DATA GOVERNANCE IN HEALTH AND THE CHALLENGES OF INTEROPERABILITY IN PUBLIC POLICIES: THE CASE OF THE DIGITAL SUS (BRAZILIAN UNIFIED HEALTH SYSTEM)

A GOVERNANÇA DE DADOS EM SAÚDE E OS DESAFIOS DA INTEROPERABILIDADE NAS POLÍTICAS PÚBLICAS: O CASO DO SUS DIGITAL

GOBERNANZA DE DATOS EN SALUD Y LOS DESAFÍOS DE LA INTEROPERABILIDAD EN LAS POLÍTICAS PÚBLICAS: EL CASO DEL SUS DIGITAL (SISTEMA ÚNICO DE SALUD DE BRASIL)

https://doi.org/10.56238/sevened2026.009-050

Amanda Silva Madureira[1], André Victor Moraes Ribeiro[2], Danielle Cerqueira Castro[3], Gabriela da Silva Ribeiro[4], Luiz de França Belchior Silva[5], Maria José Carvalho de Sousa Milhomem[6], Vinicius Milhomem Guimarães[7]

ABSTRACT

Data has become central to governmental action, especially in the formulation and evaluation of public policies. In Brazil, the LGPD, combined with the Access to Information Law, the Civil Rights Framework for the Internet, and the Digital Government Law, structures information governance and security. In the health sector, advances were made with the National Policy on Health Information and Informatics, the digitization of medical records, teleconsultations, and vaccination systems. More recently, the SUS Digital Program and the adoption of the CPF as a unique identifier strengthen interoperability. In this sense, based on the hypothetical-deductive method, this article analyzes data governance in the SUS, its challenges of integration, funding, and coordination between public and private systems.

Keywords: Data Governance in Health. Interoperability. Digital Health.

[1]Dr. in Public Policy. Universidade Federal do Maranhão (UFMA). E-mail: Madureira.amanda@gmail.com
Orcid: https://orcid.org/0000-0003-3281-1839
[2] Graduated in Law. Faculdade Laboro. E-mail: MoraesSolomon@gmail.com
Orcid: https://orcid.org/0009-0001-3420-308X
[3] Specialist in Electoral Law. Universidade Federal do Maranhão (UFMA).
E-mail: daniellecerqueiracastro@gmail.com. Orcid: https://orcid.org/0009-0009-8392-6581
[4] Specialist in Restorative Dentistry. Faculdade de Ciências do Tocantins (FACIT).
E-mail: Gabiribeirou@gmail.com Orcid: https://orcid.org/0000-0002-4682-2603
[5] Dr. in Legal and Social Sciences. Universidad del Museo Social Argentino (UMSA).
E-mail: luizfbelchiorsilva@hotmail.com Orcid: https://orcid.org/0009-0003-0064-0016
[6] Dr. in Legal and Social Sciences. Universidad del Museo Social Argentino (UMSA).
E-mail: mjcsm@hotmail.com Orcid: https://orcid.org/0000-0001-8844-3364
[7] Postgraduate certificate in Transport Engineering. União Brasileira de Faculdades (UNIBF).
E-mail: Milhomem62@gmail.com Orcid: https://orcid.org/0009-0000-7193-2401

RESUMO
Os dados tornaram-se centrais para a atuação governamental, especialmente na formulação e avaliação de políticas públicas. No Brasil, a LGPD, aliada à Lei de Acesso à Informação, ao Marco Civil da Internet e à Lei do Governo Digital, estrutura a governança e a segurança da informação. Na saúde, houve avanço com a Política Nacional de Informação e Informática em Saúde, a informatização de prontuários, teleconsultas e sistemas de vacinação. Recentemente, o Programa SUS Digital e a adoção do CPF como identificador único fortalecem a interoperabilidade. Nesse sentido, partindo-se do método hipotético-dedutivo, o artigo analisa a governança de dados no SUS, seus desafios de integração, financiamento e articulação entre sistemas públicos e privados.

Palavras-chave: Governança de Dados em Saúde. Interoperabilidade. Saúde Digital.

RESUMEN
Los datos se han vuelto fundamentales para la acción gubernamental, especialmente en la formulación y evaluación de políticas públicas. En Brasil, la LGPD, en combinación con la Ley de Acceso a la Información, el Marco de Derechos Civiles para Internet y la Ley de Gobierno Digital, estructura la gobernanza y la seguridad de la información. En el sector salud, se lograron avances con la Política Nacional de Información e Informática en Salud, la digitalización de historiales médicos, las teleconsultas y los sistemas de vacunación. Más recientemente, el Programa SUS Digital y la adopción del CPF como identificador único fortalecen la interoperabilidad. En este sentido, con base en el método hipotético-deductivo, este artículo analiza la gobernanza de datos en el SUS, sus desafíos de integración, financiamiento y coordinación entre los sistemas público y privado.

Palabras clave: Gobernanza de Datos en Salud. Interoperabilidad. Salud Digital.

