Saudi Journal of Medicine and Public Health

https://saudijmph.com/index.php/pub

https://doi.org/10.64483/202412450

Strategic Data Stewardship in Modern Healthcare: An Integrated Governance Framework for Ensuring Quality, Privacy, and Ethical Disclosure Across Clinical, Operational, and Analytical Domains

Sattam Deghaim M Albanaqi [(1)] , Mohammed Ali Albathali [(2)] , Nourah Saad Turki Alotaibi [(3)] , Bader Ghazai Ghazi Alotaibi [(3)] , Wael Ali Mohammed Otayn [(4)] , Faisal Awad Mohammed Alsharari [(5)] , Saad Shtewi Qasiem Alsharari [(6)] , Abdulrahman Awad Shtewi AlSharari [(7)] , Faisal Tabia Qasem Alsharari [(8)] , Jumaah Husain A Alenazi [(9)] , Mohammed Hathal Thunayyan Alotaibi [(10)] , Modhi Falaj Herbash Alotaibi [(10)]

(1) Branch of the Ministry of Health in Hafar Al-Batin, Saudi Arabia,
(2) Long-Term Care Hospital, Ministry of Health, Saudi Arabia,
(3) Ministry Of Health, Saudi Arabia,
(4) Jazan City / General Season Hospital,Ministry of Health, Saudi Arabia,
(5) Al-Qurayyat General Hospital,Ministry of Health, Saudi Arabia,
(6) Medical Warehouses, Al-Jawf Health Cluster, Al-Qurayyat,Ministry of Health, Saudi Arabia,
(7) Al-Qurayyat General Hospital, Al-Qurayyat, Al-Jawf Health Cluster,Ministry of Health, Saudi Arabia,
(8) Al-Qurayyat Ambulance Transport Center, Al-Qurayyat, Al-Jawf Health Cluster,Ministry of Health, Saudi Arabia,
(9) Al-Amal Hospital for Mental Health, Al-Qurayyat, Al-Jawf Health Cluster,Ministry of Health, Saudi Arabia,
(10) Health security at Al-Fawaz Health Center,Ministry of Health, Saudi Arabia

Abstract

Background: The digital transformation of healthcare generates vast sensitive data, creating critical imperatives for robust data governance to ensure quality, privacy, and secure access across clinical and operational domains.
Aim: This study aims to develop an integrated conceptual framework to address pervasive governance gaps in healthcare organizations, including informal data-sharing and unclear accountability, which undermine data reliability and compliance.
Methods: Using a conceptual methodology, the study synthesizes governance theory with healthcare operational realities through a critical analysis of literature and best practices in informatics and data management.
Results: The proposed framework is built on four pillars: (1) strategic leadership and accountability structures; (2) risk-based data classification; (3) formalized request and disclosure workflows; and (4) embedded data quality and metadata management. It provides a structured model to transform data into a governed, high-integrity asset.
Conclusions: Effective data governance is foundational for trustworthy, data-driven healthcare. This framework offers an actionable blueprint for organizations to transition from ad-hoc practices to proactive stewardship, thereby enhancing decision-making, ensuring compliance, and supporting safe patient care.

Keywords: data governance, healthcare, data quality, privacy, health safety, data disclosure, clinical informatics, stewardship

Introduction

The contemporary healthcare ecosystem is fundamentally data-driven. From electronic health records (EHRs) and pharmacy informatics systems to laboratory information management systems (LIMS) and population health databases, organizations generate and consume vast quantities of sensitive information (Scott et al., 2017). For professionals across pharmacy, nursing, medical laboratories, health informatics, and administration, this data is the lifeblood of clinical decision-support, medication safety, diagnostic accuracy, operational efficiency, and strategic planning (Groves et al., 2013). However, this reliance introduces profound governance challenges. Data quality errors can lead to medication misadventures or diagnostic inaccuracies (van der Nat et al., 2022). Inappropriate data disclosure violates patient privacy regulations like HIPAA and GDPR (Mishra & Mishra, 2022). Inconsistent data definitions cripple comparative analytics and performance benchmarking (Liaw et al., 2021).

