Crimson Publishers
Wings to the Research

Review Article

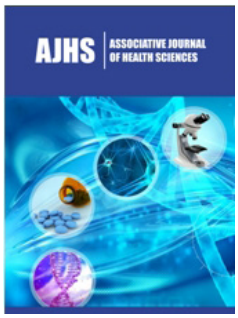
The Provision of Data Intermediation Services Related to Health: Main Challenges and Opportunities Associated with Innovation in Health Data Usage

Filipa Rubina Ferreira de Freitas[1]* and Altino Sousa Freitas[2]

[1]PhD student in law, Faculty of Law of the University of Lisbon and Master's Degree in Management and Public Policies, Instituto Superior Ciências Sociais e Políticas, Portugal

[2]Master's in Management and Public Police from the Higher Institute of Social Sciences and Policies, University of Lisbon, Portugal

ISSN: 2690-9707



***Corresponding author:** Filipa Rubina Ferreira de Freitas, PhD student in law, Faculty of Law of the University of Lisbon and Master's Degree in Management and Public Policies, Instituto Superior Ciências Sociais e Políticas, Portugal

Submission: November 11, 2024
Published: November 20, 2024

Volume 3 - Issue 4

How to cite this article: Filipa Rubina Ferreira de Freitas* and Altino Sousa Freitas. The Provision of Data Intermediation Services Related to Health: Main Challenges and Opportunities Associated with Innovation in Health Data Usage. Associative J Health Sci. 3(4). AJHS. 000569. 2024.
DOI: 10.31031/AJHS.2024.03.000569

Abstract

Data governance in the healthcare sector is a crucial element in ensuring the security, privacy, and integrity of confidential patient information. This paper addresses the challenges and opportunities related to sharing health data with data intermediation service providers, in partnership with hospitals. The research highlights the importance of complying with legal standards, such as the General Data Protection Regulation (GDPR) and the Data Governance Regulation, in data intermediation processes, emphasizing the need for conducting data protection impact assessments, adopting cybersecurity practices, and ensuring regulatory compliance. Effective data governance policies not only facilitate innovation in the healthcare sector but also strengthen public trust, creating a secure and efficient environment for using health data. The study also analyzes the infringement process initiated against Portugal by the European Commission in 2024, due to its failure to transpose the Data Governance Regulation, a European Union regulation that aims to improve data usage and facilitating its sharing, between the public and private sectors within the European bloc.

Keywords: Data governance; Digital health; Data protection; General data protection regulation; Data protection impact assessment

Introduction

The healthcare sector has undergone significant transformations with the advancement of information technologies and the increasing use of digital data. In this context, data governance has become an essential component to ensure the security, privacy, and integrity of confidential patient information. The sharing of health data, aimed to improve the treatment and the efficiency of healthcare systems, it requires a rigorous approach to ensure compliance with legal standards, such as the General Data Protection Regulation (GDPR) and the Data Governance Regulation.

This paper addresses the importance of data governance in the healthcare sector, focusing on the data intermediation process conducted by an external private company in collaboration with a hospital. Through this analysis, we explore the challenges and opportunities that arise from using health data, highlighting the legal requirements and best practices needed to ensure safe and efficient information sharing.

Implementing a data protection impact assessment, adopting cybersecurity practices, and complying with data protection regulations are essential to enable partnerships between public and private entities in the healthcare sector. Furthermore, we discuss the need for

robust technological infrastructure capable of protecting data while contributing to innovation and public trust.

Thus, this paper aims to examine the legal requirements and best data governance practices, with an emphasis on compliance with relevant legislation, such as the GDPR and the Data Governance Regulation, to ensure that health data intermediation is conducted safely and in accordance with European standards.

This exploratory study is qualitative in nature, with a descriptive and interpretive approach focused on a single case study. To achieve this study, we conducted research using document analysis and, as data analysis and processing techniques, content analysis, and the legal-normative triangulation of the normative legal framework, data protection regime, and the resulting action.

The study also analyzes the infringement process initiated against Portugal by the European Commission following its failure to transpose the Data Governance Regulation, an EU regulation aimed at improving data use and facilitating its sharing between the public and private sectors within the European bloc. It includes data analysis and conclusions intended to be useful in an increasingly global world.

The Use and Protection of Health Data

The use of health data has proven to be a powerful tool for transforming healthcare systems and improving patient care. However, the use of such data, especially in a context of growing digitalization and stringent regulation, faces several challenges. José Manuel Mendes [1] points out that health data privacy is essential to protect citizens' rights in a digital society, and only through solid governance can sensitive information be managed ethically and transparently. This stance reflects the need for strict measures to protect sensitive data and citizens' privacy.

One of the biggest challenges to innovation in health data usage is the protection of individual privacy. Health data is highly confidential, and its handling requires rigor to prevent data leakage. The EU's GDPR is a fundamental basis in this regard. However, implementing its standards remains challenging. Ana Paula Monteiro [2] emphasizes that GDPR compliance in healthcare institutions is not just a legal obligation, but a moral responsibility that aims to protect patients' dignity and privacy. This ethical commitment becomes even more complex in the interactions between public and private institutions, where, as Monteiro [3] notes, health data regulation faces ongoing challenges.

