The Nature and Improvement of Data Silos in the Medical Field

Jiaqi Li

Business School, University of New South Wales, Sydney, Australia
lisa0481232588@gmail.com

Abstract. Nowadays, healthcare data silos have attracted increasing attention in the context of digital health transformation, as they significantly influencing healthcare quality, operational efficiency, and public health governance. However, existing studies have largely focused on technical interoperability and data standardisation, while governance-related barriers including data ownership ambiguity and fragmented responsibilities is insufficiently discussed. This paper analyses the nature, manifestations, causes, and governance implications of healthcare data silos, with a particular focus on hospital-level and inter-organisational data governance rather than software development. The analysis shows that healthcare data silos are not only technical problems caused by incompatible systems, but also institutional and governance problems shaped by unclear data ownership, weak governance capacity, cybersecurity and privacy concerns, regulatory ambiguity, system heterogeneity, and uneven organisational incentives. These barriers solidly reduce willingness to share data and reinforce fragmented healthcare ecosystems. Based on these findings, this paper proposes three recommendations: clarifying data ownership and stewardship, strengthening cybersecurity frameworks with tiered data accessibility, and establishing cost-sharing mechanisms to support interoperability and long-term digital health transformation.

Keywords: Healthcare Data Silos, Digital Health, Data Governance

1 Introduction

Human society is rapidly stepping into a digital era, especially in technological innovation, establishing a widespread development on robot and big data in all range. In healthcare field, there is a significant growth of telemedicine and mobile health applications, as well as increasing adoption to Electronic Health Records (EHRs), with 11 of 27 surveyed OECD countries, including most developed countries such as Denmark and Sweden, showing more modernise healthcare environment [1].

Furthermore, nowadays, global is rapidly aging due to increased life expectancy (reached 73.3 years in 2024) and declining fertility [2]. Thus, the raising demand from elderly and youth for continuous and coordinated care highlight the necessities and importance of transforming medical technological into a more advanced level, encourage to create a more convenient and stable medical environment for all stakeholders.

© The Author(s) 2026
L. C. Yoong (ed.), *Proceedings of the 2026 2nd International Conference on Financial Innovation and Marketing Management (FIMM 2026)*, Advances in Economics, Business and Management Research 408,
https://doi.org/10.2991/978-94-6239-801-6_14

Within existing healthcare research, majority focusing on technical interoperability and data standardization, including Health Level 7(HL7) and Health Information Exchange (HIE) Studies [3]. Portal such as 'My Healthcare Record' in Australia and 'Helsenorge.no' in Norway has already contained official personal health record. Even though HL7 FHIR are widely, but it is still not fully address to all scenarios. However, a challenge of data governance should be raised and identified, including an issue of data fragmentation, ownership ambiguity and ethical dilemma of medical record sharing and privacy.

Theoretically, researching in healthcare digitalisation in medical field contribute to the development a national wide or even cross-national data governance framework, enabling medical industries build up a comprehensive and cross-departmental space for stakeholders to exchange information, and co-create value. Practically, it not only provides recommendations for regulators as a guidance to develop a holistic policy but also enhances the reliability and interoperability in designing governance mechanisms. Further improve global healthcare service into an idea of patient-centered care.

In light of this, this paper aims to analyse the development of a multi-level governance framework of healthcare data silos. Focusing on hospital-level and inter-organizational data governance and emphasising governance mechanisms rather than software development.

2 Manifestations of Healthcare Data Silos

2.1 Data Silos

In healthcare, data silos refer to situations where patient information is generated and stored in heterogeneous and non-interoperable systems, which limits data accessibility and prevents digital collaboration between healthcare organisations. Generally, it is always caused by incompatible technology or special industry culture, restricting data sharing and collaboration, strongly influencing process efficiency and decision making [4]. Data silos can be classified based on its origin: technical data soils, which is always caused by incapability of system structure; factors such as interests or responsibilities among organisations and regulations usually leads to institutional data silos; governance-level data silos, which exist in some countries that lack of a unified governance mechanism.

2.2 Problem Manifestation in the Healthcare Context

Within medical field, it is confirmed that the increasing use of HERs in healthcare information systems has created a massive data silo among worldwide healthcare providers since 1990s [5].

The characteristic of data silo can be diversified. Typically manifest as patient information is dispersed across multiple institutions, departments, and information systems rather than consolidated into holistic records. Furthermore, data silos demonstrate isolation, whereby data remains confined within specific hospitals or technical boundaries,

limiting cross-institutional accessibility. The dispersion of medical records across heterogeneous systems often results in biased or non-representative samples, limiting the generalisability and reliability of research results. In addition, impeded seamless interoperability is caused by system architecture incompatibility, such as non-aligned data format among different hospital departments.

