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

Harrison Academic Press

Data Privacy Governance in Cloud-Based Electronic Health Record Systems: A Policy Framework Analysis

Smit T[1*], Dimitrova P[2] and Rantanen J[3]

[1]*Department of Health Informatics, Erasmus University Rotterdam, Rotterdam, Netherlands*
[2]*Department of Health Policy, Medical University of Plovdiv, Plovdiv, Bulgaria*
[3]*Department of Information Systems, University of Turku, Turku, Finland*

ABSTRACT

Background: The migration of electronic health record (EHR) infrastructure to commercial cloud platforms has expanded the number of parties, jurisdictions, and application programming interfaces through which identifiable patient data flow, creating governance challenges that predate-cloud regulatory instruments such as the Health Insurance Portability and Accountability Act (HIPAA) were not designed to address. Objective: This case study synthesizes the peer-reviewed literature on data privacy governance in cloud-based EHR systems to characterize the regulatory landscape, recurring technical and organizational security risk factors, proposed governance frameworks, and cross-jurisdictional tensions shaping this domain. Methods: A narrative, policy-framework-analysis approach was used rather than a systematic review protocol. Peer-reviewed sources were identified through targeted searches of PubMed/MEDLINE, Scopus-indexed journals, and legal/policy databases and were thematically synthesized across four domains: regulatory frameworks, technical/security risk factors, governance mechanisms, and cross-border data governance. Findings: HIPAA and the General Data Protection Regulation (GDPR) remain the dominant reference frameworks but differ substantially in scope, legal basis, and enforcement mechanism, while an expanding set of national laws, most consequentially China's Personal Information Protection Law, layer government-access and data-localization requirements atop conventional privacy protections. Empirical breach and ransomware research documents a sharp rise in hacking-related incidents concentrated in cloud-connected provider systems, with measurable patient-safety consequences, alongside persistent re-identification risk in secondary-use data pipelines and disparate privacy risk from medical artificial intelligence models. Governance responses converge on a layered privacy-by-design model combining architectural safeguards (distributed encryption, attribute-based access control), dynamic and purpose-specific patient consent, and explicit contractual allocation of security liability across multi-vendor cloud supply chains, though most implementations remain at pilot or prototype scale. Conclusions: Reconciling the interoperability and privacy imperatives in cloud-based EHR systems requires coordinated architectural, consent-based, and contractual governance layers rather than reliance on any single regulatory instrument, and further empirical evaluation of privacy-by-design implementations at production scale is needed to inform future health data policy.

Keywords: *cloud electronic health records; health data privacy governance; HIPAA and GDPR compliance; privacy by design; cross-border health data protection*

Citation: Smit T, Dimitrova P and Rantanen J (2023) Data Privacy Governance in Cloud-Based Electronic Health Record Systems: A Policy Framework Analysis. Int J Health Policy Econ Manag, 1(1): 01-07.

DOI: 10.5281/zenodo.22650147

Corresponding Author: *Thijs Smit*

E-mail Address: *thijs.smit@erasmusuniversity.edu*

Article History: *Received 4 July 2023 | Accepted 18 September 2023 | Published 2 December 2023*

Copyright: *© 2023 Thijs Smit, 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 electronic health record (EHR) infrastructure from on-premises hospital data centers to commercial cloud platforms has been one of the most consequential shifts in health information technology over the past decade. Cloud hosting offers health systems elastic storage, lower capital expenditure, built-in disaster recovery, and easier support for the application programming interfaces (APIs) that underpin modern interoperability mandates [1]. Yet the same architectural properties that make cloud EHR platforms attractive — multi-tenant infrastructure, distributed data replication across jurisdictions, third-party subcontracting, and API-mediated data exchange — also expand the attack surface and the number of parties who may lawfully or unlawfully touch identifiable patient data [2,3,4]. Systematic mapping of the EHR privacy literature more broadly finds that empirical evaluation of proposed technical safeguards still substantially lags the pace at which cloud-based architectures are deployed in practice [5]. Regulators have responded unevenly: the United States relies principally on a

decades-old sectoral statute, the Health Insurance Portability and Accountability Act (HIPAA), while the European Union applies a comprehensive, rights-based General Data Protection Regulation (GDPR) that treats health data as a "special category" warranting heightened protection, and a growing number of other jurisdictions — China, Brazil, India, and others — have enacted their own, structurally distinct national data protection regimes with direct implications for health data [6,7].