Despite its critical importance, data governance in healthcare is often relegated to the IT department or implemented through disjointed policies, creating a dangerous misalignment between technical data management and frontline clinical and

*Corresponding author e-mail: Khdt1400@hotmail.com (Sattam Deghaim M Albanaqi).
Receive Date: 17 December 2024, Revise Date: 30 December 2024, Accept Date: 31 December 2024

operational realities (Tiffin et al., 2019). Decisions regarding data access and sharing are frequently made through informal channels, lacking standardized documentation, clear accountability, or consistent validation against quality benchmarks (Kariotis et al., 2020). This study posits that effective data governance is not a technical subroutine but a core institutional competency. It requires an integrated, multidisciplinary framework that aligns strategic oversight with the practical needs of data producers and consumers across all healthcare domains. This paper conceptualizes such a framework, focusing on the triumvirate of data quality, privacy, and controlled disclosure as foundational pillars for trustworthy healthcare data ecosystems.

Research Problem and Objectives

The central problem addressed is the *governance gap*: the disconnect between the recognized value of healthcare data and the immature, often informal structures in place to manage it as a strategic asset (Abraham et al., 2019). This gap manifests in several high-risk practices: the proliferation of "shadow" data exchanges outside approved channels; the fulfillment of urgent data requests that bypass quality checks; and the reporting of conflicting metrics from different departments due to unclear data ownership and definitions (Enticott et al., 2020). For a pharmacy technician verifying an order, a nurse documenting care, or a lab technician reporting a critical value, this governance vacuum translates into uncertainty about data provenance and reliability (Oktaviana et al., 2022).

The consequences are severe. They include regulatory non-compliance and financial penalties, patient safety incidents rooted in poor data quality, eroded trust among care teams, and strategic decisions based on flawed intelligence (Abouelmehdi et al., 2017). This study argues that these are not isolated technical failures but symptoms of a systemic governance deficit.

The objectives of this study are therefore to:

1. Conceptualize a holistic, multidisciplinary model of data governance applicable across the healthcare continuum.
2. Critically analyze governance failures related to data disclosure, quality assurance, and accountability pathways.
3. Examine the impact of fragmented data ownership and the absence of a "single source of truth" on clinical and operational consistency.
4. Propose an integrated conceptual framework that closes these governance gaps by institutionalizing stewardship, standardizing processes, and embedding quality and privacy-by-design principles.

Data Governance in Healthcare

Data governance is defined as the exercise of authority, control, and shared decision-making over the management of data assets (International, 2017). In healthcare, it is the orchestration of people, processes, and technology to ensure data is accurate, accessible, consistent, and secure throughout its lifecycle (Mosley et al., 2010). This is not solely an informatics concern. For pharmacists, governance ensures the integrity of medication lists and allergy data, directly impacting patient safety (van der Nat et al., 2022). For nurses, it governs the documentation standards that support care continuity and outcome measurement (Topaz et al., 2017). Medical laboratory scientists rely on governance for standardized test nomenclature and the secure transmission of results (Vassilakopoulou et al., 2016). Health informaticians design systems that enact governance policies, while health safety and security professionals focus on the privacy and breach management aspects (Spector-Bagdady et al., 2023).

Effective governance establishes clear roles: Data Trustees (executive leadership providing strategic oversight), Data Stewards (subject matter experts, e.g., a lead pharmacist or lab director, defining data standards), and Data Custodians (IT professionals managing the technical environment) (Khatri & Brown, 2010). This structure formalizes accountability, ensuring that someone is responsible for the definition, quality, and appropriate use of every critical data element (Otto, 2011). Figure 1 illustrates the proposed integrated data governance framework for healthcare, structured around four interdependent pillars: strategic leadership and accountability, risk-based data classification, formalized data request and disclosure workflows, and embedded data quality and metadata management.