The GDPR provides a solid foundation for protecting such data, but applying its standards remains challenging, especially in contexts where data needs to be used for research and development [4]. Additionally, ensuring that data is irreversibly anonymized or that individuals' consent is obtained clearly and transparently is a complex task. Transparency in data usage and the risk of misuse remain major concerns for both citizens and organizations involved [5].

Another critical point is the interoperability of health systems, as many EU countries have systems that do not allow secure and efficient data exchange. This fragmentation makes it difficult to integrate data to promote innovation. Luís Antunes [6] observes that cybersecurity in the healthcare sector is a priority not only for protecting patient privacy but also for ensuring the integrity of the systems operating and mediating these sensitive data. Moreover, he emphasizes that robust technological infrastructure, aligned with best governance practices, is essential to resist cyber threats and safeguard health data [7].

The lack of common standards for data formats and fragmented systems hinders the efficient and integrated use of health data to foster innovation [8].

For instance, hospitals, clinics, and healthcare providers may use different systems for storing and managing patient data, making it difficult to combine or compare data from various sources. Interoperability between these systems is crucial to ensure that data can be shared and effectively used in innovation initiatives, such as creating big data analysis platforms or developing personalized medicine [9].

The inequality in data access and the technology needed to use it is another major obstacle. In some regions, a lack of technological infrastructure, such as the digitization of health records, limits the ability of healthcare providers and researchers to access crucial data. Carla Pereira da Silva [10] explains that effective data governance implementation in healthcare organizations depends on an organizational culture that prioritizes continuous training and awareness of data protection challenges and obligations. Silva [11] adds that data governance goes beyond compliance; it is an ongoing practice aimed at strengthening public trust in healthcare systems, which is essential to increase patient engagement and willingness to share information for research.

In some regions, the lack of technological infrastructure, such as digitalization of health records, limits healthcare providers and researchers' ability to access crucial data [4]. Additionally, individuals may lack access to platforms that allow them to control and share their health data.

The lack of digital training and disparities in technology access among different social and geographic groups represent a significant barrier to innovation, as the data available for research may not accurately reflect the needs of all population groups.

Finally, the rapid evolution of technologies such as artificial intelligence (AI) and wearable devices creates regulatory gaps. Often, legislation fails to keep pace with new types of data and technological practices. Miguel Pupo Correia [12] argues that data intermediation in the healthcare sector presents risks that require strict governance to ensure that intermediary companies respect and protect patients' data privacy. Correia [13] further notes that adopting advanced technologies, such as blockchain and anonymization, represents a necessary evolution for protecting sensitive data in the healthcare sector, strengthening governance, and fostering innovation.

These expert observations underscore the importance of robust data governance, cybersecurity, and compliance practices

to protect sensitive information, promote public trust, and enable advancements in healthcare.

Data protection framework in the European union

The European Union has taken a firm stance on creating a single European data space to foster innovation and the digital economy. This objective was set in the European Strategy for Data [COM (2020) 66 final], introduced in February 2020, and complemented by the White Paper on Artificial Intelligence [COM (2020) 65 final], aiming to position the European Union as a leader in data economy, research, and innovation. This single space is a fundamental step to maximizing data use for scientific, economic, and social progress, requiring a robust and harmonized legislative structure that ensures both personal data protection and the free flow of data within the EU [14].

Key regulations supporting this transformation include Regulation 2016/679, on personal data protection; Regulation 2018/1807, on the free flow of non-personal data; Directive 2019/1024, on open data; and Regulation 2022/868 on data governance. Additionally, the European Health Data Space (EHDS), created in 2020, aims to facilitate the exchange of electronic health data, portability, and the use of private data for secondary purposes [15].

The EHDS aims to ease the exchange of health data between Member States, ensuring security and privacy. It promotes data portability and collaborative efforts for altruistic purposes, such as scientific research. The Data Governance Act (2022/868) and other cybersecurity regulations are essential in regulating the intermediation of these data, creating a secure and efficient environment for data use in the healthcare sector. The establishment of the EHDS is a critical step toward creating a single health data market in the EU, with a strong emphasis on privacy protection and promoting scientific and technological innovations.

The initial framework for health data intermediation services and the EU legislative context can be analyzed considering various strategies and regulations established to create a single data market. The EU data space is a political priority designed to maximize data use to boost innovation and economic development, especially in healthcare [16].

Through the European Strategy for Data (COM (2020) 66 final) and the White Paper on Artificial Intelligence (COM (2020) 65 final), the EU has outlined a roadmap to transform data into strategic assets. This transformation is part of creating a single data market, including regulations that ensure the free flow and protection of data. Health data are critical in this context, enabling innovations in care, public policy, and research.