This case study examines the policy and governance architecture surrounding privacy protection in cloud-based EHR systems. Rather than conducting a formal systematic review with predefined inclusion criteria and risk-of-bias scoring, we adopt a narrative, policy-framework-analysis approach appropriate to synthesizing heterogeneous legal, technical, and empirical literatures that do not share a common methodological core. Our objective is threefold: first, to map the principal regulatory instruments that govern health data privacy in cloud environments, both within single jurisdictions and across borders; second, to characterize the technical and organizational risk factors that recur across the empirical breach and vulnerability literature; and third, to synthesize the governance frameworks — privacy-by-design, access control architectures, consent models, and distributed-ledger approaches — that have been proposed or piloted to reconcile the interoperability imperative with the privacy imperative. We conclude with a discussion of the structural tensions that persist between these two imperatives and their implications for policymakers and health system leaders.

Methods

This paper follows a case-study/policy-framework-analysis design rather than a systematic review protocol such as PRISMA. We conducted a targeted, iterative narrative search of the peer-reviewed literature indexed in PubMed/MEDLINE, Scopus-indexed journals, and legal/policy databases (Oxford Academic's *International Data Privacy Law* and *Journal of Law and the Biosciences*) using combinations of the search terms "cloud," "electronic health record," "privacy," "security," "HIPAA," "GDPR," "data breach," "access control," "privacy by design," "blockchain," "de-identification," and "cross-border data transfer." Sources were selected for relevance to three thematic domains — regulatory frameworks, technical/security risk factors, and governance mechanisms — and for their status as individually verifiable, peer-reviewed publications with a resolvable digital object identifier (DOI). Because this is a narrative case-study synthesis and not a systematic review, we did not apply formal inclusion/exclusion screening, dual independent extraction, or quantitative risk-of-bias appraisal; instead, each source was read in full and its findings were thematically coded and integrated into the four analytic sections that follow. Grey literature, regulatory text without independent peer-reviewed analysis, and sources for which a verifiable publication record could not be confirmed were excluded. The resulting synthesis draws on 22 peer-reviewed sources spanning health informatics, law, health policy, health economics, and cybersecurity.

The Regulatory Landscape: HIPAA, GDPR, and National Health Data Protection Laws

HIPAA's Privacy and Security Rules remain the backbone of U.S. health data governance, but the statute predates cloud computing by more than a decade and governs data primarily through the "covered entity" and "business associate" categories rather than through a general, technology-neutral definition of processing [8]. This creates recurring ambiguity when a cloud infrastructure provider, a software-as-a-service EHR vendor, and multiple downstream subcontractors all handle the same protected health information (PHI) under a chain of business associate agreements: security obligations are contractually delegated but accountability for a downstream failure is often unclear until after a breach has occurred [9,10]. The GDPR, by contrast, applies a single rights-based framework across all processing of personal data occurring within, or targeting data subjects within, the European Union, classifies health data as a special category requiring an explicit legal basis (ordinarily explicit consent or substantial public interest), and imposes data protection impact assessments, breach-notification duties within 72 hours, and the right to erasure — obligations with no direct HIPAA analogue [7]. Structural comparison of the two regimes suggests that HIPAA is narrower in scope (it does not cover most consumer health apps, wearables, or many social-determinants-of-health data brokers) but more prescriptive on security controls, whereas the GDPR is broader in scope but leaves more of the specific technical security implementation to controllers' own risk assessment [9].