Figure 1. Integrated Data Governance Framework for Healthcare Organizations

The Critical Governance Challenge of Controlled Data Disclosure

A pervasive weakness in many organizations is the informal governance of data disclosure. Requests for patient cohorts, performance metrics, or research data often occur via email, instant message, or verbal conversation, lacking formal approval trails

(Williamson et al., 2022). This informality creates significant risk. A health assistant may inadvertently disclose information beyond the "minimum necessary" in response to an urgent verbal request (Rose et al., 2023). A nurse manager might share unit-level data with a research colleague without review by the privacy officer (Ngesimani et al., 2022).

This practice divorces data disclosure from accountability and legal review. It fosters a culture where data is perceived as a free commodity rather than a regulated asset (Hubbard et al., 2020). The absence of a standardized request mechanism means the purpose of use is rarely scrutinized, data quality is assumed rather than verified, and re-disclosure controls are not communicated. A robust governance framework must replace this ad-hoc model with a formal, transparent, and auditable process for all internal and external data disclosures.

The Tyranny of Urgency

Healthcare operates under constant time pressure. Emergent clinical decisions, executive reporting deadlines, and public health emergencies demand rapid data access (World Health Organization, 2021). However, urgency often conflicts with rigorous data quality assurance. When a medical laboratory is pressured for real-time infection statistics, validation and deduplication steps may be shortcut, leading to inaccurate prevalence rates (Li et al., 2021). When pharmacy leadership needs immediate medication utilization reports, data from disparate dispensing systems may be merged without resolving semantic differences (e.g., "dose" vs. "unit") (Bond, 2020).

Governance must differentiate between *data availability* (the data exists in a system) and data readiness (the data has been validated, harmonized, and certified for a specific use) (Loshin, 2010). A key governance function is to institute "speed bumps" or validation checkpoints that are appropriate to the risk level of the decision being supported. Even urgent requests must pass through a minimal, expedited governance pathway that documents the request, certifies the quality level of the data provided, and obtains necessary approvals (Dixon-Woods et al., 2020).

Fragmented Requests and the Elusive "Single Source of Truth"

The absence of governed disclosure often leads to redundant, contradictory data flows. Different departments—finance, quality improvement, clinical operations—may independently request what is essentially the same dataset (e.g., "all outpatient visits for Q3") but receive different figures (Liaw et al., 2021). This is not typically a technical error but a governance failure stemming from unclear data ownership and a lack of a designated "single source of truth" (SSOT).

An SSOT is the officially sanctioned, authoritative data asset for a given key metric, maintained by an appointed Data Steward (Kuzio et al., 2022). For example, the master "patient demographic" file should be stewarded by Health Informatics, and the "approved medication formulary" by Pharmacy & Therapeutics. When anyone needs this data, the governance framework directs them to this source. This prevents departments from creating their own siloed, potentially divergent copies. For health safety officers tracking incident reports, an SSOT ensures they are analyzing the same definitive dataset as the risk management team, leading to consistent insights and actions (Strome & Liefer, 2013). Table 1 shows the common data governance challenges across healthcare professions.

Table 1: Common Data Governance Challenges Across Healthcare Professions

Healthcare Domain	Exemplary Data Asset	Primary Governance Challenges	Potential Risks
Pharmacy	Medication Administration Records, Drug Formulary	Inconsistent drug nomenclature; Uncontrolled access to controlled substance data; Integration errors from robotic dispensing systems.	Medication errors, Regulatory (DEA) non-compliance, and Billing inaccuracies.
Nursing	Clinical Documentation, Vital Signs Flowcharts	Unstructured narrative notes limiting analytics; Variation in assessment documentation; Pressure to bypass documentation for urgency.	Compromised care continuity; Inaccurate outcome measurement; Legal liability.
Medical Laboratories	Test Results, Genomic Sequences	Standardizing complex test codes (LOINC); Ensuring data integrity from analyzer to EHR; Securing highly sensitive genetic data.	Diagnostic errors, Privacy breaches, and Ineffective public health surveillance.
Health Informatics	EHR Database, Analytics Warehouses	Legacy system integration; Balancing data accessibility with security; Managing evolving data standards (FHIR, HL7).	System interoperability failures; Data silos; Inability to support advanced analytics.
Health, Safety & Security	Incident Reports, Access Logs	Under-reporting of safety events; Inconsistent classification of incidents;	Inability to identify systemic risks; Non-compliance with

	Integrating sources.	disparate	safety data	safety standards; Uninvestigated breaches.