The General Data Protection Regulation (2016/679) establishes the basis for protecting privacy in the processing of personal data, including health data. Complementary to this, the Regulation on the Free Flow of Non-Personal Data (2018/1807) promotes the circulation of non-personal data, essential for aggregated analyzes and scientific research.

The Public sector bodies hold large volumes of protected data, such as personal data, trade secrets, and intellectual property, which cannot be considered open data. However, these data may be reused according to European and national legislation, always respecting privacy and confidentiality. Regulation (EU) 2022/868, regarding European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), establishes conditions for reusing data held by public sector bodies, reinforcing that reuse conditions must be transparent, non-discriminatory, and appropriate for data categories and intended uses.

Healthcare data regulation is essential to ensure privacy protection, foster sector innovation, and enable efficient data management within the European digital context. The existing regulatory framework and challenges associated with handling these data within the EU are discussed by several scholars, such as De Hert et al. [4], who emphasize the role of the General Data Protection Regulation as an essential tool for ensuring citizens' privacy, particularly concerning health data processing [4].

The General Data Protection Regulation (EU Regulation 2016/679) serves as the primary EU legislation for protecting personal data, including health data. As discussed by Custers et al. [5], the GDPR mandates that sensitive data, such as health data, require higher protection standards, emphasizing transparency, security, and individual control over their data [5].

The Free Flow of Non-Personal Data Regulation (EU Regulation 2018/1807) facilitates the circulation of aggregated or anonymous data, promoting data analysis for research and innovation. Hargittai et al. [9] note that combining non-personal data with robust GDPR regulation can accelerate research in areas like public health and new treatment development without compromising individual privacy [9].

While the European Health Data Space (EHDS) aims to create an environment that fosters interoperability of health data among Member States, as discussed by Kroes et al. [8], who stress that interoperability is essential for efficient and secure data exchange across different healthcare systems [8].

Applicable requirements for data intermediation service providers

The Data Governance Act (Regulation (EU) 2022/868), established by the European Union, mandates that data intermediation service providers adhere to stringent requirements when intermediating the sharing of personal and non-personal data. The Regulation defines data intermediation services as the creation of platforms or infrastructures that enable data sharing between different parties, making it essential to ensure neutrality and security in data use, as stipulated in article 1 of the Regulation. The principle of neutrality in intermediation is crucial to ensure that service providers act without influencing or manipulating data exchanges (Regulation (EU) 2022/868, article 5).

Furthermore, data intermediation service providers must act solely as intermediaries and refrain from using the data for

other purposes, in compliance with article 6 of the General Data Protection Regulation (GDPR) - 2016/679, which prohibits processing personal data for purposes incompatible with the original purposes. Transparency and trust are core principles of the GDPR, essential for ensuring that parties involved, such as data subjects and users, have control over how data is shared and used (articles 5 and 12 of the GDPR).

The Chapter III of the Data Governance Act of the European Union specifically addresses the requirements for data intermediation services. These services aim to facilitate data sharing between data subjects and data holders on one side, and data users on the other, promoting a network for information exchange through platforms or technological infrastructures to establish commercial relationships. This intermediation process also enables the exercise of data subjects' rights regarding their personal data, as stipulated in article 2(11) of the Regulation.

The Regulation defines "data sharing" as an operation in which the data subject or holder provides data to a user, allowing either joint or individual use of the data. This sharing may occur through voluntary agreements or under EU or national laws, either directly or through a third entity. The sharing may take place via open or commercial licenses, either free of charge or subject to fees (article 2(10)).

The figure of the "data holder" refers to a collective entity - including public bodies or international organizations - or an individual who, although not the data subject, has the right to grant access to or share certain data, whether personal or not, as defined by EU or applicable national laws (article 2(8)). In turn, the "data user" is any natural or legal person with legal access to certain data and the right to use it, whether for commercial purposes or not, in compliance with current legislation, including the GDPR concerning personal data (article 2(9)).

These data intermediation services, whether public or private, may involve various data-sharing formats, such as bilateral or multilateral data exchanges. Applicable models include the creation of platforms or databases for shared and collective data use and the implementation of a specific infrastructure to connect data subjects and holders to users (recital 27).

In the context of personal health data, intermediation services play a vital role in promoting efficient use and secure bilateral data sharing. However, the lack of specific applicable legislation currently prevents the initiation of operations in certain areas.

The category of data intermediation services, as defined in the Data Governance Act, includes service providers who act directly on behalf of data subjects. These providers must assist data subjects in exercising their rights under the GDPR, including rights such as consent for data processing (article 6), access (article 15), rectification (article 16), erasure (article 17), and data portability (article 20).

These services, as described in article 4 of the Data Governance Act, are not altruistic, as they aim to generate profit, implying the need for careful supervision by competent authorities to prevent misuse of data subjects' data, as established in article 71 of the GDPR.