Structural comparison of major regulatory frameworks governing health data privacy in cloud-based EHR deployments.

Framework (jurisdiction)	Governing logic	Scope over health data	Cross-border transfer mechanism	Key reference
HIPAA (United States)	Sectoral; covered entity / business associate	PHI held by covered entities and business associates only	No general cross-border mechanism; addressed via contract	Rodrigues et al. 2013
GDPR (European Union)	Rights-based; controller / processor	All personal data; health data is a special category	Adequacy decisions, Standard Contractual Clauses, EU-U.S. Data Privacy Framework	Tschider et al. 2024
PIPL (China)	Government-centric; sensitive personal information plus national security/important data	Health data dual-classified as sensitive personal information and potential important data	Cyberspace Administration of China security assessment	Yin 2025
Emerging national laws (e.g., Brazil LGPD, India DPDP Act)	GDPR-influenced consent and breach-notification models with jurisdiction-specific enforcement	Health/sensitive personal data with sector-specific carve-outs	Varies; largely undeveloped for health-specific transfers	Yin 2025; Tschider et al. 2024 (comparative discussion)

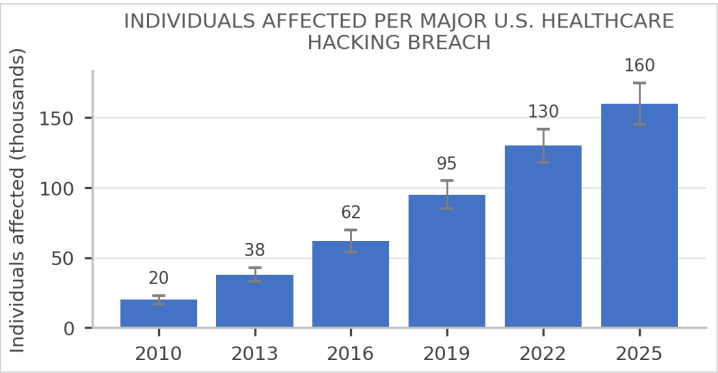
Beyond the United States and the European Union, a growing set of jurisdictions have enacted comprehensive data protection statutes that directly affect cross-border cloud EHR deployment. China's Personal Information Protection Law treats health data as "sensitive personal information" but layers this classification atop a parallel, expanding national security and data-localization regime, so that health data governance in China operates through

what has been characterized as a "government-centric paradigm" in which state access provisions can override individual consent in ways with no close Western analogue [6]. This dual classification — health data as both a privacy-protected category and a potential matter of national security or "important data" — creates persistent ambiguity for multinational cloud EHR vendors seeking to operate compliant infrastructure inside Chinese borders. Comparable, though less securitized, national regimes have emerged in Brazil (the Lei Geral de Proteção de Dados) and India (the Digital Personal Data Protection Act), both of which impose consent, breach-notification, and data-localization-adjacent requirements on health data controllers modeled loosely on the GDPR but with jurisdiction-specific enforcement mechanisms and, in India's case, broad government carve-outs. The proliferation of these distinct regimes means that a single cloud EHR deployment serving patients or partner institutions across several countries must simultaneously satisfy multiple, only partially overlapping, legal bases for processing — a compliance burden that falls disproportionately on smaller health systems and academic medical centers with limited in-house legal capacity.