2.3 Influences of Healthcare Data Silos

The influence of data silos towards enterprise success can be significant. From the perspective of a customer, patient may experience repeatedly submit the medical report and related documentation during the process of transferring hospital due to their medical reports are not permitted to be accessed between different organisations.

Clinicians are facing additional risk of medical errors as there is a lack of longitudinal health records. Decisions are made under incomplete information, which is either from patient's self-reported symptoms or external documentations they provide. Neither source usually offers a complete and integrated medical history, which is due to lack of a holistic database, this is technical data silos.

Standing on the side of hospital administrators, there is not only an operational inefficiency as data across different departments cannot be integrated simultaneously but also restricting the hospital's ability to implement data-driven performance management, including predicting patient flow and optimizing resource allocation. Results in reduced strategic flexibility and a constrained institutional adaptability in the broader context of digital health transformation.

For government and public health authorities, data silos posed a substantial challenge to regulatory oversight. Fragmented datasets would impede some surveillance dead zone, raising difficulties of tracking treatment quality. It also weakens real-time epidemiological surveillance towards population-level health governance, a delayed outbreak detection would weaken the capacity for coordinated public health responses.

3 Cause Analysis

3.1 Organisational & Institutional Barriers

The reason of data silos becomes an unmarkable issue within medical industry is the common unwillingness among majority of the organisations. The fundamental barrier is the lack of clarity of the data ownership as various parties are evolving in accessing patient's medical information, they may claim legitimate interests in the same dataset, including patients as the data subjects, hospitals as the data collectors and custodians, governments as regulators and insurers as users of billing and claims data. Organsiations have hesitation to share the data when the ownership is unclear as unauthorised data with unknown access right may bring legal liability and contain risks of misuse or loss of control. Therefore, institution tend to play safe and retain data internally rather than collaborating, eventually creating a 'default non-sharing' data environment. This problem is further reinforced by insufficient governance capacity at the national level. According to World Health Organisation (WHO), although more than 70% of countries

are covered with a digital health strategy and scaled digital health programmes, governance capacity still remains even and facing certain challenges including fragmented resources and inconsistent technical standards [6]. Clear governance mechanisms plays a crucial role in building a unified standard system, as it not only defined institutional responsibilities, but also coordinated oversight, avoiding data structural fragmentation in data ecosystems caused by incompatible systems or inconsistent data standards.

3.2 Regulatory and Legal Barriers

Cybersecurity Threats & Privacy Concerns. Medical data is highly sensitive as it reveals intimate details about a person's medical records and physical and mental health histories, holding a potential risk of causing discrimination, stigma, and economic harm. Thus, it becomes a major target of cyberattacks, attracting threats such as ransomware attacks, unauthorized access or even data breaches. In regard to digital healthcare systems, the more interconnected the system becomes, the larger the attack surface becomes. Therefore, cybersecurity brings people a strong institutional reluctance into data sharing as integration raises probability of vulnerabilities explosion, which would not only result in legal and financial consequences, but also easily cause reputational damage when breaches happen, leading to mistrust from patients for institutions to protect their information.

Despite the considerations of data breaches from hackers, privacy concerns also is one of the factors that intimidate people stepping into holistic digital healthcare systems. The purpose of using the information can be various, either malicious or good mindset, thus, the accessibility plays a significant role in protecting sensitive medical information from data leakage. Proper considerations should be included when institution decide to use the data, for example, whether patients have meaningfully consented, or whether data will be reused beyond the original clinical purpose or not. Data silo is the phenomena of a lack of trust among stakeholders in medical industries, as they may concern one another to misuse sensitive data or overreach in secondary use.

Regulatory Ambiguity. Among many countries' medical regulatory settings, the rules governing healthcare data sharing are incomplete, fragmented or even difficult to interpret, which creates additional barriers for organisations to align with proper implementation, exacerbating the formation of data silos. For instance, Indonesia's 2023 Health Law has been criticized for unclear provisions regarding the authority responsible for determining criminal allegations against medical personnel and the role of law enforcement agencies in dispute resolution. Due to this ambiguity, it takes 23 months of disciplinary investigations before reaching a decision in the case of Siti Chomsatun [7]. Therefore, Regulatory ambiguity often leads to legal uncertainty, which is something institution becomes conservative as compliance risk should always be minimised all round.