One of the key requirements of the Data Governance Act is conducting a Data Protection Impact Assessment (DPIA). This assessment, required before implementing any personal data processing procedures, is mandated by the EU GDPR. The DPIA aims to identify, evaluate, and mitigate potential risks related to personal data processing, especially in high-risk contexts, such as healthcare. Conducting this assessment is essential to ensure that data intermediation practices comply with legal provisions and that users' personal data are handled with maximum security and protection.

Ensuring users, the right to informed consent regarding the use of their personal information is a legal obligation established by the GDPR, particularly in articles 6 and 7, which address data processing legality and consent. article 7 of the GDPR requires that consent be "freely given, specific, informed, and unambiguous," ensuring that data is processed solely for determined purposes, with full awareness and control by the data subject. This consent, as per the GDPR, can be withdrawn at any time, reinforcing individuals' rights over their personal data.

To fulfill this obligation, healthcare service providers must adopt protective mechanisms that limit data access to authorized individuals and for specific purposes. Article 32 of the GDPR establishes that data controllers must adopt "appropriate technical and organizational measures to ensure a level of security appropriate to the risk," including access control practices and security measures in data processing.

Additionally, ensuring that technological infrastructures are prepared to address cybersecurity threats aligns with the NIS2 Directive (Network and Information Systems Security Directive), which imposes strict cybersecurity requirements across the EU, necessitating a proactive stance against cyber risks, using measures such as data encryption and robust authentication. These practices are essential to protect health data, considered sensitive data under article 9 of the GDPR, as inadequate protection could pose significant risks to individuals.

Compliance with cybersecurity guidelines is also critical to prevent data breaches, as emphasized by Luís Antunes [7], who highlights the importance of robust infrastructure that follows best governance practices to ensure the security and integrity of systems. These practices include continuous monitoring and rapid response to security incidents, which are essential for protecting health data.

Measures to consider in data protection

Public trust in the handling of their health data is essential for the success of any innovation initiative. Fears about data breaches, misuse, or sales of personal information may make individuals reluctant to share their data with researchers or healthcare professionals [8].

In some cases, citizens may fear that their health data will be used for commercial purposes, such as advertising or insurance, or accessed without proper consent. This could affect individuals' willingness to participate in research studies or use digital health technologies, limiting the reach of innovations and reducing their potential positive impact.

The rapid evolution of health technologies, such as artificial intelligence (AI) and health monitoring devices, creates a regulatory gap in many situations. Current legislation often does not fully cover new data types and practices emerging with these technological innovations [4].

For example, AI technologies that analyze large volumes of health data may raise new issues concerning accountability in cases of medical errors or automated decisions, such as incorrect diagnoses or inappropriate treatments [5].

To ensure that health data usage is effective and beneficial, it is necessary to implement various strategies to address the challenges mentioned and harness the opportunities presented by innovation. Below are some key strategies that can be adopted to maximize the potential of health data.

The use of health data poses significant privacy risks, necessitating the strict implementation of data protection laws, such as the General Data Protection Regulation in the European Union [15]. However, regulation alone is insufficient. Healthcare organizations should adopt good digital security practices, such as encryption, a fundamental technique for data protection, ensuring data integrity and confidentiality both in transit and at rest [17]; anonymity technologies, which play a crucial role in protecting individual identities, allowing data analysis without compromising privacy [18]; obtaining informed consent that is clear and transparent, enabling patients to understand how their data will be used [19]; proactive monitoring systems to detect unauthorized access and minimize security risks [20]. Additionally, public education on data protection measures is essential to build trust and acceptance [21].

The interoperability of healthcare systems is crucial for improving data exchange and care efficiency [22]. Strategies to promote this interoperability include establishing technical standards, such as HL7 FHIR, which has proven effective in facilitating data exchange among healthcare systems [23]; integration platforms that can centralize and analyze data from diverse sources, enabling more comprehensive and efficient care [22]; collaboration among governments, healthcare organizations, and technology companies to promote more integrated and innovative systems [24].

Digital inclusion is an essential strategy to ensure that all individuals, regardless of location or socioeconomic status, can access and contribute to the use of health data. Some of these strategies include investing in digital infrastructure in remote regions to ensure access to digital health platforms [25]; digital literacy programs that are essential to empower vulnerable populations to use digital health platforms [26]; and public policies should be oriented toward ensuring that the benefits of health data usage are accessible to all, including marginalized groups [27].

To ensure collaboration between citizens and healthcare organizations, establishing a culture of trust is essential. These strategies include healthcare organizations ensuring transparency in data collection and use practices, allowing patients to understand how their data is being utilized [19]; feedback mechanisms, such as public consultations, to help create an environment of trust and collaboration between citizens and healthcare organizations [28]; and independent audits to help ensure that security and privacy practices are upheld [21].

The speed of technological innovations requires dynamic and adaptable regulations. Some strategies include creating multidisciplinary committees with technology and ethics experts to help formulate flexible regulations that keep pace with innovations [29]; involving all stakeholders in creating regulations to ensure that the new standards meet the sector's needs [22]; and testing new technologies in controlled environments as an effective way to ensure they are safe before large-scale implementation [20].