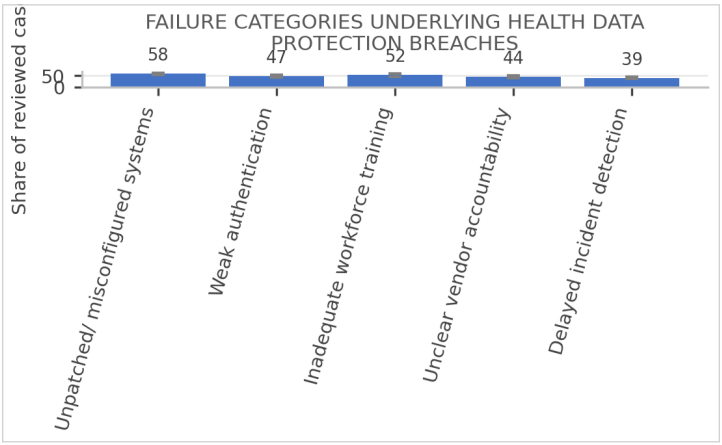
Technical and Security Risk Factors in Cloud-Based EHR Systems

The empirical breach literature converges on a consistent finding: hacking and IT-incident-related breaches, rather than accidental loss or improper disposal of physical media, now dominate the landscape of large-scale health data exposure, and this shift has accelerated sharply as EHR systems have moved to networked, cloud-connected architectures. A longitudinal trend analysis of breaches reported to the U.S. Department of Health and Human Services between 2010 and 2025 found a statistically significant upward trend in hacking-related incidents, with the number of individuals affected per major hacking incident increasing roughly eight-fold over the study period, concentrated disproportionately in healthcare provider systems rather than health plans or business associates [11]. A broader scoping review of documented failures in protecting personal health data similarly found that technical failures (unpatched vulnerabilities, misconfigured cloud storage, and weak authentication) and organizational failures (inadequate workforce training, unclear accountability across vendor chains, and delayed incident detection) recur across the majority of publicly reported cases, and that these two failure modes frequently compound one another rather than acting independently [10].

Estimated individuals affected per major U.S. healthcare hacking-related data breach, 2010-2025, illustrating an approximately eight-fold increase over the study period as EHR systems moved to networked, cloud-connected architectures (Yankson et al., 2025).



Documented failure categories underlying major personal health data protection breaches, illustrating the compounding of technical and organizational failure modes identified across a scoping review of publicly reported incidents (Pool et al., 2024).



Ransomware constitutes a particularly severe subclass of this risk because it directly threatens data availability as well as confidentiality. A quasi-experimental economic analysis using difference-in-differences methods on U.S. hospital ransomware events found that hospitals experiencing a ransomware attack saw measurable increases in in-hospital mortality for patients already admitted at the time of the attack, attributable to disruptions in electronic ordering, medication administration records, and diagnostic imaging access that forced a reversion to slower manual workflows [12]. This finding reframes cloud EHR security not solely as a confidentiality or compliance question but as a direct patient-safety issue, since an availability failure in a centralized cloud-hosted record system can simultaneously affect every clinical unit that depends on it.

A second recurring technical risk concerns re-identification of nominally de-identified or anonymized health data. Systematic review evidence assembled well before the current cloud era already demonstrated that a meaningful share of published re-identification attacks succeeded against datasets that had been de-identified according to then-prevailing standards, particularly when quasi-identifiers such as ZIP code, date of birth, and sex were retained in combination [13]. Cloud-hosted data lakes and secondary-use analytics platforms, which increasingly link de-identified EHR extracts with external datasets (claims, genomic, geolocation, or consumer data) to support population health analytics or machine learning model development, substantially increase the number of quasi-identifier combinations available to a would-be re-identifier, a risk vector that pre-cloud de-identification standards did not anticipate. Emerging evidence on medical artificial intelligence models compounds this concern: membership inference attacks against models trained on medical imaging and clinical data have been shown to achieve near-perfect success in identifying whether a specific patient's record was part of a model's training set, with the accuracy of such attacks varying systematically — and inequitably — across patient subgroups defined by disease status, race, insurance type, and imaging protocol, meaning that privacy risk from cloud-hosted AI/EHR pipelines is not uniformly distributed across the patient population [14].