Governance of Information Systems and Operational Veracity

A critical yet often overlooked governance layer involves the alignment between information system outputs and operational reality. A hospital's EHR may generate a "bed occupancy rate" of 95% based on its admission/discharge logic, while frontline nurses experience a perceived occupancy of 110% due to boarders in the emergency department (Wiler et al., 2015). The system indicator is *technically* accurate per its programming, but is contextually misleading. This misalignment occurs when governance for system development (focused on technical approval) is disconnected from governance for indicator use (focused on operational validity) (Liaw et al., 2021).

Effective governance must close this feedback loop. Clinical and operational staff (nurses, health assistants) must have formalized channels to report discrepancies between system-reported data and observed reality (Oktaviana et al., 2022). Data stewards and informatics teams are then accountable for investigating and reconciling these gaps, whether through system refinement, indicator redefinition, or improved user training. This ensures that data used for leadership dashboards and performance incentives truly reflects the state of care delivery.

Proposed Conceptual Framework for Integrated Data Governance

To systematically address the multifaceted governance challenges prevalent in modern healthcare—spanning informal disclosure, data inconsistency, and misaligned system indicators—this study proposes a robust, integrated conceptual framework. This framework is architected upon four interdependent, foundational pillars designed to transform data from an unmanaged operational byproduct into a strategically governed, high-integrity organizational asset. The pillars collectively establish the necessary leadership structures, risk-based policies, controlled operational processes, and embedded quality mechanisms required for sustainable data stewardship across all professional domains (Ahmadi et al., 2022; Mosley et al., 2010).

The first pillar, strategic leadership & accountability structure, establishes the essential executive oversight and domain-level ownership required for governance to be effective. Governance must be championed at the highest organizational level to ensure it receives adequate resources and authority. This is operationalized through a data governance council (DGC), ideally co-chaired by clinical (e.g., Chief Medical Officer), operational (e.g., Chief Operating Officer), and informational (e.g., Chief Information Officer) leadership, which sets the strategic direction, approves overarching policies, and resolves cross-domain disputes (Khatri & Brown, 2010). Beneath this council, the framework mandates the establishment of domain-specific data stewardship committees—such as a Pharmacy Data Committee or a Laboratory Data Committee. Staffed by frontline subject matter experts (e.g., lead pharmacists, laboratory directors, senior nurses), these committees are vested with the authority and responsibility to define data standards, quality rules, and authorized uses for their specific clinical or operational domains, thereby embedding accountability directly within the business units that both create and rely on the data (Otto, 2011).

Concurrent with this leadership structure, the second pillar, risk-based data classification & standardized lifecycle policies, provides the granular policy framework that dictates how different types of data are handled. All organizational data assets must be systematically classified according to sensitivity (e.g., public, internal, confidential, restricted) and primary purpose (e.g., clinical care, operational analytics, research) (International Organization for Standardization, 2013). This classification, performed by the Domain Stewards, directly dictates the stringency of governance controls applied. For instance, a "restricted" classification for genetic test results would trigger requirements for stringent access logging, encryption, and multi-level disclosure reviews, whereas an "internal" classification for equipment maintenance logs may permit broader internal access with fewer restrictions (Cohen & Mello, 2018). This classification then informs comprehensive, standardized policies that govern the entire data lifecycle, from initial collection standards and defined retention periods to protocols for permitted use, secure sharing, and eventual secure disposal.

The third pillar, formalized data request & disclosure workflow, operationalizes the principles of controlled disclosure through a mandatory, technology-supported process for all non-routine data exchanges, moving decisively away from ad-hoc practices. This workflow typically involves a sequenced, auditable process: (1) intake, where a requester submits a formal application detailing the specific data fields, scholarly or operational purpose, duration of use, and proposed security safeguards; (2) steward review, where the relevant Domain Data Steward assesses the request's appropriateness, maps it to the Single Source of Truth (SSOT), and evaluates the technical and quality readiness of the requested data; (3) privacy/security review, conducted by the Privacy Officer or Health Information Management (HIM) office to ensure compliance with HIPAA, GDPR, and other applicable regulations; (4) approval/denial, where a final authority grants approval (often with specific conditions) or denies the

request, with a clear rationale documented for transparency and auditability; and (5) provision & monitoring, where data is provided in a secure manner (e.g., de-identified, within a controlled analytics sandbox) and subsequent access and use are actively monitored and logged (Wang et al., 2022).