The use of health data offers numerous opportunities to improve healthcare systems. Some of these opportunities include using health data to create personalized treatments tailored to patients' genetic and behavioral characteristics, improving therapeutic outcomes [30]; using large volumes of data to identify early risk factors and implement preventive interventions with great potential to improve public health [31]; and automating and using artificial intelligence (AI) to process data, which can reduce medical errors and increase efficiency in hospitals and clinics, resulting in better care and reduced costs [32].

Infringement Procedure against Portugal

In May 2024, the European Commission initiated an infringement procedure against Portugal for failing to transpose the Data Governance Regulation, a European Union regulation aimed at improving the use of data and facilitating sharing between the public and private sectors within the European bloc. This regulation is part of the European Union's effort to create a single data market, promoting innovation and ensuring member states' competitiveness. Portugal's non-compliance, primarily due to the lack of designation of competent authorities and the absence of necessary normative acts to properly regulate data intermediation services, was highlighted as a major issue [16].

The Data Governance Regulation, approved in 2022 and entering into force on 24 September 2023, aims to ensure a robust legal framework for data sharing and governance in the European Union. It establishes the conditions for the creation of data intermediation platforms, which facilitate access to public and private data, while ensuring privacy protection and compliance with the General Data Protection Regulation. Its implementation aims not only to improve the use of data for innovation purposes, but also to reduce the legal and operational barriers that hinder the circulation of data in the European internal market [33].

However, for the regulation to be fully effective, member states need to transpose its provisions into national law, establishing the structures required for practical implementation.

In the case of Portugal, the lack of a clear regulatory framework for data intermediation services, as well as the failure to designate competent authorities responsible for overseeing and monitoring this area, were the main shortcomings pointed out by the European Commission [34].

The regulation requires member states to appoint authorities responsible for overseeing the implementation of the data governance regime. These authorities must ensure that data-sharing practices are secure, transparent, and compliant with EU standards [35].

Beyond the appointment of competent authorities, it is essential for member states to implement normative acts regulating the operation of data intermediation service providers. Without these acts, providers lack clarity on the legal requirements to be followed, which could undermine the regulation effectiveness and the EU data market [36].

This infringement may lead to more severe legal consequences if Portugal fails to take corrective measures within the timeframe set by the European Commission. If the Portuguese government does not provide an adequate response or fails to implement the necessary measures within two months, the case may be referred to the European Court of Justice [37].

Consequences and potential impacts on the infringement proceedings may evolve for an action in the Court of Justice of the European Union, the consequences for Portugal may be significant.

The European Union has the option to impose financial penalties on member states that do not meet their obligations. These fines can be substantial and may increase if non-compliance persists over time [14].

Non-compliance with the Regulation undermines the effectiveness of the single data market, which is essential for innovation and competitiveness within the EU's digital economy. The absence of an adequate regulatory framework could delay or even hinder the implementation of data intermediation platforms, crucial for creating an efficient data ecosystem [38]. Beyond the legal consequences, this infringement may impact Portugal's reputation within the European landscape, eroding trust among companies and investors in the country's regulatory environment [39].

To address this, Portugal must appoint authorities responsible for overseeing data intermediation services, ensuring these entities have the resources and authority needed to regulate data governance [40]. It will be necessary to establish normative acts regulating data intermediation service providers, defining the conditions for their operation and ensuring transparency and security in data transactions [41].

Portugal will need to communicate to the European Commission that it is adopting measures to correct the identified deficiencies and avoid action in the European Court of Justice. Compliance with the Data Governance Regulation is crucial, not only to avoid sanctions but also to ensure that Portugal effectively integrates into the European digital market, leveraging the opportunities for innovation that data governance can offer [42]. For a company to operate legally under Portuguese jurisdiction and in compliance with European Union standards, it must meet the conditions established by the Data Governance Regulation, especially regarding the handling and sharing of health data. This regulation, which seeks to create a trusted environment for data circulation, establishes clear rules for data governance in sensitive areas such as healthcare, obligating data intermediation entities to respect citizens' rights and ensure data is used transparently and securely.

Cooperation between entities should therefore respect not only legal obligations but also foster a culture of trust and digital transparency, supporting an ethical relationship with users. Carla Pereira da Silva [12] points out that data governance goes beyond mere legal compliance; it involves promoting a trust-based relationship that encourages users to participate in digital health initiatives, assured that their data will be treated ethically and securely. User trust thus becomes the foundation for successful health data sharing, especially in an environment where security and privacy are continually challenged by emerging digital threats.

Data Governance in the Healthcare Sector

Data governance in the healthcare sector involves defining policies, practices, and organizational structures aimed at ensuring that health data is managed ethically, securely, efficiently, and in compliance with applicable laws and regulations, such as the General Data Protection Regulation (GDPR) and the Data Governance Act.