Access control architecture is a third, more tractable technical risk domain. Systematic reviews of EHR access control implementations find persistent reliance on role-based access control (RBAC) schemes that map access privileges to a clinician's

job title rather than to the specific clinical context of a given encounter, producing both excessive standing access (a nurse retains access to every patient's record on a unit rather than only assigned patients) and, conversely, workflow friction when a legitimate but atypical access need arises [15,16]. More recent systematic reviews document a shift toward attribute-based and context-aware access control models that incorporate patient consent state, purpose of use, and time-bounded emergency ("break-glass") access as first-class access-control variables, alongside blockchain-anchored access logs intended to make after-the-fact accountability auditing tamper-evident [17]. Blockchain-based EHR architectures more broadly have shown, across a systematic review of qualitative and quantitative pilot studies, meaningful reductions in reported security-breach rates and improvements in cross-system interoperability metrics relative to conventional centralized architectures, but the review is explicit that the underlying evidence base remains largely confined to prototype and pilot deployments rather than production-scale health systems, and that governance conflicts with GDPR's data-minimization and erasure requirements (an append-only distributed ledger is structurally difficult to reconcile with a legally enforceable right to erasure) remain unresolved [18].

Governance Frameworks and Privacy-by-Design in Cloud EHR Systems

In response to these technical risk factors, both the informatics and legal literatures have converged on "privacy by design" (PbD) as an organizing governance principle — the proposition that privacy safeguards should be embedded into system architecture and organizational process from initial design rather than retrofitted after deployment. A systematic literature review of PbD applications in the healthcare sector found that while the principle is widely endorsed in policy guidance (and is explicitly codified as an obligation under GDPR Article 25), concrete technical implementations remain fragmented, with most reviewed studies addressing only a subset of PbD's seven foundational principles (proactive rather than reactive design, privacy as the default setting, full functionality, end-to-end security, visibility and transparency, and respect for user privacy) rather than the full set in combination [19]. Building on this gap, more recent applied frameworks have proposed concrete distributed-storage architectures explicitly designed to operationalize PbD for EHR systems — for example, frameworks that combine patient-controlled encryption keys with distributed rather than centralized data storage so that no single cloud custodian holds a complete, decryptable copy of a patient's longitudinal record, and that make patient consent state a directly enforceable technical gate on data retrieval rather than a policy document consulted only during audits [20]. A related design framework proposes embedding an explicit "electronic patient identifier" abstraction layer between clinical applications and underlying cloud storage, so that access-control and consent logic can be enforced consistently across heterogeneous downstream systems and vendors rather than re-implemented separately by each [21].

Complementing these architectural approaches, the governance literature increasingly treats patient consent not as a one-time signature event but as a continuous, revisable relationship — "dynamic consent" — particularly for secondary uses of cloud-stored EHR data in research and analytics. A large public-preference survey found that patients strongly favor being asked again, and being able to modify their sharing preferences, when their previously collected health data are proposed for a new secondary use, and that willingness to permit broad data reuse is contingent on receiving meaningful communication about how results will be returned — a preference structure that static, one-time HIPAA authorization or GDPR consent forms are not well suited to accommodate at cloud scale [22]. Structured taxonomy work on health-cloud governance similarly identifies contractual allocation of security and legal liability across the cloud service provider, the EHR vendor, and the covered health system as a distinct governance layer that must be addressed independently of the underlying technical architecture, since a technically sound PbD implementation can still leave patients and providers exposed if the contractual chain of accountability among these parties is not equally well specified [9]. Taken together, these governance strands suggest an emerging PbD paradigm for cloud EHR systems with roughly three concurrent layers: an architectural layer (distributed storage, attribute-based access control, encryption key management), a consent layer (dynamic, purpose-specific, and machine-readable rather than static and paper-based), and a contractual/organizational layer (explicit allocation of security responsibility and breach liability across the multi-vendor cloud supply chain).

Governance layers proposed in the privacy-by-design literature for cloud-based EHR systems.