Finally, the fourth pillar, embedded data quality & metadata management, ensures that governance delivers on its promise of trustworthiness by making quality an inherent characteristic of the data ecosystem, not a retrospective correction. This requires several key practices: the implementation of proactive quality rules defined by stewards and engineered into systems wherever possible, such as forced-field validations in EHRs or automatic range checks for laboratory values (Dammery et al., 2023); the certification of readiness, whereby key datasets for executive reporting or research are formally "certified" by stewards once they meet pre-defined quality thresholds; and active metadata management, involving the maintenance of accessible, business-friendly data dictionaries and lineage documentation that explicitly define each critical data element (e.g., the precise business logic for calculating a "hospital-acquired infection rate"). This robust metadata is essential for ensuring semantic consistency across medical laboratories and enabling true interoperability within health informatics systems (International, 2017).

The synergy of these four pillars is encapsulated in Table 2 and Figure 2, which outlines the core components, their respective roles, and the key outputs of the proposed integrated framework. This structure provides a comprehensive blueprint for healthcare organizations to build a governance program that is both principled and practicable.

Figure 2. Key Risks Associated with Inadequate Data Governance in Healthcare

Table 2: Components of the Proposed Integrated Data Governance Framework

Framework Pillar	Key Components	Responsible Roles	Outputs/Deliverables
1. Leadership & Accountability	Data Governance Council; Domain Stewardship Committees; Charter & Bylaws; Funding Model.	Executive Sponsors; Chief Data Officer; Clinical & Operational Leads (as Stewards).	Strategic Roadmap; Approved Policies; Resolved Escalations; Resource Allocation.
2. Classification & Policy	Data Sensitivity Schema; Business Glossary; Lifecycle Management Policies (Retention, Archival, Deletion).	Data Stewards; Privacy Officer; Legal & Compliance.	Classification Taxonomies; Approved Policy Documents; Audit Protocols.
3. Request & Disclosure Workflow	Standardized Request Form/Portal; Triage & Routing Logic; Review Checklists; Approval Authority Matrix; Audit Logs.	Data Custodians (IT); Request Coordinators; Data Stewards; Privacy/Security Officers.	Fulfilled Data Requests; Denial Records with Rationale; Comprehensive Audit Trails.
4. Quality & Metadata	Data Quality Dimensions & Metrics; Validation Rules; Data Certification Process; Business Glossary; Lineage Documentation.	Data Stewards; Data Analysts; Quality Improvement Staff; Informatics.	Data Quality Scorecards; Certified Datasets; Published Data Dictionary; Lineage Maps.

Implications for Multidisciplinary Healthcare Practice Adopting the proposed integrated data governance framework necessitates a profound cultural and operational transformation across all healthcare disciplines, redefining roles, responsibilities, and workflows to align with the

principles of strategic data stewardship. For pharmacy and nursing professionals, this shift moves clinical documentation beyond a clerical task, re-conceptualizing it as a foundational data creation act with intrinsic quality responsibilities. It empowers designated nurse and pharmacy data stewards to authoritatively define the standards, terminologies, and validation rules for their domains, thereby ensuring that data generated at the point of care—from medication administration records to nursing assessments—is inherently reliable, structured, and fit for secondary use in analytics, research, and quality improvement (Topaz et al., 2017; George et al., 2017). In medical laboratories, the framework formalizes the critical role of laboratory directors and managers as the chief stewards for all diagnostic and test data. This formal stewardship ensures the rigorous application of standardized coding systems like LOINC and SNOMED CT, governs the validation of data transmission pathways from analyzers to the EHR, and establishes protocols for the handling of highly sensitive genomic data, thereby safeguarding diagnostic integrity and supporting accurate clinical decision-making (Dahlquist et al., 2023).