1 INTRODUCTION

The data, in the face of a myriad of application possibilities, already show themselves as an inexorable governmental reality. In the public sector, particularly, the use of data has proven effective for the formulation, evaluation and implementation of public policies. As a structuring normative guideline, Brazil approved and regulated the General Data Protection Law (LGPD) by ensuring greater control by citizens over their personal information, by requiring explicit consent for data collection and use, as well as in the creation of an entire regulatory infrastructure with the objective of protecting the fundamental rights of freedom and privacy and the free development of the natural person, intermediated by the National Data Protection Authority – ANPD (Brazil, 2018).

Progressively, the Brazilian government has embraced a series of normative diplomas focused on information infrastructure, such as: the Access to Information Law – Law 12,527/2011, the Civil Rights Framework for the Internet – Law No. 12,965/2014 and the Digital Government Law – Law No. 14,129/2021, which modernized the Public Administration by creating a single digital platform. It is the adoption of a complex regulatory and operational system that aims to provide security in the production and dissemination of data in our territory.

Historically, health information has been segregated into several sections, without covering the entire population. In 2015, for example, the Ministry of Health approved the National Policy on Health Information and Informatics and outlined the initial parameters for the production of health data. Currently, the growing computerization through electronic medical records, medical care through teleconsultations, production of vaccination data that serve for monitoring, for example, in the National Immunization Policy, regulation of hospital care in line with health policies, the dispensation of medicines and integration with supplementary health is notorious.

For all these reasons, the Ministry of Health approved, through Ordinance GM/MS No. 3,232/2024, the SUS Digital Program and Ordinance SD/MS No. 1,184/2025, which consolidated the Individual Taxpayer Registry (CPF) as the citizen's unique identifier in the public health system in the country. Thus, the Digital Health Strategy for Brazil – ESD (2020 to 2028) within the scope of the Ministry of Health establishes the conceptual foundation for the transformation of Digital Health by the states, Federal District and Municipalities.

In this sense, this article seeks to understand the normative and operational effort of data governance in the health area. The research problem that guided the present work was: how does data governance enable interoperability in SUS Digital and what are the main challenges for its implementation?

It is based on the hypothesis that the challenge of obtaining reliable health information faces the problem of the absence of complete integration and interoperability of information systems, whose root is largely the underfunding model of the health system, based on the absence of interaction between the official databases of the Ministry of Health and integration with systems of private providers, in the scope of supplementary health and private health.

This article examines the normative framework that structures data governance in the Brazilian public health system, considering the ordinances and resolutions issued by the Ministry of Health between 2020 and 2025, as well as the structuring legislation that includes the Federal Constitution of 1988, the Organic Health Law, the General Data Protection Law, and the Electronic Government Interoperability Standards. The analysis also considers studies on international experiences of health data integration and the conflicts between technical centralization and federative autonomy in large-scale systems. The research focused on understanding the tensions that emerge when interoperability standards meet the realities of municipalities with different technical and financial capacities.

Thus, the article is structured in the following sections: a) the fundamentals of data governance in the Public Sector; b) the legal and normative framework for the digital SUS; c) interoperability as an enabler of the digital SUS and d) the challenges of security, privacy and legal compliance. The hypothetical-deductive research method is presented and, as a research procedure, the bibliographic and documentary use, based on official government databases as well as scientific literature, with the use of the following research descriptors: a) health data governance; b) interoperability; c) digital health and d) health governance policies.

2 FUNDAMENTALS OF DATA GOVERNANCE IN THE PUBLIC SECTOR

Data governance in the Brazilian public sector has become a strategic imperative for the consolidation of an efficient Digital State, a concept that articulates the digitalization of public administration with new forms of digital governance (Belli; Guglielmi, 2022; Belli et al., 2024).

Data management involves developing, executing, and overseeing plans that control and protect these assets. Well implemented, it converts scattered records into strategic inputs that guide decisions, subsidize evidence-based policies, and support services to citizens. In this sense, data governance is in line with the constitutional diction of article 37 of the Federal Constitution of 1988 by establishing that the public administration must obey the principles of legality, impersonality, morality, publicity and efficiency (Brasil, 1988). Data governance applies this last principle by eliminating redundancies, enabling rational use of

resources, and enabling evidence-based decisions. Interoperability between systems concretizes the constitutional principle of efficiency in concrete practices.

Governance is structured on complementary dimensions. The exercise of authority defines responsibilities for the quality and security of information. The architecture establishes the map that allows connection between systems. Integration consolidates data between different repositories, allowing for a single citizen's view. Security ensures respect for the General Data Protection Law and quality ensures reliable data. Document management handles unstructured data. In the Unified Health System, these dimensions allow the continuity of care between levels of care (Brasil, 1988; Belli et al., 2024).

Ten main functions make up data management in public administration. Governance itself exercises authority and control, setting standards and responsibilities over assets. The architecture establishes technical drawings to meet the organizational strategy, providing the map that allows integration. Security implements protection policies. In the health sector, this function gains relevance because the LGPD classifies health data as sensitive (Brasil, 2018).

