Sarcouncil Journal of Multidisciplinary

ISSN(Online): 2945-3445

Volume- 06| Issue- 06| 2026

Research Article **Received:** 13-05-2026 | **Accepted:** 08-06-2026 | **Published:** 23-06-2026

Learning from Global Models: A Comparative Analysis of Health Data Governance Frameworks and Their Implications for U.S. Health Information Policy and System Design

***Omonye Jones Silas*[1] *and Solomon Doe Adjaottor*[2]**

[1]*University of the Cumberlands, USA.*

[2]*Department of Accounting and Finance, Kwame Nkrumah University of Science and Technology, Ghana.*

Abstract: Health data governance has become a critical component of modern healthcare systems due to increasing digitization, large-scale data sharing, and the growing importance of data-driven research and innovation. This review identifies key governance models and examines their implications for U.S. health information policy and system design. Using the Boolean function, keywords were used to search for and source articles, which were later screened. A total of eleven articles were finally obtained and synthesized for this study. The literature shows that normative governance frameworks across countries share common principles such as protection of individual rights, transparency, accountability, and public interest. However, fragmentation exists in terminology, enforcement mechanisms, and lifecycle coverage, particularly in the governance of secondary data reuse. Organizational governance studies highlight the importance of institutional structures, including clearly defined roles, governance committees, stewardship responsibilities, and standardized procedures. Evidence also shows that governance effectiveness depends on infrastructure, workforce training, and sustainable institutional capacity. Technical governance architectures introduce new approaches that embed governance rules directly into digital infrastructures. Blockchain-based systems strengthen security, transparency, and auditability through decentralized ledgers and smart contracts, while federated learning enables privacy-preserving data analysis by keeping sensitive patient data at local sources. Operational and design governance further translate governance principles into daily practice through privacy- and security-by-design, structured data quality management, and formal consent and access control mechanisms. The findings suggest that strengthening lifecycle governance, institutional capacity, system design, and workforce training can support more secure, interoperable, and trustworthy health information systems.

Keywords: Health data, Data governance frameworks, Health information, Blockchain, Federated Learning.

INTRODUCTION

Hospitals are the most significant health data producers in terms of clinical data and administrative data (Wang *et al*., 2022). Health data is generated in hospitals from patient registration, doctor and nurse examinations, laboratory examinations, and drug prescriptions (Oderkirk & Ronchi, 2018). Remote Patient Monitoring (RPM) is one of the healthcare applications used to collect and record vital signs of patients outside of physical clinic locations. RPM includes different types of sensors that can be worn or implanted. These sensors send information through wireless communication to a local base station, which further sends the information to a central monitoring station and alarm the physicians to intervene effectively with the patient's case (Frikha *et al*., 2021). All this data is stored in what is known as "Electronic Health Record".

Electronic health record (EHR) is a digital record that includes certain health information such as personal information, patient medical history, diagnoses, allergies, vital signs, lab data results, and more (Zaabar *et al*., 2021). Health data from EHR can be used for multiple purposes including research, organization planning, health insurance claims, and police work (Skovgaard, Wadmann & Hoeyer, 2019; Li *et al*., 2019; Ministry of Health of the Republic of Indonesia, 2022). Electronic health records provide important and extremely confidential personal information for healthcare assessment and monitoring. As such sharing healthcare information should be carefully managed to preserve the data security (Keshta *et al*., 2020).

Due to its semantic nature, data can decouple from the events they refer to (Alaimo *et al*., 2020) and transform into larger objects (Aaltonen, Alaimo, & Kallinikos, 2021). Data can also increase with use rather than being consumed, get diffused as they travel, and be shared without being depleted (Vassilakopoulou *et al*., 2019). This brings implications for data governance, particularly in the case of sensitive and personal data (Winter & Davidson, 2019), where the regulatory conditions differ from governing non-personal data. In fact, some of the core challenges in sharing personal health data lie in decisions related to data governance, including protecting intellectual property rights and privacy according to the legal

***Corresponding Author:** Omonye Jones Silas

DOI- https://doi.org/10.5281/zenodo.20819595

provisions (Parmiggiani & Grisot, 2020; Utomi *et al*., 2024), and retaining control once data are shared across multiple actors (Van den Broek & Van Veenstra, 2015). In 2018, the European Union introduced the General Data Protection Regulation aiming to bring more clarity to the governance of personal data (European Commission, 2016) which similarly applies to health data.

Information governance (IG) which is closely related to data governance, focuses on developing an infrastructure made up of rules and guidelines for bettering information management in healthcare organizations (Al-Badi & Tarhini, 2018; Oware & Mensah, 2025). The American Health Information Management Association (AHIMA) defines IG as a broad organizational framework for managing information during the life cycle of information, supporting the strategic, operational, legal, and statutory programs and risks in the organization (Al-Badi and Tarhini, 2018). According to the Association of Records Managers and Administrators (ARMA), IG is a strategic framework including standards, processes, roles, and criteria that hold organizations and individuals accountable for creating, organizing, protecting, using and disposition of information by the objectives of the organization (Tse & Chow, 2018). Health Information Governance in healthcare organizations is a critical framework that establishes centralized policies, procedures, and accountabilities for managing patient information effectively (O'Hara, 2019).

Global health data governance frameworks remain fragmented across regulatory, organizational, technical, and operational domains, limiting interoperability, effective oversight, and coherent guidance for strengthening U.S. health information systems. This review aims to identify key governance models and examine their implications for U.S. health information policy and system design. Implementing health data governance helps hospitals improve patient safety and research in the health sector (Li *et al*., 2021; Osifowokan *et al*., 2025). It establishes policy, protects data and information assets, and determines accountabilities and processes for managing data and information (Pan American Health Organization, 2022).