Data governance can be understood as a set of established practices and processes to ensure that data is managed effectively, with respect for individual rights and legal norms. In a sector as sensitive as healthcare, data governance becomes a fundamental aspect for ensuring patient privacy, transparency in data use, and compliance with legal standards. Authors like Khatri and Brown [43] assert that data governance encompasses various processes, including the creation of standards, policies, and responsibilities to ensure data quality and regulatory compliance.

Data governance in healthcare is essential for facilitating data sharing between different entities securely and efficiently. The primary objective is to ensure that data is used in a controlled manner, respecting privacy and security policies. As argued by Dahlberg [44], data governance serves as an enabler for innovation and collaboration among stakeholders in the healthcare ecosystem.

To ensure secure data sharing, governance must be structured with a series of control measures, including defining who has access to the data, how the data will be used, and how data auditing will be conducted. Data governance also includes the establishment of practices to anonymize and pseudo-anonymize data, in order to protect the identity of individuals, especially when data is shared between entities.

The Data Governance Act specifically aims to regulate the flow of data within the European Union, promoting the ethical and transparent use of data. According to Frey [45], implementing a robust data governance system is essential for effective regulatory enforcement.

One of the requirements of the Data Governance Act is the need to ensure that all parties involved in health data intermediation conduct a Data Protection Impact Assessment (DPIA), as mandated by the GDPR. The DPIA allows organizations to identify risks associated with the processing of personal data and to take measures to mitigate them. This process, as highlighted by Gonzalez et al. [46], contributes to effective governance by promoting data security and legal compliance.

Citizen trust in health data sharing is critical for the success of initiatives with partnerships. Data governance ensures that data processing practices are transparent, and that users' rights are respected. As argued by Zwitter and Hazen [47], transparency in data governance practices is essential to ensure public acceptance of health data use.

Data governance also helps ensure that data is used for specific and legitimate purposes, such as improving healthcare and conducting research, without compromising user privacy and protection. Authors such as Sengupta et al. [48] highlight that effective governance enables a balance between innovation benefits in healthcare and patient data protection, contributing to the development of more personalized and efficient solutions.

While data governance offers many opportunities to enhance the use of health data, it also presents significant challenges. Implementing effective governance policies in healthcare requires not only legal compliance but also adapting to new technologies and evolving data security and privacy needs. Authors like Parker et al. [49] note that one of the biggest challenges of data governance in healthcare is the fragmentation of data protection policies across different entities, which can hinder data interoperability and integration.

In addition, it is essential to ensure that the technologies used are aligned with the best cybersecurity practices, protecting data from attacks and information leaks. To overcome these challenges, data governance needs to be dynamic and capable of quickly adapting to new threats and technological changes, as suggested by McKinsey & Company [50].

Methodological Approach

This exploratory study takes a qualitative approach, with a descriptive and interpretive focus, centered on a single case study, following Flick's (2009) guidance on the importance of a deep understanding of the phenomenon in question through the analysis of a single situation or context. The choice of a qualitative approach reflects the aim of holistically understanding the elements that comprise the study's subject, enabling a rich and detailed interpretation of the data collected.

For the purpose of this study, a research based on document analysis was conducted, which is set up as a fundamental data collection technique for obtaining information about the object of study, considering that the analyzed documents are primary sources and offer a clear of the legal and regulatory context involved. Documentary analysis allowed the identification of relevant rules, regulations and legal decisions, while providing a solid basis for understanding the practices and guidelines in force.

Regarding data analysis and processing techniques, content analysis was used, a method characterized by the systematic extraction and interpretation of information from the analyzed documents. Content analysis facilitated the organization and categorization of information, as well as the identification of patterns and trends related to the legal and regulatory context of data protection. According to Bardin (2011), this technique is particularly useful when seeking to understand the implicit dimensions within texts, beyond what is explicitly addressed.

Additionally, legal-normative triangulation was employed as an additional analysis strategy. Triangulation is a data validation process using different sources or analytical approaches. In this case, a triangulation was conducted among the legal-normative framework, data protection regulations, and actions resulting from these regulations to ensure a comprehensive and robust analysis. Legal-normative triangulation allowed for a deeper reflection on the legal, ethical, and practical implications of data processing within the study context, enabling the correlation between theory, existing legislation, and implemented practices.

The combination of these methodological approaches provided a detailed and multifaceted understanding of the problem, favoring a critical analysis of norms and actions related to data protection, with special attention to how these norms are applied and interpreted in specific situations. The use of triangulated analysis, as suggested by Denzin (1978), strengthens the reliability of results by validating information and increasing the depth of interpretive analysis.

Analysis

This analysis was guided by themes such as compliance with data protection legislation, challenges and opportunities in health data sharing, data governance policy implementation, and evaluation of potential legal infringements.

The texts emphasize the need for health entities and data intermediary companies to strictly comply with legal standards, such as the GDPR and Data Governance Act, to ensure patient data protection and secure data sharing. Compliance with these standards is seen as essential to ensure that data is used securely and responsibly while protecting data subjects' rights, including rights to informed consent, access, deletion, and data portability.