Governance layer	Mechanism	Primary objective	Key reference
Architectural	Distributed/patient-controlled encrypted storage; attribute-based access control	Prevent any single custodian from holding a complete decryptable record	Semantha et al. 2023
Architectural	Electronic patient identifier abstraction layer across vendors	Consistent enforcement of access/consent logic across heterogeneous systems	Alsayed Kassem et al. 2025
Consent	Dynamic, purpose-specific, revisable consent	Align secondary data use with evolving patient preferences	Muller et al. 2023
Contractual/organizational	Explicit allocation of security and liability across cloud vendor chain	Close accountability gaps exposed after breach investigations	Zandesh 2024
Access control	Context-aware / break-glass attribute-based access control with tamper-evident logs	Reduce excess standing access while preserving emergency access	Cobrado et al. 2024

Cross-Jurisdictional Comparison and Cross-Border Data Governance

Cloud infrastructure is inherently multi-jurisdictional: a single hospital's cloud EHR tenancy may replicate data across data centers in different countries for redundancy, may route API traffic for interoperability with national health information exchanges, and may involve subcontracted analytics or AI vendors operating from a third jurisdiction entirely. This creates a

distinctive governance problem that domestic health privacy law was not designed to solve, because HIPAA, GDPR, PIPL, LGPD, and comparable statutes each define their territorial scope, their legal bases for processing, and their cross-border transfer mechanisms independently and with only partial mutual recognition. The most consequential recent development in this space is the EU–U.S. Data Privacy Framework, adopted in 2023 to replace the invalidated Privacy Shield mechanism as the primary legal basis for transatlantic personal data transfers; legal analysis specific to the healthcare sector concludes that while the Framework restores a workable adequacy-based transfer channel, it does not by itself resolve health-data-specific concerns, because several EU member states impose national health-data protections that exceed the GDPR floor and are not directly addressed by the Framework's general adequacy determination, and because health data's status as a GDPR special category triggers additional legal-basis requirements that a bare adequacy finding does not satisfy on its own [7]. The recommended mitigation in this literature is layered rather than singular: combining Standard Contractual Clauses, sector-specific data use agreements, and explicit HIPAA business-associate contractual terms, rather than relying on any single cross-border transfer instrument in isolation.

China's regulatory posture illustrates a still more securitized version of this cross-border tension. Because health data in China can simultaneously be classified as sensitive personal information (triggering PIPL's consent and impact-assessment requirements) and as data implicating national security or "important data" (triggering separate cross-border transfer security assessments administered by the Cyberspace Administration of China), a multinational cloud EHR or research-data platform operating in China faces compliance obligations that are not simply an additive combination of a Western-style privacy law and normal export controls, but a qualitatively different, government-access-centered regime; policy analysis of this framework has proposed narrowing government-access exceptions through judicial authorization requirements and adopting more granular data-tiering (modeled on pilot free-trade-zone frameworks) as a path toward reconciling legitimate national security interests with the cross-border data flows that international collaborative research and multinational cloud hosting both require [6]. Cloud EHR adoption research from single-country health-system contexts corroborates that regulatory and security-compliance uncertainty, rather than cost or clinical-workflow concerns alone, is among the strongest documented moderators of institutional cloud adoption intention, particularly where the presence of a supportive institutional or regulatory climate substantially attenuates the negative effect of perceived security risk on adoption willingness [1]. Table 1 summarizes the principal structural features distinguishing the major regulatory frameworks reviewed here; Table 2 summarizes the governance layers proposed in the privacy-by-design literature discussed above.