METHODOLOGY

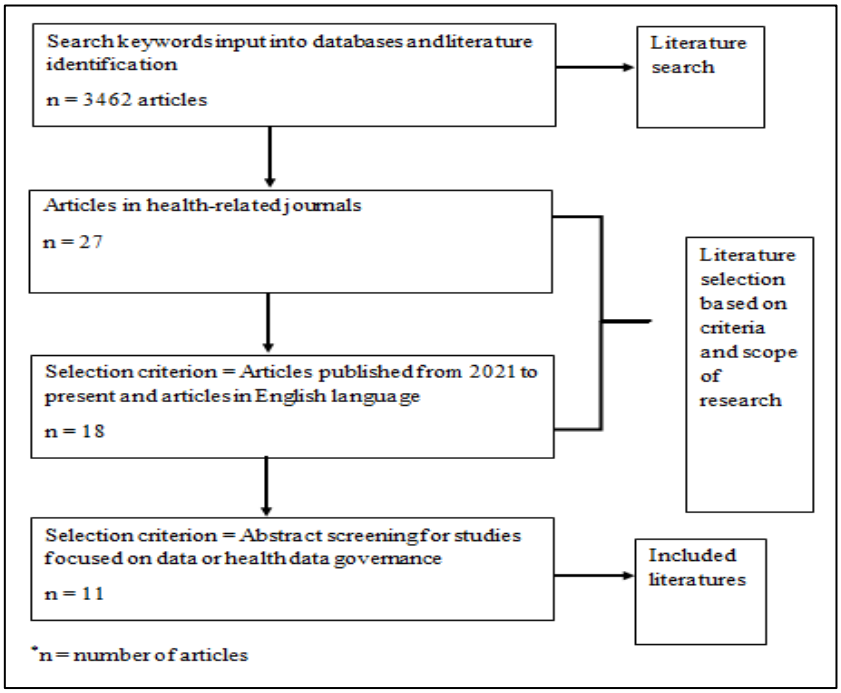
This literature review aims to synthesize and compare data governance frameworks across the globe. Drawing exclusively on 11 high-quality empirical and review studies which integrates findings across health data and general data related studies. A systematic literature review approach was adopted in this study because the subject matter was narrower and more specific to warrant a scoping literature review method. A review protocol was outlined prior to conducting the systematic review, which is in accordance with the review guidelines proposed by (Kitchenham *et al*., 2010). The research questions were first defined, after which the keywords identified in this research were input into databases to select the relevant literature materials. The databases that were used to source literature materials in this study included: Science Direct, Google Scholar, Web of Science, and Research Gate. Search keywords or statements used in this study are as follows:

1. Health Data Governance Frameworks and Their Implications
2. Health AND data OR Information AND Governance OR Stewardship OR Management
3. Health AND data AND governance frameworks AND global models

A selection criterion consisting of documents within health data or data in the general context was used to filter the documents and select relevant literature. A total of 27 literature materials were obtained using the above keywords and criteria for searching literature in the various search engines. Out of this number, only 18 were selected after excluding articles published before 2021 and articles written in languages other than English. The abstracts of 18 resultant studies were screened and studies that that were not related to data or health data governance were excluded from the review. A total of 11 studies satisfied the selection criteria and were thus used in this study. All pertinent information was gathered from the selected literature materials and subsequently synthesized in accordance with the main theme of the research. A thematic analysis was used to discuss the relevant information captured in the literature section.

Publisher: SARC Publisher

PRISMA Flow Diagram Used In this Study



CONCEPTUAL FRAMEWORK MAPS

Conceptual Map 1: Normative & Regulatory Governance

The literature reviewed reveals that normative and regulatory governance forms the foundational layer of global health data governance frameworks. Across contexts, this layer defines the legal authority, ethical principles, and lifecycle scope under which health data are collected, processed, shared, and reused. It illustrates both convergence around core principles and fragmentation in operationalization.

The benchmarking analyses conducted by Marcucci *et al*. (2023a; 2023b) provide a macro-level assessment of 58 data governance frameworks across sectors, including health. Their findings indicate that most frameworks share common normative foundations centered on trust, protection of individual rights, and promotion of public interest. Confidentiality, accountability, transparency, and security are the most frequently cited principles. However, the authors identify a lack of harmonized terminology and inconsistent operational definitions across jurisdictions, which limits cross-border interoperability and policy coherence. A major finding concerns lifecycle governance. Only a minority of frameworks provide comprehensive oversight across the full data lifecycle; from collection and storage to sharing and reuse (Marcucci *et al*., 2023a; 2023b). In particular, governance of secondary data reuse is underdeveloped, despite its central role in research, public health surveillance, and innovation. This gap suggests that while privacy protection is emphasized, frameworks often neglect structured governance mechanisms for socially beneficial reuse. Furthermore, most frameworks are non-binding and lack robust monitoring mechanisms. Dedicated governance bodies are absent in many cases, and participatory processes involving data subjects are rare. Collectively, these results depict a fragmented global governance landscape characterized by normative convergence but institutional and operational weakness.

Ahmed *et al*. (2025) assess the adequacy of established regulatory models involving ISO standards, the General Data Protection Regulation (GDPR), and the Health Insurance Portability and Accountability Act (HIPAA), within blockchain-enabled health systems. Their quantitative analysis of healthcare and IT professionals reveals widespread dissatisfaction with the capacity of these frameworks to address modern technical demands. Participants identified deficiencies in encryption standards, granular access controls, interoperability mechanisms, and automated audit capabilities when applied to decentralized architectures. Particular concern was expressed regarding consent management, data minimization, and anonymization in blockchain systems, where immutability and transparency may conflict with traditional regulatory expectations. The study by Ahmed *et al*. (2025) concludes that legacy

Publisher: SARC Publisher

regulatory models (i.e. ISO, GDPR, and HIPAA) provide important foundational principles but are insufficient for emerging decentralized infrastructures. As health data become increasingly itinerant and distributed, regulatory governance must evolve beyond static compliance checklists and toward adaptive, technology-aware frameworks. This finding reinforces the lifecycle and interoperability gaps identified by Marcucci *et al*. (2023a; 2023b).