3.3 Economic Ambiguity

System Heterogeneity. There are various system development vendors across all countries, different organisations may considerate using different digital systems with different versions. It drives an increased difficulty for organisations and system developers in medical field to build up a holistic data sharing systems as the architecture and coding standard are unique among one and another. This heterogeneity would not only spend integration costs, but also additional cost for staffs who needs to be trained to adopted to new systems, as well as costs of long-term maintenance. Which is hardly to afford for startups or small and medium-sized enterprises as they may not support APIs, it would be extremely difficult for them to get rid of data silos. As interoperability becomes financially burdensome, integration is often postponed among the institution with limited capital, further driven the formation of data silos.

Organisational Interest Conflicts. Data in healthcare is not only a clinical resource but also a strategic institutional asset that can generate research value, operational advantage, and commercial benefits. Consequently, many organisations, particularly those operating in competitive environments, are reluctant to share data and instead prefer to retain it for internal research, analytics, and decision-making purposes. This reluctance is further compounded by the multi-stakeholder nature of healthcare data exchange, in which different actors possess distinct purpose and data priorities. Because stakeholders assess data-sharing requests from different institutional perspectives, consensus-building is often complex, time-consuming, and costly. A case study published in JAMIA Open demonstrates that establishing an academic health system requires extensive coordination among multiple institutional stakeholders, each evaluating different dimensions of a request, including ethics, privacy, and technical feasibility. This process often leads to sequential approvals, intensive cross-departmental communication, increased coordination costs, and delayed data access [8]. Moreover, conflicts of interest are intensified by uneven cost-benefit distribution across organisations of different sizes, as some institutions may derive greater value from shared data than others. In digital healthcare environments, such tensions can further entrench data silos, as organisations may fear losing patients, reputation, or market position if greater data portability enables patients to move more easily between providers without repeating tests or reconstructing medical histories. As a result, organisational interest conflicts, combined with stakeholder complexity, weaken incentives for collaboration and contribute to fragmented governance, selective participation, and defensive data retention, thereby exacerbated the formation of data silos.

4 Recommendation

4.1 Clarify Data Ownership & Stewardship

The analysis of organisational and institutional implementation barriers establishes the issue of unclear data ownership, fragmented responsibilities, and lack of coordination across healthcare stakeholders. To address this problem, it is recommended to reinforce

a necessity of clarifying data ownership and stewardship. First of all, a clear definition of data ownership with appropriate accessibility and management structure should be set in order to increase institutional willingness to share data so that data silo can be alleviated to some extent. By building up a stewardship model, allowing institutions to manage data responsibly without claiming exclusive ownership, ensuring accountability for data quality, access control, and ethical use.

Data stewardship model is not enough for data governance, it requires a centric data coordination department to facilitate collaboration between hospitals, insurers, and public health agencies. This multi-stakeholder governance model takes a critical role to harmonise various positions among stakeholders and oversee compliance with governance rules. Effectively helps to overcome data silos caused by institutional fragmentation and ensure seamless data accessibility.

4.2 Strengthen Cybersecurity Framework & Data Accessibility

Addressing cybersecurity threats and privacy concerns should be actively encouraged among medical institutions. It is recommended that cybersecurity framework should be strengthened among each organization, strictly follows cybersecurity framework such as NIST, ISO270001 and Essential 8. The necessity of recommending medical orgnisations prioritising cybersecurity framework can be reveled in Mayo Clinic's case in 2020, after data breaches incident, Mayo Clinic strengthened their collaboration with cybersecurity firms, advanced monitoring systems and improved infrastructure security [9]. Cybersecurity framework guides organisations to encrypted stored or transmitted data and store them under continuous monitoring and threat detection systems, productively increasing database's confidentiality, diminish the probability data silos caused by cyber-attack.

In addition, accessibility of data is recommended to attentively decide as it can improve governance transparency by clearly defining who can access what data and under what conditions, avoiding insider threats while gaining trust from patients. A tiered data access model is encouraged for institutions to use as it ensures that different users receive different levels of data access depending on their roles and purposes. For instance, clinicians may only access identifiable patient records for treatment whereas researchers may only access anonymized or de-identified datasets. This approach balances data sharing with privacy protection, allowing healthcare data to be utilized while minimizing ethical and legal risks. By doing so, data silos can be mitigated as data sharing systems can be built based on strictly protected privacy.

4.3 Cost-Sharing Mechanism

Every project needs financial support, mitigating data silo requires high costs of system integration or infrastructure upgrades, however, many institutions, especially smaller hospitals, may lack the resources and financial support to participate in interoperability initiatives. Therefore, it is recommended to launch a cost-sharing mechanisms to help small-medium-sized enterprise get rid of data silo and distribute the financial burden across stakeholders who benefit from improved data sharing.