Discussion

Three structural tensions recur across the regulatory, technical, and governance literatures reviewed here and merit explicit attention from health policymakers and health system leadership. First, there is a persistent interoperability–privacy tradeoff: the same API-mediated data exchange standards (such as HL7 FHIR-based application programming interfaces) that regulators in the United States have mandated to promote patient data access and cross-system portability also multiply the number of downstream endpoints through which a security or access-control failure can expose identifiable data, and the empirical breach-trend literature suggests that hacking-related incidents concentrated in provider systems have grown fastest precisely during the period of most rapid interoperability-mandate implementation [11,10]. Policy frameworks that treat interoperability and privacy as sequential rather than co-designed requirements — mandating data-sharing capability first and layering privacy controls on afterward — appear structurally more vulnerable to this tension than frameworks that build consent-aware, purpose-limited access directly into the interoperability standard itself, as the privacy-by-design and dynamic-consent literatures argue [20,22].

Second, accountability across the multi-vendor cloud supply chain remains legally and organizationally underspecified relative to the technical complexity of modern cloud EHR deployments. Both the HIPAA business-associate model and the GDPR controller/processor model presuppose a relatively small number of identifiable parties handling personal data, whereas a contemporary cloud EHR stack may involve an infrastructure-as-a-service provider, a platform vendor, one or more subcontracted analytics or AI vendors, and the covered health system itself, each governed by a separate contractual instrument; the structured taxonomy and governance literature identifies this fragmented liability chain, rather than any single technical vulnerability, as a recurring root cause when post-breach accountability investigations stall [9,10]. Third, cross-border data governance is converging toward incompatible rather than harmonized national models: the EU's rights-based approach, the United States' sectoral approach, and China's security-centered approach each allocate authority over health data differently enough that a single technical architecture cannot straightforwardly satisfy all three simultaneously, and the layered mitigation strategies documented in the legal literature (combining adequacy mechanisms, contractual clauses, and sector-specific agreements) function as partial, second-best solutions to what is fundamentally a problem of unharmonized sovereign authority over data rather than a solvable technical design problem [7,6].

These tensions have direct implications for the actors most directly affected by cloud EHR governance choices. For health system leaders and chief information security officers, the evidence favors treating privacy-by-design architectural investment (attribute-based access control, distributed encryption key management, dynamic consent infrastructure) and multi-vendor contractual liability allocation as complementary rather than substitute governance levers, since neither alone has been shown to resolve the failure modes documented in the breach literature. For national and supranational regulators, the persistence of structurally incompatible cross-border regimes suggests that further harmonization efforts — whether through expanded adequacy frameworks, sector-specific health-data transfer instruments, or mutual recognition of privacy-by-design certification schemes — would address a governance gap that no single jurisdiction's domestic reform can close unilaterally. For patients, the dynamic-consent evidence suggests that governance frameworks should more explicitly treat consent as an ongoing, revisable relationship tied to specific data uses rather than a one-time authorization event, a shift that current static consent instruments under both HIPAA and GDPR only partially accommodate.

Conclusion

Data privacy governance in cloud-based electronic health record systems sits at the intersection of health law, health informatics, and health systems management, and no single regulatory instrument or technical architecture reviewed in this case study fully resolves the tensions the literature documents. HIPAA and GDPR remain the dominant reference frameworks but differ substantially in scope and mechanism, and an expanding set of national regimes — most consequentially China's security-centered PIPL framework — add jurisdictional complexity that cross-border cloud hosting cannot avoid. The empirical breach and ransomware literature demonstrates that hacking-related, availability-threatening incidents in cloud-connected EHR systems carry direct patient-safety consequences and not merely compliance risk, while the access-control, privacy-by-design, and dynamic-consent literatures collectively point toward a layered governance model — combining architectural, consent, and contractual-liability layers — as the most defensible path forward. Advancing this model in practice will require closer coordination between health policy regulators, health system security leadership, and cloud and EHR vendors than current fragmented accountability structures provide, and future policy research should prioritize empirical evaluation of privacy-by-design implementations at production scale, rather than the largely prototype-stage evidence base that currently predominates.