Faridoon & Kechadi (2024) conceptualizes regulatory alignment as a core pillar of healthcare data governance. Their framework emphasizes that compliance with GDPR, HIPAA, and related standards should not be treated as an external requirement but embedded within organizational structures and system design. The authors argue that effective governance requires clearly defined roles, including data governance committees, data owners, stewards, and custodians. Regulatory compliance must extend across the entire data lifecycle and be supported by continuous staff training and automated compliance monitoring. Importantly, the study highlights the "human factor," noting that insider threats and low technical awareness among healthcare personnel can undermine otherwise robust regulatory frameworks. This organizational perspective complements the macro-level benchmarking literature by showing that normative principles must be translated into internal governance architectures. Regulatory alignment is therefore not merely legal adherence but structural integration within institutional workflows.

Okyere Boadu *et al*. (2025) examine information governance practices in healthcare facilities in Ghana, providing empirical insight into how global standards are adopted in real-world settings. The study finds that while institutional policies referencing HIPAA, GDPR, and other standards are often present, staff knowledge and training remain moderate or low. Approximately two-thirds of professionals reported familiarity with major regulatory standards, and most facilities employed authentication mechanisms, secure platforms, and periodic compliance audits. However, training on data stewardship was limited, creating a knowledge-practice gap. Data quality challenges persisted despite policy frameworks, reflecting resource constraints and limited institutional capacity. These findings demonstrate that normative adoption does not automatically translate into effective implementation. Regulatory governance is shaped by local context, infrastructure maturity, and workforce competencies. Thus, global standards must be supported by localized capacity-building strategies to achieve meaningful compliance.

Paparova *et al*. (2023) introduce a distinct perspective by examining the evolution of a national digital health service under GDPR. The study conceptualizes "data governance spaces," defined not by organizational boundaries but by data processing purposes. This model distinguishes between data handling (where actors process data under a single authority for a uniform purpose) and data handover (where multiple actors independently determine purposes of the data, resulting in authority multiplication). The introduction of GDPR significantly reshaped governance dynamics by clarifying roles between data controllers and processors and requiring explicit legal bases for processing. The absence of specific enabling legislation constrained governance flexibility, increasing reliance on citizen consent mechanisms. The study demonstrates that regulatory change can alter institutional authority structures, redistribute accountability, and redefine data-sharing relationships. This purpose-based governance model highlights the dynamic nature of normative frameworks. Regulation does not merely impose constraints; it actively reorganizes governance ecosystems by redefining responsibilities and legal authority.

Synthesis

Across the reviewed literature, protection of individual rights, public interest, trust, and accountability are consistently emphasized (Marcucci *et al*., 2023a; 2023b; Ahmed *et al*., 2025). Governance is strongest at the stages of collection and storage but weaker in reuse and cross-border data flows (Marcucci *et al*., 2023a; 2023b). Non-binding guidance, weak monitoring mechanisms, and insufficient training undermine effectiveness (Okyere Boadu *et al*., 2025). Legacy regulatory frameworks struggle to accommodate decentralized and blockchain-based systems (Ahmed *et al*., 2025). Regulatory frameworks such as GDPR reshape governance relationships by redefining controller and processor roles (Paparova *et al*., 2023).

Collectively, these findings indicate that normative and regulatory governance frameworks are essential but insufficient in isolation. While global convergence around human rights–based principles is evident, fragmentation persists in lifecycle coverage, enforcement capacity, and

Publisher: SARC Publisher

technological adaptability. For U.S. health information policy and system design, the results suggest the need for harmonized definitions, lifecycle-inclusive governance mechanisms, stronger institutional oversight structures, and adaptive regulatory models capable of integrating emerging digital architectures.

Conceptual Map 2: Organizational Governance

The second conceptual map focuses on organizational governance, examining how health data governance is structured, operationalized, and institutionalized within and across healthcare systems. Paparova *et al*. (2023) introduce the concept of "data governance spaces" as a purpose-driven model for organizing authority and responsibility in national digital health systems. Based on a ten-year case study of a national health service platform, the authors argue that traditional organization-centric governance frameworks are insufficient for managing the complex movement of personal health data across multiple actors. The core finding is that governance is defined by the purpose of data processing rather than by technical or organizational boundaries.

Two primary modes are identified. First is data handling, where multiple actors process data under a single authority for a uniform purpose. In this configuration, actors function as data processors subordinate to a primary data controller. Second is data handover, where data are transferred or copied, allowing receiving actors to determine their own purposes and means of processing. This results in the multiplication of authorities, as each entity becomes an independent data controller. These modes generate two governance dynamics; (i) vertical dynamics, characterized by subordination and centralized accountability; and (ii) horizontal dynamics, characterized by distributed authority and parallel accountability structures. The study further highlights the impact of GDPR in clarifying controller–processor relationships and reshaping institutional responsibilities. Governance is therefore described as dynamic and continuously renegotiated rather than static. This model emphasizes that organizational governance must explicitly define authority boundaries, accountability mechanisms, and legal bases for data processing in multi-actor environments (Paparova *et al*., 2023).

Oktaviana *et al*. (2025) examine health data governance within a national cardiovascular center in Indonesia, identifying priority governance domains at the hospital level. The findings reveal that despite increasing digitization through Hospital Information Systems (HIS), governance maturity remains uneven. Three core governance domains are identified. First is data quality management, which addresses incomplete, inaccurate, or inconsistent Electronic Health or Medical Records (EHRs or EMRs), which directly affect patient safety, insurance claims, and research. Second is metadata management, which is ensuring clear definitions, standardization, and semantic consistency across departments to enable interoperability and integration. Third is data security management, which has to do with protecting confidentiality and integrity as hospitals transition to more complex digital ecosystems. The study by Oktaviana *et al*. (2025) also identifies structural barriers, including low governance awareness among staff, limited IT infrastructure, shortages of skilled personnel, and the absence of dedicated governance units. In many cases, governance responsibilities are assigned to IT or medical record departments without additional institutional capacity. These findings suggest that organizational governance at the hospital level depends heavily on resource allocation, leadership commitment, and formalized governance structures. Without dedicated oversight units and trained personnel, policies alone are insufficient to ensure data integrity and security (Oktaviana *et al*., 2025).