To achieve cost-sharing mechanisms, government subsidies is recommended to be involved in order to encourage healthcare organizations to adopt interoperable systems. For instance, according to Australian Government Department of Health, government invested $107.2 million to modernize digital health systems and strengthen interoperability infrastructure during 2022 to 2023 [10]. The subsidies may finance for digital infrastructure development, demonstrate how government's participation can reduce financial barriers for healthcare providers and accelerate system modernization.

Moreover, is it also suggested to raise dedicated healthcare digitalization funds which allow governments to provide sustained financial support for long-term digital health transformation, including data standardization projects, and research infrastructures for real-world health data. For instance, the European Union launched the EU4Health programme (2021-2027) to strengthen the resilience and accessibility of healthcare systems across member states following the COVID-19 pandemic. The programme represents the largest health funding initiative in the EU, with a budget of approximately € 4.4 billion allocated to improve healthcare systems, address cross-border health threats, and support digital transformation in health services [11]. By providing financial support through grants and procurement mechanisms to national authorities, health organisations, and research institutions, this kind of funding aiming to reduce financial barriers to digital health adoption and promotes more coordinated and interoperable healthcare data ecosystems, mitigating data silos through effective actions.

5 Conclusion

This paper examined the issue of healthcare data silos in the context of digital health transformation and analysed the key barriers that prevent effective health information sharing across organisations. It found that healthcare data silos are not simply a technical problem resulting from poor interoperability or incompatible systems. Instead, the participation of technical, organisational, and governance-related factors enhance the formation of data silos. The analysis highlighted that problems such as fragmented governance structures, privacy and cybersecurity concerns and organisational interest conflicts all contribute to limited data sharing and the persistence of siloed information environments. Concluding that although technical standards such as HL7, FHIR, and health information exchange systems have improved the foundation for interoperability, technical solutions alone are insufficient to resolve the problem. Without clear accountability, coordinated governance mechanisms, healthcare organisations are likely to continue adopting defensive data retention practices.

Therefore, based on these findings, this paper argues that reducing healthcare data silos requires a more comprehensive governance-oriented approach that combines technical interoperability with clear ownership arrangements, stronger cybersecurity protection, and sustainable cost-sharing mechanisms. Future research could further examine how these governance strategies can be adapted across different national healthcare systems and institutional contexts.

References

1. Slawomirski, L., Lindner, L., de Bienassis, K., Haywood, P., Hashiguchi, T. C. O., Steentjes, M., Oderkirk, J.: Progress on implementing and using electronic health record systems: Developments in OECD countries as of 2021. OECD Health Working Papers (2023)
2. United Nations.: Ageing. United Nations (n.d.) https://www.un.org/en/global-issues/ageing#:~:text=Older%20people%20exercising%20in%20Bosnia,of%20children%20under%20age%2018 last accessed 2026/3/15
3. Ghanbari, S.: From Data Silos to Interoperable Ecosystems: Challenges and Solutions for EHR/HIE Integration in Digital Health. Trends in Health Informatics **2**(2), 82-90 (2025)
4. Kinast, B., Ulrich, H., Bergh, B., Schreiweis, B.: Functional requirements for medical data integration into knowledge management environments: Requirements elicitation approach based on systematic literature analysis. Journal of Medical Internet Research **25**, e41344 (2023)
5. Saberi, M. A., Mcheick, H., Adda, M.: From data silos to health records without borders: a systematic survey on patient-centered data interoperability. Information **16**(2), 106 (2025)
6. Global Initiative on Digital Health.: World Health Organization (n.d.) https://www.who.int/publications/m/item/global-initiative-on-digital-health last accessed 2026/3/22
7. Amiati, M., Halim, H., Hassim, J. Z.: Navigating ambiguity: Critiques of Indonesia's Health Law and its impact on legal redress for medical malpractice victims. Hasanuddin Law Review **10**(1), 94-107 (2024)
8. Davis, H. A., Kerkman, D., Hoberg, A. A., Countryman, M., Beaver, W., Bybee, K., Knosp, B. M.: Establishing data governance for sharing and access to real-world data: a case study. JAMIA Open **8**(3), ooaf041 (2025)
9. Okafor, C. M., Kolade, A., Onunka, T., Daraojimba, C., Eyo-Udo, N. L., Onunka, O., Omotosho, A.: Mitigating cybersecurity risks in the U.S. healthcare sector. International Journal of Research and Scientific Innovation **10**(9), 177-194 (2023)
10. Australian Government Department of Health.: How the 2022-23 Budget is investing in digital health. Australian Government (2022)
11. European Commission.: EU4Health Programme 2021-2027--A Vision for a Healthier European Union. European Commission (2021)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