Concurrently, the role of health informatics is elevated from a focus on system maintenance to one of strategic enablement. Informaticians are tasked with designing and configuring systems that actively enforce governance policies, such as embedding stewardship-approved pick-lists, automating data quality checks, and implementing the standardized request-and-disclosure workflows that operationalize the governance model (Scott et al., 2017). For health safety and security professionals, the framework provides a structured mechanism to classify safety incidents and reports by risk, manage breach investigations with clear data lineage, and proactively control access to sensitive information, enabling a transition from reactive security firefighting to proactive, policy-based control and risk mitigation (Strome & Liefer, 2013).

Crucially, for health assistants and all frontline staff, the implementation of clear governance structures creates operational clarity and enhances psychological safety. Staff gain a concrete understanding of formal channels for data requests, their individual responsibilities in protecting patient information, and, ultimately, a justified trust in the quality and consistency of the data they rely on for daily patient care. To ensure this comprehensive model does not impede operational agility, the framework is designed with intentional flexibility, instituting tiered governance processes that provide expedited pathways for urgent, low-risk requests—such as those for routine operational dashboards—while mandating more rigorous, multi-step review for novel, high-risk data disclosures, such as those involving identifiable data for external research (Wieland-Jorna et al., 2023). This balanced approach ensures that the governance structure enables, rather than obstructs, both safe patient care and responsible innovation.

Conclusion

This study has highlighted that the most pressing data-related risks in healthcare—from patient safety incidents to regulatory breaches—are often symptoms of governance failure, rather than technological inadequacy. The proposed integrated conceptual framework addresses this root cause by institutionalizing stewardship, formalizing processes, and embedding quality and privacy into the data lifecycle. It provides a common language and structure for collaboration among the diverse professionals who create, manage, and use healthcare data.

While conceptual, this framework is grounded in established principles from information science, management, and healthcare ethics. It offers a robust blueprint for organizations to build or mature their governance programs. Future empirical research should focus on implementing and evaluating this framework in diverse settings (e.g., academic hospitals, community clinics, public health agencies) to refine its components and demonstrate its impact on measurable outcomes such as data error rates, compliance audit findings, time-to-insight, and ultimately, patient care quality and safety. In an era of big data and AI, robust governance is the non-negotiable foundation for a trustworthy, innovative, and ethical healthcare system.

References

1. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. *Procedia Computer Science*, *113*, 73-80. https://doi.org/10.1016/j.procs.2017.08.292
2. Abraham, R., Schneider, J., & Vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International journal of information management*, *49*, 424-438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008
3. Ahmadi, S., Tavana, M. M., Shokouhyar, S., & Dortaj, M. (2022). A new fuzzy approach for managing data governance implementation relevant activities. *The TQM Journal*, *34*(5), 979-1012. https://doi.org/10.1108/TQM-01-2021-0015
4. Bond, C. (2020). Pharmacy Practice Research: Evidence, Impact and Synthesis. In *Pharmacy practice research methods* (pp. 1-30). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-2993-1_1
5. Cohen, I. G., & Mello, M. M. (2018). HIPAA and protecting health information in the 21st