Okyere Boadu *et al*. (2025) provide empirical evidence on the implementation of Information Governance (IG) structures across healthcare facilities in Ghana. The study evaluates data stewardship, regulatory compliance, and quality management practices among healthcare professionals. A key finding is the gap between policy existence and practical understanding. While approximately 78% of professionals confirmed the presence of formal governance policies, overall knowledge levels were moderate. Training on data stewardship was particularly limited, which constrained effective implementation (Okyere Boadu *et al*., 2025). The IG model identified in the study includes (i) formal organizational policies guiding data stewardship; (ii) periodic compliance audits; (iii) authentication systems and secure platforms; (iv) explicit consent mechanisms for data reuse, and (v) both automated and manual data quality checks (Okyere Boadu *et al*., 2025). However, governance effectiveness varied significantly across professional roles, with health information officers demonstrating greater familiarity than other clinicians. The study underscores that governance capacity is shaped by human factors, training, and organizational culture

Publisher: SARC Publisher

(Okyere Boadu *et al*., 2025). Overall, the IG model highlights the importance of institutionalized stewardship roles, continuous education, and structured audit mechanisms. It also demonstrates that governance performance is context-sensitive, influenced by resource availability and workforce competencies (Okyere Boadu *et al*., 2025).

Alvarez-Romero *et al*. (2023) analyzed governance structures of 41 health data hubs across Europe and globally, focusing on the secondary use of health data for research. The study identifies the centralized data hub model as the dominant organizational structure, with 70% of hubs operating under centralized management. According to Alvarez-Romero *et al*. (2023), the centralized data hub model is characterized by: (i) formalized access procedures, such as legal contracts and collaboration agreements to identify and vet data providers; (ii) Standardized data access agreements and data processing agreements to regulate data sharing; (iii) Data protection impact assessments to evaluate privacy risks before processing; (iv) high adoption of anonymization and pseudonymization techniques; and (v) structured quality controls, error-checking tools, and version control mechanisms.

The study by Alvarez-Romero *et al*. (2023) also highlights funding stability as a critical governance factor. Most hubs rely on national funding, while others depend on short-term grants, raising concerns about long-term sustainability. Unlike hospital-level governance models focused on internal data management, the data hub model emphasizes cross-institutional coordination, research enablement, and controlled secondary use. Governance in this model is formalized, contract-driven, and supported by standardized documentation. Transparency, including publicly accessible governance policies, is identified as a best practice for building trust.

Synthesis

All models emphasize clearly defined roles, whether through controller–processor distinctions (Paparova *et al*., 2023), governance committees (Oktaviana *et al*., 2025), stewardship roles (Okyere Boadu *et al*., 2025), or contractual agreements (Alvarez-Romero *et al*., 2023). Governance effectiveness depends on infrastructure, trained personnel, and sustainable funding. Resource constraints undermine policy implementation (Oktaviana *et al*., 2025; Okyere Boadu *et al*., 2025). Standardized agreements, documented procedures, audit mechanisms, and risk assessments are central to operational governance (Alvarez-Romero *et al*., 2023; Okyere Boadu *et al*., 2025). Governance structures evolve in response to regulatory changes and technological shifts (Paparova *et al*., 2023). Organizational models must therefore remain adaptable. Data quality management, metadata standardization, and security safeguards are consistently identified as core organizational responsibilities (Oktaviana *et al*., 2025; Alvarez-Romero *et al*., 2023).

The organizational governance literature demonstrates that effective health data governance is institutional rather than purely regulatory. It requires defined authority structures, dedicated governance units, standardized procedures, trained personnel, and sustainable funding. Purpose-based governance models clarify accountability across actors, hospital-level frameworks prioritize data quality and security, IG models emphasize stewardship and compliance in practice, and data hubs formalize research-oriented data sharing. Together, these models show that governance effectiveness depends on organizational design and operational capacity, offering important lessons for strengthening U.S. health information policy and system architecture.

Conceptual Map 3: Technical Governance Architectures

The third conceptual map focuses on technical governance architectures, examining how governance principles are embedded directly into digital infrastructures. Unlike normative or organizational governance models, which define rules and responsibilities, technical governance architectures operationalize these rules through system design, cryptographic mechanisms, distributed computation, and automated enforcement. Two primary models emerge from the literature: (1) blockchain-based governance and (2) federated learning governance. Together, these architectures aim to address long-standing weaknesses in centralized healthcare data systems, including security vulnerabilities, limited interoperability, weak auditability, and privacy risks.

Blockchain-based governance

Across multiple studies, blockchain is presented not merely as a storage technology but as a governance paradigm that restructures authority, accountability, and trust in healthcare data management (Singh *et al*., 2022; Zaabar *et al*., 2021; Yaqoob *et al*., 2022; Ahmed *et al*., 2025). The central critique motivating blockchain adoption is the vulnerability of centralized Electronic Health Record (EHR) systems. These

Publisher: SARC Publisher

systems are described as prone to single points of failure, cyberattacks, data breaches, and fragmented accountability structures (Yaqoob *et al*., 2022).

A consistent finding across studies is that decentralization enhances system resilience. By distributing data verification and transaction recording across multiple nodes, blockchain reduces dependence on a central authority and mitigates risks associated with server failure or targeted attacks (Yaqoob *et al*., 2022). Singh *et al*. (2022) similarly argue that decentralized architectures prevent catastrophic system breakdowns common in centralized cloud-based models. Zaabar *et al*. (2021) operationalize decentralization through a six-layer architecture in "HealthBlock," which separates IoT data collection, off-chain storage, and blockchain management. Rather than storing large medical files directly on-chain, the system stores cryptographic hashes on a permissioned blockchain while maintaining actual records in a decentralized off-chain database (OrbitDB with IPFS). This hybrid model addresses scalability limitations associated with earlier blockchain implementations that attempted full on-chain storage.

Blockchain's immutability is identified as a core governance feature. Cryptographic hashing ensures that once data are recorded, they cannot be altered without detection (Yaqoob *et al*., 2022; Zaabar *et al*., 2021). This property strengthens audit trails, enabling transparent and tamper-evident tracking of data creation, modification, and access. Zaabar *et al*. (2021) demonstrate that storing only hashes on-chain ensures that any unauthorized alteration of off-chain medical records becomes immediately detectable. This approach enhances data integrity while preserving system performance. Similarly, Yaqoob *et al*. (2022) emphasize that blockchain enables real-time auditability, reducing administrative burdens and increasing trust among patients, providers, and regulators.

