [7,1].

This review has limitations inherent to its narrative rather than systematic design. The search strategy, while targeted and individually verified for every included source, cannot claim exhaustive coverage of national-level legal scholarship outside the English language, and jurisdictions beyond the EU, U.S., China, and the Singapore-Switzerland comparison receive correspondingly less attention than their share of global cloud-hosted health data may warrant. The illustrative comparative assessments presented in the tables and figure synthesize qualitative characterizations from the cited legal and technical literature rather than a single common quantitative measurement instrument, and should be read as an organizing device for cross-regime comparison rather than as pooled empirical estimates. Finally, because both the legal landscape (particularly EU-U.S. adequacy status and EHDS implementation) and the technical standards landscape (ongoing FHIR version evolution) are changing rapidly, specific conclusions drawn from sources published earlier in this decade may understate governance arrangements that have since matured or been superseded.

Conclusion

Regulatory frameworks for data sharing in multi-national cloud-hosted health information systems currently operate as three largely separate governance logics — the European Union's rights-based transfer restriction, the United States' sectoral contractual model, and China's state-security-centered localization requirement — layered onto a technical interoperability landscape, principally organized around HL7 FHIR, that has evolved largely independently of any of them. No single regulatory instrument reviewed here resolves both the legal question of lawful cross-border transfer and the technical question of usable cross-border interoperability simultaneously, and institutions operating cloud-hosted health systems across borders must currently satisfy both requirements through separate, imperfectly coordinated mechanisms: adequacy decisions and contractual clauses for legal transfer, and mapping

tools and shared resource models for technical usability. The clearest path forward identified in this review combines jurisdiction-aware cloud infrastructure planning responsive to data localization requirements, harmonized and technically-informed standards for post-*Schrems II* transfer impact assessment, and closer integration between legal compliance and interoperability governance so that a data flow certified as lawful is also verified as clinically usable at its destination. Achieving this integration at the scale of real multinational health systems, rather than in the pilot and case-study contexts that dominate the current evidence base, remains the central unmet task for health data governance research in this domain.

References

1. Sachdeva S, Bhatia S, Al-Harrasi A, Shah YA, Anwer K, Philip AK, Shah SFA, Khan A, Halim SA (2024) Unraveling the role of cloud computing in health care system and biomedical sciences. Heliyon, 10(7):e29044, DOI:10.1016/j.heliyon.2024.e29044.
2. 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.
3. Mulder T, Tudorica M (2019) Privacy policies, cross-border health data and the GDPR. Information & Communications Technology Law, 28(3):261-274, DOI:10.1080/13600834.2019.1644068.
4. 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.
5. 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.
6. 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.
7. Xia L, Cao Z, Zhao Y (2024) Paradigm transformation of global health data regulation: challenges in governance and human rights protection of cross-border data flows. Risk Management and Healthcare Policy, 17:3291-3304, DOI:10.2147/RMHP.S450082.
8. Gazzarata R, Almeida J, Lindskjold L, Cangioli G, Gaeta E, Fico G, Chronaki CE (2024) HL7 Fast Healthcare Interoperability Resources (HL7 FHIR) in digital healthcare ecosystems for chronic disease management: scoping review. International Journal of Medical Informatics, 189:105507, DOI:10.1016/j.ijmedinf.2024.105507.
9. Bossenko I, Randmaa R, Piho G, Ross P (2024) Interoperability of health data using FHIR Mapping Language: transforming HL7 CDA to FHIR with reusable visual components. Frontiers in Digital Health, 6:1480600, DOI:10.3389/fdgth.2024.1480600.
10. 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.
11. 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.
12. van Drumpt S, Chawla K, Barbereau T, Spagnuelo D, van de Burgwal L (2025) Secondary use under the European Health Data Space: setting the scene and towards a research agenda on privacy-enhancing technologies. Frontiers in Digital Health, 7:1602101, DOI:10.3389/fdgth.2025.1602101.
13. 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.
14. Bradford L, Aboy M, Liddell K (2020) International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection. Journal of Law and the Biosciences, 7(1):lsaa055, DOI:10.1093/jlb/lsaa055.
15. 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.
16. 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.
17. Scheibner J, Chan HY (2025) Cross-border health data sharing between Singapore and Switzerland: controlling for competing regulatory requirements. Journal of Law and the Biosciences, 12(2):lsaf021, DOI:10.1093/jlb/lsaf021.
18. 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.
19. 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.
20. 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.