Compliance with data governance standards is central to the efficient and secure operation of the healthcare sector, ensuring trust among patients, healthcare professionals, and other stakeholders involved in data processing. Non-compliance may lead to legal sanctions and loss of public trust.

Health data sharing faces several challenges, including protecting patient privacy, cybersecurity, informed consent, and resistance to data sharing. The texts mention the importance of transparency and trust in overcoming these challenges, highlighting the need for effective data governance policies.

Data sharing can offer significant opportunities for healthcare innovation, such as the development of new treatments, more precise research, and improvements in healthcare system efficiency. Additionally, data utilization can lead to the creation of new business models and technological solutions.

Data sharing can be both a challenge and an opportunity, depending on how institutions address privacy, security, and governance issues. Overcoming these challenges can unlock a vast potential for healthcare service improvement.

The texts indicate that in 2024, the European Commission initiated an infringement procedure against Portugal for failing to comply with the Data Governance Act transposition. Non-compliance with this regulation can lead to negative consequences for the country, such as restrictions on data flow between the public and private sectors and even financial penalties. The infringement may also hinder collaboration with other EU countries and limit the use of data for innovation and research.

Non-compliance with the Data Governance Act transposition could impact access to new technologies and international partnerships, as well as weaken public and investor trust in data initiatives in the country.

The texts highlight the importance of implementing robust data governance policies to ensure the security and privacy of health data. This is essential to strengthen public trust in the use of sensitive data and to create a secure environment for innovation. Additionally, data governance policies not only protect data but also promote transparency, which facilitates public acceptance of data sharing.

Public trust can be significantly strengthened when data governance policies are clear, transparent, and ensure the security of sensitive information. This facilitates cooperation between the public and private sectors and patients, promoting healthcare innovation and advancement.

The main challenges identified are non-compliance with the Data Governance Act and resistance to data sharing. There are also issues related to the effective implementation of security measures, such as encryption and strong user authentication. On the other hand, health data sharing offers great potential for research innovations, new treatments, and healthcare management improvements. Adopting robust data governance policies can facilitate the secure use of data for these purposes.

Non-compliance with the Data Governance Act transposition could hinder collaboration among EU countries and restrict the use of health data in innovative research, with negative impacts on the healthcare sector's competitiveness and public trust.

We recommend improving the implementation of data governance policies, focusing on transparency, cybersecurity, and respect for data subjects' rights.

Conclusion

Data governance in the healthcare sector is essential to ensure the security, privacy, and integrity of patients' sensitive data.

The implementation of robust governance policies, aligned with the requirements of the Data Governance Regulation and the General Data Protection Regulation, is crucial to guarantee the safe and efficient sharing of health data.

Data governance is not only about legal compliance but also plays a crucial role in promoting innovation in the healthcare sector, enabling technological advancements while preserving the protection of individual data. Additionally, an effective data governance system strengthens public trust, creating a collaborative and transparent environment among the various stakeholders involved.

Partnerships represent a significant opportunity to enhance the use of health data, but they require a firm commitment to legal compliance and best governance practices. To ensure that data intermediation is conducted safely and in compliance with current legislation, it is essential to implement a Data Protection Impact Assessment (DPIA), as stipulated by the General Data Protection Regulation. This assessment will help identify risks and implement mitigation measures to ensure the safety and privacy of users' data.

Moreover, the organization should adopt rigorous data security practices, such as encryption and pseudo anonymous, to protect sensitive information during the intermediation process. These measures not only meet legal requirements but also help build a trusted environment, essential for the acceptance of health data use for clinical and research purposes.

By adopting these data governance and security practices, there will be a significant contribution to creating a more efficient, secure, and accessible healthcare ecosystem. Transparency and a commitment to data protection are undoubtedly essential elements to strengthen users' trust in the use of their personal data to improve the healthcare system.

References

1. Mendes JM (2020) Privacy and data governance in the digital society. Law and Society Journal 28(4): 101-115.
2. Monteiro AP (2021) Moral responsibility in GDPR compliance in healthcare institutions. Journal of Health and Law 7(2): 65-78.
3. Monteiro AP (2022) Health data regulation: Challenges and public-private interactions. Studies in Law and Technology 4(1): 34-49.
4. De Hert P (2021) The impact of the GDPR on health data regulation. European Data Protection Law Review 7(2): 146-158.
5. Custers B (2020) Data protection regulation and health data: Ensuring rights while promoting innovation. Journal of Data Protection & Privacy 4(1): 24-38.
6. Antunes L (2021) Cybersecurity in the health sector: Privacy and system integrity. Security and Information Technology 12(2): 47-59.