Another defining feature of blockchain-based governance is the use of smart contracts. These self-executing codes automate compliance by enforcing predefined rules for data access and sharing (Yaqoob *et al*., 2022; Zaabar *et al*., 2021). In HealthBlock, dual Hyperledger Fabric channels manage distinct governance domains: one channel for medical device interactions and another for consultation and EHR access control (Zaabar *et al*., 2021). This layered approach allows granular permission granting while maintaining system efficiency. Ahmed *et al*. (2025) identify smart contracts as a critical mechanism for addressing regulatory gaps in legacy frameworks such as ISO, GDPR, and HIPAA. Their findings suggest that automated compliance mechanisms embedded within blockchain systems may compensate for weaknesses in traditional regulatory enforcement, particularly in decentralized environments.

Blockchain architectures are also presented as enablers of interoperability. Yaqoob *et al*. (2022) argue that standardized data codes and distributed ledgers facilitate seamless exchange across heterogeneous healthcare providers. This addresses fragmentation inherent in traditional EHR systems. Economically, blockchain adoption is projected to reduce costs associated with fraud, counterfeit pharmaceuticals, and data breaches (Yaqoob *et al*., 2022). Although these projections remain prospective, the studies collectively frame blockchain as a mechanism for aligning privacy, security, transparency, and operational efficiency.

Despite its promise, blockchain-based governance faces limitations. Ahmed *et al*. (2025) report dissatisfaction among professionals regarding the adequacy of existing regulatory frameworks when applied to blockchain systems. Issues such as consent management, anonymization, and data minimization become complex within immutable and transparent ledgers. These findings indicate that technological innovation alone cannot resolve governance challenges; regulatory adaptation and ethical safeguards remain necessary.

Federated learning governance

Federated learning (FL) governance, discussed primarily by Singh *et al*. (2022), represents a complementary architecture that emphasizes privacy-preserving distributed computation. Unlike blockchain, which focuses on decentralized transaction recording, FL addresses the risks associated with centralized data aggregation for machine learning.

In traditional machine learning models, patient data are transferred to centralized servers for training, increasing exposure to breaches and privacy violations. Federated learning reverses this model by training algorithms directly on local devices (e.g., smartphones or medical sensors) and transmitting only model updates rather than raw data (Singh *et al*., 2022). This approach significantly reduces the need for large-scale data transfers and minimizes data leakage risks. By keeping raw patient data at the source, FL operationalizes data minimization principles

Publisher: SARC Publisher

embedded in regulatory frameworks such as GDPR. The architecture thus embeds privacy protections directly into system design (Singh *et al*., 2022).

Singh *et al*. (2022) further integrate FL with blockchain to enhance integrity and trust. While FL prevents raw data transfer, it is vulnerable to malicious model updates. Blockchain addresses this vulnerability by recording model updates on a tamper-proof ledger and verifying participant identities. The inclusion of a "privacy broker" and "integrity manager" ensures secure coordination between devices without compromising system flow. This hybrid architecture demonstrates how technical governance models can be layered. Federated learning preserves privacy during computation, while blockchain ensures traceability and integrity of model updates. Together, they reduce reliance on centralized servers while maintaining auditability.

Federated learning also improves resource efficiency. Singh *et al*. (2022) report reduced bandwidth consumption and energy use because data are not continuously transmitted to centralized clouds. This feature is particularly relevant in IoT-based healthcare environments where devices generate continuous data streams. However, system performance may be sensitive to processing delays at network entities. Thus, while FL enhances privacy and scalability, its implementation requires reliable infrastructure and coordination mechanisms.

Synthesis

Both architectures aim to reduce dependence on centralized authorities. Blockchain distributes ledger control, while federated learning distributes computational processes (Singh *et al*., 2022; Yaqoob *et al*., 2022). Technical governance embeds privacy protections into system design through cryptography, hashing, permissioned access, and on-device training (Zaabar *et al*., 2021; Singh *et al*., 2022). Smart contracts and immutable ledgers automate enforcement and monitoring, reducing manual oversight requirements (Yaqoob *et al*., 2022; Ahmed *et al*., 2025). While blockchain promises interoperability, integration with legacy regulatory and institutional frameworks remains complex (Ahmed *et al*., 2025). Off-chain storage and hybrid blockchain-FL models address scalability constraints and computational overhead (Zaabar *et al*., 2021; Singh *et al*., 2022).

Technical governance architecture represents a shift from rule-based compliance toward architecture-based enforcement. Blockchain-based models enhance decentralization, immutability, transparency, and automated access control, while federated learning prioritizes privacy-preserving computation and data minimization. Hybrid integrations further strengthen integrity and scalability. However, these architectures must be aligned with evolving regulatory frameworks and institutional capacities to achieve sustainable governance. For U.S. health information policy and system design, the findings suggest that embedding governance principles directly into digital infrastructures may strengthen privacy, interoperability, and resilience in increasingly distributed health data ecosystems.

Conceptual Map 4: Operational and Design Governance

The fourth conceptual map focuses on operational and design governance, examining how governance principles are translated into daily practices, workflows, and system architectures. While normative frameworks define legal obligations and organizational models define authority structures, operational governance determines how data are protected, validated, accessed, and reused in practice.

Privacy and security by design

Faridoon and Kechadi (2024) propose a conceptual framework that places Privacy and Security by Design (PSbD) at the core of healthcare data governance. Their analysis argues that privacy and security are often treated as secondary add-ons in digital health systems, leading to fragmented protections and reactive compliance. In contrast, PSbD integrates safeguards from the earliest stages of system architecture. The framework is built on three interconnected pillars: (1) governance organization, (2) data communication and quality, and (3) privacy and security by design (Faridoon & Kechadi, 2024). Within this model, regulatory alignment with GDPR, HIPAA, and related standards is embedded into technical and organizational processes. Clearly defined roles such as data owners, stewards, custodians, and governance committees are necessary to ensure accountability across the data lifecycle.