century. *Jama*, *320*(3), 231-232.doi:10.1001/jama.2018.5630
6. Dahlquist, J. M., Nelson, S. C., & Fullerton, S. M. (2023). Cloud-based biomedical data storage and analysis for genomic research: Landscape analysis of data governance in emerging NIH-supported platforms. *Human Genetics and Genomics Advances*, *4*(3). https://doi.org/10.1016/j.xhgg.2023.100196
7. Dammery, G., Ellis, L. A., Churruca, K., Mahadeva, J., Lopez, F., Carrigan, A., ... & Braithwaite, J. (2023). The journey to a learning health system in primary care: a qualitative case study utilising an embedded research approach. *BMC Primary Care*, *24*(1), 22. https://doi.org/10.1186/s12875-022-01955-w
8. Dixon-Woods, M., Campbell, A., Chang, T., Martin, G., Georgiadis, A., Heney, V., ... & Nelson, E. C. (2020). A qualitative study of design stakeholders' views of developing and implementing a registry-based learning health system. *Implementation Science*, *15*(1), 16. https://doi.org/10.1186/s13012-020-0976-1
9. Enticott, J., Braaf, S., Johnson, A., Jones, A., & Teede, H. J. (2020). Leaders' perspectives on learning health systems: a qualitative study. *BMC Health Services Research*, *20*(1), 1087. https://doi.org/10.1186/s12913-020-05924-w
10. George, R., Truong, T., & Davidson, J. (2017). Establishing an Effective Data Governance System: Data governance is necessary for compliance with current regulatory expectations or data integrity in pharmaceutical R&D and manufacturing organizations. *Pharmaceutical Technology Europe*, *29*(11), 40-44.
11. Groves, P., Kayyali, B., Knott, D., & Kuiken, S. V. (2013). The'big data'revolution in healthcare: Accelerating value and innovation. *McKinsey & Company*.
12. Hubbard, D., Freda, A., & Swanagan, A. (2020). Data governance 101: IR's critical role in data governance. *New Directions for Institutional Research*, *2020*(185-186), 51-65. https://doi.org/10.1002/ir.20329
13. International, D. (2017). *DAMA-DMBOK: Data management body of knowledge*. Technics Publications, LLC.
14. International Organization for Standardization. (2013). *ISO/IEC 27001: 2013: Information Technology--Security Techniques--Information Security Management Systems--Requirements*. International Organization for Standardization.
15. ISO. (2015). ISO 8000-1:2015 Data quality — Part 1: Overview. International Organization for Standardization. Retrieved from: https://www.iso.org/standard/50798.html
16. Kariotis, T., Ball, M. P., Tzovaras, B. G., Dennis, S., Sahama, T., Johnston, C., ... & Borda, A. (2020). Emerging health data platforms: From individual control to collective data governance. *Data & Policy*, *2*, e13. doi:10.1017/dap.2020.14
17. Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, *53*(1), 148-152. https://doi.org/10.1145/1629175.1629210
18. Kuzio, J., Ahmadi, M., Kim, K. C., Migaud, M. R., Wang, Y. F., & Bullock, J. (2022). Building better global data governance. *Data & Policy*, *4*, e25. doi:10.1017/dap.2022.17
19. Li, J., Yu, G., Ding, W., Huang, J., Li, Z., Zhu, Z., ... & Yin, J. (2021). Data governance system of the National Clinical Research Center for child health in China. *Translational Pediatrics*, *10*(7), 1905. https://doi.org/10.21037/tp-21-272
20. Liaw, S. T., Guo, J. G. N., Ansari, S., Jonnagaddala, J., Godinho, M. A., Borelli Jr, A. J., ... & Kahn, M. G. (2021). Quality assessment of real-world data repositories across the data life cycle: a literature review. *Journal of the American Medical Informatics Association*, *28*(7), 1591-1599. https://doi.org/10.1093/jamia/ocaa340
21. Loshin, D. (2010). *The practitioner's guide to data quality improvement*. Elsevier.
22. Mishra, V., & Mishra, M. (2022). Privacy and security concerns with electronic health records-shreds of evidence from India. *IMI Konnect*, *11*(3), 41-54.
23. Mosley, M., Brackett, M. H., Earley, S., & Henderson, D. (2010). *The DAMA guide to the data management body of knowledge*.
24. Ngesimani, N. L., Ruhode, E., & Harpur, P. A. (2022). Data governance in healthcare information systems: A systematic literature review. *South African Journal of Information Management*, *24*(1), 1475. https://hdl.handle.net/10520/ejc-info_v24_i1_a1475
25. Oktaviana, S., Handayani, P. W., & Hidayanto, A. N. (2022, August). Health Data Governance Issues in Healthcare Facilities: Perspective of Hospital Management. In *2022 10th International Conference on Information and Communication Technology (ICoICT)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICoICT55009.2022.9914865
26. Otto, B. (2011). Organizing data governance: Findings from the telecommunications industry and consequences for large service

providers. *Communications of the Association for Information Systems*, *29*(1), 3. https://doi.org/10.17705/1CAIS.02903