7. Antunes L (2022) Technological infrastructure and data protection in healthcare. Journal of Health Cybersecurity 15(1): 82-94.
8. Kroes J (2021) The challenges and opportunities of the European Health Data Space. European Journal of Health Law 28(4): 419-430.
9. Hargittai E (2021) The role of non-personal data in healthcare innovation in the EU. Health Policy and Technology 10(3): 100-112.
10. Silva CP (2019) Data governance and continuous training in healthcare organizations. Portuguese Journal of Health and Law 6(3): 50-64.
11. Silva CP (2020) Compliance and public trust in health systems. Health Management Journal 12(1): 29-42.
12. Correia MP (2020) Data intermediation and patient data protection in the healthcare sector. Technology and Law 5(3): 125-138.
13. Correia MP (2021) Blockchain and anonymization: Evolution for data protection in healthcare. Innovation and Security in Health 3(2): 55-67.
14. European Court of Justice (2020) Judgments on non-compliance with EU regulations. ECJ Case Law 22(4): 67-82.
15. European Commission (2016) General Data Protection Regulation (GDPR). Official Journal of the European Union.
16. European Commission (2024) Data Governance Regulation and Compliance Monitoring. Official Journal of the European Union.
17. Singh A (2021) Secure data sharing in healthcare: Challenges and solutions. Journal of Cybersecurity.
18. Shokri R (2011) Privacy-preserving data mining. IEEE Transactions on Knowledge and Data Engineering.
19. Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. Information Systems Research 17(1): 61-80.
20. Hughes A (2019) Improving data privacy and security in health systems. Healthcare Informatics Research.
21. O Neill M (2020) Building public trust in health data utilization. Journal of Health Communications.
22. Zhao J (2020) Interoperability of health data systems. Journal of Healthcare Engineering.
23. Rath S (2019) FHIR standard and its role in health data interoperability. Health Information Science and Systems.
24. González M (2018) Collaboration between healthcare and tech firms: A case study. Health Policy and Technology.
25. Mishra S, Mahanta S (2021) Digital health infrastructure in rural areas. Journal of Telemedicine and Telecare.
26. Parsons M (2015) Digital literacy and health platforms. Journal of Medical Internet Research.
27. Vega A (2020) Health data and social inequality. International Journal of Public Health.
28. Coughlan R (2019) Public engagement and trust in data use: Key factors. Health Information Management Journal.
29. Gupta A, Sagar M (2020) Adapting regulatory frameworks for healthcare technologies. Regulatory Affairs Journal.
30. Collins FS, Varmus H (2015) A new initiative on precision medicine. New England Journal of Medicine 372: 793-795.
31. Yasmin S (2020) Early detection of diseases using predictive modeling. Journal of Biomedical Informatics.
32. Bates DW (2018) Big data in healthcare: Challenges and opportunities. Journal of the American Medical Association.
33. Tolk A (2023) The role of data governance in advancing the EU digital single market. Journal of Digital Economy 45(2): 112-130.
34. Zhao L (2023) Regulating data intermediaries: The EU approach. European Law Journal 29(3): 277-294.
35. Finkelstein L (2022) The challenges of data governance and regulatory oversight. Journal of Information Policy 31(1): 45-60.
36. Akhter S, Rahman M (2021) Legal frameworks for data intermediaries: A comparative study. International Journal of Data Law 14(2): 88-102.
37. Jones R (2024) EU law and the enforcement of data protection regulations. European Legal Review 49(1): 1-15.
38. Baur F, Ho R (2023) The impact of regulatory compliance on innovation in the digital economy. Technology Policy Quarterly 18(3): 123-140.
39. Barta R (2022) Reputation and legal compliance in the EU: The case of data governance. Journal of Public Policy 38(2): 200-215.
40. Pereira J (2024) Establishing regulatory authorities for data governance in Portugal. Portuguese Law Review 30(1): 55-72.
41. Chen Z, Zhang X (2021) The legal challenges of data governance and intermediaries. Journal of Technology and Law 23(4): 145-162.
42. Meyer S (2023) Opportunities and challenges in EU data regulation. Digital Transformation Journal 17(2): 101-118.
43. Khatri V, Brown CV (2010) Designing data governance. Communications of the ACM 53(1): 148-152.
44. Dahlberg T (2014) Data governance in healthcare: A critical overview. Journal of Healthcare Management 59(3): 218-225.
45. Frey R (2017) Regulation and data governance in the EU: Challenges for health data sharing. Journal of European Law 24(3): 301-314.
46. Gonzalez R (2018) The role of data governance in GDPR Compliance. European Journal of Privacy and Data Protection 3(2): 142-154.
47. Zwitter A, Hazen J (2018) Governance in big data: Legal and ethical challenges. Big Data & Society 5(1): 1-15.
48. Sengupta S (2019) Data protection and healthcare: The governance of health data in the digital age. Journal of Health Policy and Technology 7(2): 118-128.
49. Parker C (2020) Governance of healthcare data: Challenges and opportunities. International Journal of Medical Informatics 142: 104243.
50. McKinsey & Company (2021) Securing healthcare data in the digital age. Healthcare & Life Sciences.