A key operational component is the use of Privacy-Enhancing Technologies (PETs), which allow data analysis without exposing personally identifiable information. Faridoon and Kechadi (2024) emphasize privacy-preserving analytics, secure encryption practices, and structured access

Publisher: SARC Publisher

controls as core design features. Automated compliance systems are also highlighted as a mechanism for continuously monitoring logs and detecting policy deviations, reducing reliance on manual oversight. Importantly, Faridoon and Kechadi (2024) identify the "human factor" as a critical vulnerability in healthcare systems. Insider threats, low cyber security awareness, and inadequate staff training undermine even well-designed infrastructures. Thus, PSbD requires not only technical controls but also continuous workforce education and accountability structures. Overall, this section suggests that operational governance must move from reactive risk mitigation toward proactive system design, where privacy and security protections are embedded in software development, infrastructure planning, and organizational workflows.

Data quality governance

Data quality governance emerged as a central operational theme across hospital-level and research-oriented frameworks (Oktaviana *et al*., 2025; Okyere Boadu *et al*., 2025; Alvarez-Romero *et al*., 2023). Poor data quality compromises patient safety, insurance claims, clinical decision-making, and research reliability. Consequently, operational governance must include structured quality management mechanisms. Oktaviana *et al*. (2025) identify significant data quality challenges within hospital information systems, including incomplete records, inaccurate entries, redundancy, and inconsistent documentation. These deficiencies limit interoperability and hinder effective data reuse. The study emphasizes three priority domains: data quality management, metadata management, and data security management. Metadata management is particularly important for ensuring semantic clarity and standardized definitions across hospital departments. Without clear metadata frameworks, integration across systems becomes difficult. Oktaviana *et al*. (2025) argue that structured documentation and standardized terminologies are necessary to support both clinical operations and secondary research use.

Okyere Boadu *et al*. (2025) report that healthcare facilities employ both automated and manual data quality checks. Electronic Health Record systems often include built-in validation rules, while monthly audits and peer reviews provide additional oversight. Despite these measures, quality issues persist due to limited staff training, resource constraints, and inconsistent data entry practices. The study by Okyere Boadu *et al*. (2025) highlights the importance of regular training and supervision in strengthening data stewardship competencies. Governance effectiveness depends not only on technical tools but also on staff capacity to interpret and apply quality standards.

Research-oriented data quality mechanisms

At the research infrastructure level, Alvarez-Romero *et al*. (2023) identify robust quality assurance mechanisms within health data hubs. The majority of hubs apply formal quality controls, utilize specialized error-checking software, and maintain version control systems to track dataset changes. Anonymization and pseudonymization processes are also commonly applied internally to preserve confidentiality. These findings indicate that operational governance in research environments often includes more formalized and standardized quality procedures compared to hospital-level settings. Dedicated governance structures and stable funding appear to support higher maturity in quality management. Across contexts, data quality governance involves six core dimensions: accuracy, completeness, consistency, timeliness, uniqueness, and validity. Effective governance integrates automated validation, manual review, metadata standardization, and staff training.

Consent and access governance

Consent and access control mechanisms represent another key operational domain. Governance frameworks must define who can access data, under what conditions, and with what oversight.

Zaabar *et al*. (2021) demonstrate how blockchain-based systems can automate access governance through smart contracts. In the Health Block architecture, patient-driven permission allows individuals to control who accesses their medical records. Two separate blockchain channels, one for medical devices and another for consultation and EHR sharing, enable granular control over data subsets. Access requests are validated through automated chain codes, reducing reliance on centralized intermediaries. This design ensures traceability and immutability of access transactions, strengthening transparency and accountability. However, it also requires strong identity management systems and secure key management infrastructures.

Okyere Boadu *et al*. (2025) reports that a majority of healthcare professionals confirm explicit patient consent is obtained for data reuse. Facilities also conduct periodic compliance audits and implement authentication systems to protect confidentiality

Publisher: SARC Publisher

during data processing and transmission. Despite policy presence, knowledge gaps among staff may limit consistent enforcement. These findings suggest that while consent procedures are formally embedded in policy, their operational effectiveness depends on staff understanding and institutional culture.

Alvarez-Romero *et al*. (2023) highlight structured contractual governance in health data hubs. Data Access Agreements (DAA) and Data Processing Agreements (DPA) formalize the terms of data sharing between providers and researchers. Additionally, Data Protection Impact Assessments (DPIA) are used to evaluate privacy risks before processing begins. These formal agreements provide legal clarity, define responsibilities, and standardize access procedures. Templates that allow contextual modifications are common, balancing flexibility with compliance. This contract-driven approach reflects a mature operational governance model designed to facilitate secure secondary data use.

Synthesis

Privacy and security must be integrated during system development rather than appended after deployment (Faridoon & Kechadi, 2024). Automated validation, encryption, and smart contracts must be complemented by training, audits, and accountability mechanisms (Okyere Boadu *et al*., 2025). Contractual agreements and impact assessments enhance clarity and transparency in data sharing (Alvarez-Romero *et al*., 2023). Reliable, standardized data are essential for compliance, interoperability, and research validity (Oktaviana *et al*., 2025). Emerging architectures emphasize patient control over data access, strengthening trust and transparency (Zaabar *et al*., 2021).

Operational and design governance models demonstrate that effective health data governance is achieved through proactive system design, structured quality management, and clearly defined access mechanisms. Privacy and security by design embed regulatory principles into technical infrastructures; data quality governance ensures reliability and interoperability; and consent and access frameworks regulate responsible data sharing. Together, these operational mechanisms translate high-level governance principles into enforceable, day-to-day practices. For U.S. health information policy and system design, the findings underscore the importance of integrating privacy safeguards, quality controls, and standardized access agreements directly into digital health architectures to strengthen accountability, trust, and system resilience.