27. Rose, R. V., Kumar, A., & Kass, J. S. (2023). Protecting privacy: health insurance portability and accountability act of 1996, twenty-first century cures act, and social media. *Neurologic Clinics*, *41*(3), 513-522. https://doi.org/10.1016/j.ncl.2023.03.007
28. Scott, P. J., Rigby, M., Ammenwerth, E., McNair, J. B., Georgiou, A., Hyppönen, H., ... & Hackl, W. (2017). Evaluation considerations for secondary uses of clinical data: principles for an evidence-based approach to policy and implementation of secondary analysis. *Yearbook of medical informatics*, *26*(01), 59-67. DOI: 10.15265/IY-2017-010
29. Spector-Bagdady, K., Armoundas, A. A., Arnaout, R., Hall, J. L., Yeager McSwain, B., Knowles, J. W., ... & American Heart Association Advocacy Coordinating Committee. (2023). Principles for health information collection, sharing, and use: a policy statement from the American Heart Association. *Circulation*, *148*(13), 1061-1069. https://doi.org/10.1161/CIR.0000000000001173
30. Strome, T. L., & Liefer, A. (2013). *Healthcare analytics for quality and performance improvement* (p. 240). Hoboken, NJ: Wiley.
31. Tiffin, N., George, A., & LeFevre, A. E. (2019). How to use relevant data for maximal benefit with minimal risk: digital health data governance to protect vulnerable populations in low-income and middle-income countries. *BMJ Global Health*, *4*(2), e001395. https://doi.org/10.1136/bmjgh-2019-001395
32. Topaz, M., Ronquillo, C., Peltonen, L. M., Pruinelli, L., Sarmiento, R. F., Badger, M. K., ... & Lee, Y. L. (2017, February). Nurse informaticians report low satisfaction and multi-level concerns with electronic health records: results from an international survey. In *AMIA Annual Symposium Proceedings* (Vol. 2016, p. 2016).
33. van der Nat, D. J., Huiskes, V. J., Taks, M., Pouls, B. P., van den Bemt, B. J., & van Onzenoort, H. A. (2022). Usability and perceived usefulness of patient-centered medication reconciliation using a personalized health record: a multicenter cross-sectional study. *BMC Health Services Research*, *22*(1), 776. https://doi.org/10.1186/s12913-022-07967-7
34. Vassilakopoulou, P., Skorve, E., & Aanestad, M. (2016). Premises for clinical genetics data governance: Grappling with diverse value logics. In *The ethics of biomedical big data* (pp. 239-256). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-33525-4_11
35. Wang, M., Li, S., Zheng, T., Li, N., Shi, Q., Zhuo, X., ... & Huang, Y. (2022). 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), e36481. https://doi.org/10.2196/36481
36. Wieland-Jorna, Y., Verheij, R. A., Francke, A. L., Tomassen, M., Houtzager, M., Joling, K. J., & Oosterveld-Vlug, M. G. (2023). Setting up a governance framework for secondary use of routine health data in nursing homes: development study using qualitative interviews. *Journal of Medical Internet Research*, *25*, e38929. https://doi.org/10.2196/38929
37. Wiler, J. L., Welch, S., Pines, J., Schuur, J., Jouriles, N., & Stone-Griffith, S. (2015). Emergency department performance measures updates: proceedings of the 2014 emergency department benchmarking alliance consensus summit. *Academic Emergency Medicine*, *22*(5), 542-553. https://doi.org/10.1111/acem.12654
38. Williamson, K., Nimegeer, A., & Lean, M. (2022). Navigating data governance approvals to use routine health and social care data to evidence the hidden population with severe obesity: a case study from a clinical academic's perspective. *Journal of Research in Nursing*, *27*(7), 623-636. https://doi.org/10.1177/17449871221122040
39. World Health Organization. (2021). Is the Eastern Mediterranean Region ready for digitalizing health? implications from the global strategy on digital health (2020–2025).