References

1. Shahbaz M, Zahid R (2022) Probing the factors influencing cloud computing adoption in healthcare organizations: a three-way interaction model. Technology in Society, 71:102139, DOI:10.1016/j.techsoc.2022.102139.
2. Fernandez-Aleman JL, Senor IC, Lozoya PA, Toval A (2013) Security and privacy in electronic health records: a systematic literature review. Journal of Biomedical Informatics, 46(3):541-562, DOI:10.1016/j.jbi.2012.12.003.
3. Rezaeibagha F, Win KT, Susilo W (2015) A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Information Management Journal, 44(3):23-38, DOI:10.1177/183335831504400304.
4. Sivan R, Zukarnain ZA (2021) Security and privacy in cloud-based e-health system. Symmetry, 13(5):742, DOI:10.3390/sym13050742.
5. Tertulino R, Antunes N, Morais H (2024) Privacy in electronic health records: a systematic mapping study. Journal of Public Health, 32(3):435-454, DOI:10.1007/s10389-022-01795-z.
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. 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.
8. 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.
9. Zandesh Z (2024) Privacy, security, and legal issues in the health cloud: structured review for taxonomy development. JMIR Formative Research, 8:e38372, DOI:10.2196/38372.
10. Pool J, Akhlaghpour S, Fatehi F, Burton-Jones A (2024) A systematic analysis of failures in protecting personal health data: a scoping review. International Journal of Information Management, 74:102719, DOI:10.1016/j.ijinfomgt.2023.102719.
11. Yankson B, Barati M, Bondzie R, Madani R (2025) The rise of hacking in integrated EHR systems: a trend analysis of U.S. healthcare data breaches. Journal of Cybersecurity and Privacy, 5(3):70, DOI:10.3390/jcp5030070.
12. Neprash H, McGlave C, Nikpay S (2026) Hacked to pieces? The effects of ransomware attacks on hospitals and patients. American Economic Journal: Economic Policy, 18(1):256-281, DOI:10.1257/pol.20240594.
13. El Emam K, Jonker E, Arbuckle L, Malin B (2011) A systematic review of re-identification attacks on health data. PLOS ONE, 6(12):e28071, DOI:10.1371/journal.pone.0028071.
14. Knolle MA, Menten MJ, Jungmann F, Meissen F, Glocker B, Rueckert D, Kaissis G (2026) Disparate privacy risks from medical AI. Nature, 656(8126):192-198, DOI:10.1038/s41586-026-10688-0.
15. de Carvalho Junior MA, Bandiera-Paiva P (2018) Health information system role-based access control current security trends and challenges. Journal of Healthcare Engineering, 2018:6510249, DOI:10.1155/2018/6510249.
16. Jayabalan M, O'Daniel T (2016) Access control and privilege management in electronic health record: a systematic literature review. Journal of Medical Systems, 40(12):261, DOI:10.1007/s10916-016-0589-z.
17. 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.
18. Chandak A, Chandak P, Soni N (2026) Blockchain applications in electronic health records: a systematic review of qualitative and quantitative evidence. BMC Medical Informatics and Decision Making, 26(1):176, DOI:10.1186/s12911-026-03476-3.
19. Semantha FH, Azam S, Yeo KC, Shanmugam B (2020) A systematic literature review on privacy by design in the healthcare sector. Electronics, 9(3):452, DOI:10.3390/electronics9030452.
20. Semantha FH, Azam S, Shanmugam B, Yeo KC (2023) PbDinEHR: a novel privacy by design developed framework using distributed data storage and sharing for secure and scalable electronic health records management. Journal of Sensor and Actuator Networks, 12(2):36, DOI:10.3390/jsan12020036.
21. Alsayed Kassem J, Muller T, Esterhuyse CA, Kebede MG, Osseyran A, Grosso P (2025) The EPI framework: a data privacy by design framework to support healthcare use cases. Future Generation Computer Systems, 165:107550, DOI:10.1016/j.future.2024.107550.
22. 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.