General Implications

The reviewed literature shows that effective health data governance emerges from the integration of four complementary governance layers: normative and regulatory governance, organizational governance, technical governance architectures, and operational and design governance. Together, these frameworks form a comprehensive system that addresses legal authority, institutional responsibility, technological enforcement, and day-to-day operational practices.

Connections among the conceptual maps

The four conceptual maps are closely interconnected and function as sequential layers of governance. Normative and regulatory governance establishes the legal and ethical foundation for health data management. Organizational governance builds upon this foundation by defining institutional roles, authority structures, and accountability mechanisms needed to implement regulatory requirements. Technical governance architectures further operationalize these structures by embedding governance rules into digital systems through cryptographic security, distributed ledgers, and privacy-preserving computation. These technologies translate governance principles into automated system functions such as secure access control and auditability. Operational and design governance connect all previous layers by guiding how governance is implemented in practice. It focuses on privacy and security by design, data quality assurance, consent management, and standardized access procedures within daily workflows.

Together, the conceptual maps illustrate a layered governance model where legal principles guide institutions, institutions shape technological systems, and operational practices ensure consistent and accountable implementation.

Implications for the United States health data and health system

The findings from the reviewed literature provide several important implications for strengthening health data governance within the United States health information system. These implications relate to regulatory design, institutional capacity, technological infrastructure, and operational practices.

First, the literature highlights the need for more comprehensive lifecycle governance within U.S. health data policy. Existing frameworks tend to

Publisher: SARC Publisher

emphasize privacy protection during data collection and storage, but governance for secondary data use, data sharing, and cross-institutional exchange remains less developed. The benchmarking analysis of global frameworks shows that governance is strongest at early stages of the data lifecycle but weaker during reuse and cross-border flows. For the United States, this suggests the importance of developing clearer governance mechanisms that regulate how health data are reused for research, public health surveillance, and innovation while maintaining privacy protections.

More so, the findings emphasize the importance of harmonized definitions and regulatory clarity. The literature identifies fragmentation in terminology and inconsistent operational interpretations across governance frameworks. Such fragmentation can create confusion among healthcare organizations and hinder interoperability between systems. For the U.S. health information infrastructure, clearer regulatory guidance and harmonized terminology could improve coordination across hospitals, research institutions, insurers, and public health agencies. This would support more consistent governance practices and reduce uncertainty in data sharing arrangements.

The conceptual maps highlight the critical role of institutional governance structures. Evidence from hospital-level and national governance models shows that policies alone are insufficient without clearly defined authority structures and dedicated governance units. Governance committees, data stewards, custodians, and formal oversight mechanisms ensure accountability and coordinated decision-making. For the U.S. health system, strengthening institutional governance structures could improve oversight of health information management and ensure consistent implementation of regulatory requirements across healthcare organizations.

Additionally, the review underscores the importance of workforce capacity and training. Studies show that gaps often exist between governance policies and staff understanding of those policies. Limited training in data stewardship and cybersecurity reduces the effectiveness of otherwise strong governance frameworks. For the United States, this finding suggests that strengthening workforce education in health information governance is essential for improving compliance, protecting patient data, and maintaining trust in digital health systems.

Furthermore, the conceptual maps suggest that technical system design will play an increasingly important role in governance. Blockchain and federated learning architectures demonstrate how privacy protection, auditability, and security can be embedded directly into digital infrastructures. These technologies reduce reliance on manual oversight and strengthen system resilience by distributing authority and computational processes. For the U.S. health information ecosystem, integrating governance principles into system architecture could improve transparency, security, and interoperability across healthcare networks.

Finally, this literature review emphasizes the importance of operational governance mechanisms such as privacy and security by design, data quality management, and standardized access agreements. Reliable and standardized health data are essential for clinical care, research, and public health decision-making. Operational governance practices such as automated validation checks, metadata standardization, and formal data access agreements help ensure data reliability and responsible sharing. For the United States, incorporating these practices into health information system design would strengthen data integrity, improve interoperability, and support evidence-based healthcare innovation.

Overall, the conceptual maps demonstrate that effective health data governance requires an integrated approach that combines regulatory frameworks, institutional structures, technological architectures, and operational practices. By strengthening governance across these interconnected dimensions, the United States can build a more secure, interoperable, and trustworthy health information system capable of supporting modern healthcare delivery and research.

CONCLUSION

This review demonstrates that effective health data governance requires the integration of regulatory frameworks, institutional structures, technological systems, and operational practices. Normative governance establishes legal and ethical principles, while organizational governance defines roles and accountability structures within healthcare institutions. Technical governance architectures embed privacy, security, and transparency directly into digital infrastructures, and operational governance ensures these principles are implemented in daily workflows through data quality management, consent mechanisms, and privacy by design. Together, these governance layers create a comprehensive framework for

Publisher: SARC Publisher

managing health data in complex digital environments. Strengthening coordination across these dimensions can improve accountability, interoperability, and trust in health information systems.

REFERENCES

1. Aaltonen, A., Alaimo, C., & Kallinikos, J. "The making of data commodities: Data analytics as an embedded process." *Journal of management information systems* 38.2 (2021): 401-429.
2. Ahmed, A., Shahzad, A., Naseem, A., Ali, S., & Ahmad, I. "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 (2025): e0324285.
3. Alaimo, C., Kallinikos, J., & Aaltonen, A. "Data and value." *Handbook of digital innovation*. Edward Elgar Publishing, (2020). 162-178.
4. Al-Badi, A., Tarhini, A., & Khan, A. I. "Exploring big data governance frameworks." *Procedia computer science* 141 (2018): 271-277.
5. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. "A systematic literature review of data governance and cloud data governance." *Personal and ubiquitous computing* 23.5 (2019): 839-859.
6. Alvarez-Romero, C., Martínez-García, A., Bernabeu-Wittel, M., & Parra-Calderón, C. L. "Health data hubs: an analysis of existing data governance features for research." *Health research policy and systems* 21.1 (2023): 70.
7. Regulation, P. "Regulation (EU) 2016/679 of the European Parliament and of the Council." *Regulation (eu)* 679.2016 (2016): 10-3.
8. Faridoon, A., & Kechadi, M. T. "Healthcare data governance, privacy, and security-a conceptual framework." *EAI International Conference on Body Area Networks*. Cham: Springer Nature Switzerland, (2024).
9. Förstel, S., Förstel, M., Gallistl, M., Zanca, D., Eskofier, B. M., & Rothgang, E. M. "Data quality in hospital information systems: Lessons learned from analyzing 30 years of patient data in a regional German hospital." *International Journal of Medical Informatics* 192 (2024): 105636.
10. Frikha, T., Chaari, A., Chaabane, F., Cheikhrouhou, O., & Zaguia, A. "[Retracted] Healthcare and Fitness Data Management Using the IoT-Based Blockchain Platform." *Journal of Healthcare Engineering* 2021.1 (2021): 9978863.
11. Keshta, I., & Odeh, A. "Security and privacy of electronic health records: Concerns and challenges." *Egyptian Informatics Journal* 22.2 (2021): 177-183.
12. Kitchenham, B., Pretorius, R., Budgen, D., Brereton, O. P., Turner, M., Niazi, M., & Linkman, S. "Systematic literature reviews in software engineering–a tertiary study." *Information and software technology* 52.8 (2010): 792-805.
13. Li, J., Yu, G., Ding, W., Huang, J., Li, Z., Zhu, Z., & Yin, J. "Data governance system of the National Clinical Research Center for child health in China." *Translational Pediatrics* 10.7 (2021): 1905.
14. Li, Q., Lan, L., Zeng, N., You, L., Yin, J., Zhou, X., & Meng, Q. "A framework for big data governance to advance RHINs: a case study of China." *Ieee Access* 7 (2019): 50330-50338.
15. Marcucci, S., Alarcon, N. G., Verhulst, S. G., & Wullhorst, E. "Mapping and Comparing Data Governance Frameworks: A benchmarking exercise to inform global data governance deliberations." *arXiv preprint arXiv:2302.13731* (2023).
16. Marcucci, S., Alarcón, N. G., Verhulst, S. G., & Wüllhorst, E. "Informing the global data future: benchmarking data governance frameworks." *Data & Policy* 5 (2023): e30.
17. Ministry of Health of the Republic of Indonesia. "Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Record." (2022).
18. O'hara, K. "Data trusts: Ethics, architecture and governance for trustworthy data stewardship." (2019).
19. Oderkirk, J., & Ronchi, E. "Governing data for better health and healthcare." *Organisation for Economic Cooperation and Development. The OECD Observer* (2018): 1-4.
20. Oktaviana, S., Handayani, P. W., Hidayanto, A. N., & Siswanto, B. B. "Healthcare data governance assessment based on hospital management perspectives." *International Journal of Information Management Data Insights* 5.1 (2025): 100342.
21. Okyere Boadu, R., Wireko Adu, V., Okyere Boadu, K. A., Ibrahim, B., Akey, P., Amishadas Mensah, A., ... & Kumasenu Mensah, N. "Examine frameworks policies

Publisher: SARC Publisher

and strategies for effective information governance in healthcare organizations." *Plos one* 20.7 (2025): e0327496.
22. Osifowokan, A. S., Ahmed, Z., Adukpo, T. K., & Mensah, N. "Enhancing data compliance in the United States healthcare system: Addressing challenges in HIPAA and HITECH Act implementation." *EPRA International Journal. Https://doi. org/10.36713/epra21263* (2025).
23. Oware, D. A., & Mensah, S. "Developing Advanced Predictive Models for Patient Flow Forecasting in Healthcare Facilities: A Systematic Review and Analysis." *International Journal of Frontline Research in Life Science*. (2025).
24. Pan American Health Organization. "Data governance in public health." (2022).
25. Paparova, D., Aanestad, M., Vassilakopoulou, P., & Bahus, M. K. "Data governance spaces: the case of a national digital service for personal health data." *Information and Organization* 33.1 (2023): 100451.
26. Parmiggiani, E., & Grisot, M. "Data curation as governance practice." *Scandinavian Journal of Information Systems* 32.1 (2020): 1.
27. Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology." *Future Generation Computer Systems* 129 (2022): 380-388.
28. Skovgaard, L. L., Wadmann, S., & Hoeyer, K. "A review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good." *Health policy* 123.6 (2019): 564-571.
29. se, D., Chow, C. K., Ly, T. P., Tong, C. Y., & Tam, K. W. "The challenges of big data governance in healthcare." *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, (2018).
30. Utomi, E., Osifowokan, A. S., Donkor, A. A., & Yowetu, I. A. "Evaluating the impact of data protection compliance on AI development and deployment in the US health sector." *World Journal of Advanced Research and Reviews* 24.2 (2024): 1100-1110.
31. Van den Broek, T., & van Veenstra, A. F. "Modes of governance in inter-organizational data collaborations." (2015).
32. Hedman, J., Bødker, M., Gimpel, G., & Damsgaard, J. "Translating evolving technology use into user stories: Technology life narratives of consumer technology use." *Information Systems Journal* 29.6 (2019): 1178-1200.
33. Wang, M., Li, S., Zheng, T., Li, N., Shi, Q., Zhuo, X., & Huang, Y. "Big data health care platform with multisource heterogeneous data integration and massive high-dimensional data governance for large hospitals: design, development, and application." *JMIR Medical Informatics* 10.4 (2022): e36481.
34. Winter, J. S., & Davidson, E. "Big data governance of personal health information and challenges to contextual integrity." *The Information Society* 35.1 (2019): 36-51.
35. Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. "Blockchain for healthcare data management: opportunities, challenges, and future recommendations." *Neural Computing and Applications* 34.14 (2022): 11475-11490.
36. Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. "HealthBlock: A secure blockchain-based healthcare data management system." *Computer Networks* 200 (2021): 108500.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Silas, O. J. & Adjaottor, S. D. "Learning from Global Models: A Comparative Analysis of Health Data Governance Frameworks and Their Implications for U.S. Health Information Policy and System Design" *Sarcouncil Journal of Multidisciplinary* 5.6 (2026): pp 8-20.

Publisher: SARC Publisher