Integration and interoperability represents the technical mechanism that allows the single vision of the citizen. In the SUS, a patient treated in primary care must have his or her history accessible when he or she needs specialized care or hospitalization in another municipality. Quality guarantees reliable information, which in health can mean the difference between correct or wrong clinical decisions. An incorrect allergy record or erroneously entered test result leads to decisions with serious consequences. Quality also underpins system management, as decisions about resource allocation depend on reliable information. Document management deals with unstructured data such as medical images and reports. The literature highlights that quality data is a central resource for government digital transformation, generating economic and social value when properly governed (Zeleti; Ojo; Curry, 2016; Belli et al., 2024).

3 LEGAL AND NORMATIVE FRAMEWORK OF THE DIGITAL SUS

The definition of Health, according to the World Health Organization (1948) presupposes complete physical, mental and social well-being, and not just the absence of disease or infirmity. This conception of the WHO results, so to speak, in a complex of government actions aimed at promoting quality of life, an adequate social environment that satisfactorily promotes the social determinants of health.

In this sense, Brazil ensured in the Federal Constitution the importance of health by establishing it as a right and duty of the State, which should be guaranteed through social and economic policies aimed at reducing risks, diseases and other problems, as well as

universal and equal access to actions and services for its promotion, protection and recovery (Brasil, 1988). The materialization of the legal protection of the right to health enabled the creation of the Unified Health System (SUS) with the objective of promoting coordinated actions to guarantee the right to health.

Progressively, it can be affirmed that the Unified Health System (SUS), normatively supported by Law 8.080/1990 - Organic Health Law (Brasil, 1990), fostered the organization of a system based on the principles of universality, equity, integrality and outlined guidelines for regionalization and hierarchization in the provision of services. Universality justifies the adoption of health services guaranteed to all people, regardless of gender, race, and occupation. Equity, on the other hand, strengthens the purpose of reducing inequalities, while comprehensiveness presupposes the articulation of health with other public policies through intersectoral action between different areas that are related to the quality of life of individuals.

Law no. 8142/90 (Brasil, 1990), in turn, provides for community participation through Health Councils, Health Conferences and SUS financing, regulating transfers and investments in the health sector. It can be stated that the consolidation of a Unified Health System (SUS) was only possible due to the broad participation of the health movement and, consequently, to the creation of public health policies directed to the needs of the population. Although it is not the object of this article, but which has a connection with the theme addressed here, the Primary Health Care Policy (PHC) is recorded, formalized by the National Primary Care Policy (PNAB), which is presented as the main guideline for the level of care in the SUS, through services that must be organized in order to contemplate all regions of the country, by identifying the health needs of citizens, based on the adoption of a priority model that is the Family Health Strategy – ESF.

The imperative need to offer a range of services to the different regions of the country, embodied in multidisciplinary teams, Basic Health Units, Hospitals, reinforced the dissemination of health data, resulting, consequently, in an organizational structure focused on the production of information in the health sector. It was then that, in 1991, the Department of Informatics of the SUS (DataSUS) was created with the responsibility of making adjustments to the structuring of the Unified Health System. Already at that time, with the massive processing of data as a result of hospital information, the health system, once linked to social security, would need its own technological infrastructure (Saldanha, 2023).

In our country, there are several Health Information Systems that were created to meet various needs, such as payments for hospitalizations, administrative demands, professional services, or even for epidemiological purposes, as was the case with COVID-19, which enabled the integration of ICU bed data so that some cities would not be left without

the offer of these services. Saldanha (2023) points out that the diagnosis of Health Information Systems ended up with an overlap due to several components and transitory purposes. For this reason, some inconsistencies between systems, repetitions and errors are pointed out due to processes that should be improved over time. In addition, there is segregation between the Supplementary Health information systems (such as private health services) and the public instances of the SUS.

In order to normatively unify the issue of information and production of data in Health, the World Health Organization – WHO outlined the document entitled "Global Digital Health Strategy" with the purpose of supporting health systems in achieving universal health coverage through the use of disruptive technologies. It was then that digital health could be defined as a practice associated with the use of digital technologies to improve health, recognizing the advances in Artificial Intelligence, Internet of Things, and should be an integral part of health priorities, in order to benefit people in an ethical, safe and reliable environment under the principles of transparency, accessibility, scalability, and representativeness (WHO, 2021).

In Brazil, the Ministry of Health approved, through Ordinance GM/MS No. 3,232/2024, the SUS Digital Program, instituting a health care model by producing and making reliable information about health status available to those who need it, in order to offer the best possible care (Bertotti, 2021). Also noteworthy is the publication "Digital Health Strategy 2020-2028) – ESD, which seeks to align the various public and private activities and projects towards the digital transformation of health in Brazil.

From this perspective, some key elements can be recognized, such as: respect for the interests of states, municipalities and the population in the articulation of actions aligned with the principles of the SUS, the guidelines of the National Health Council and the Tripartite Interagency Commission; the essential involvement of public, private and supplementary health actors and the adoption of a Monitoring and Evaluation Plan so that it enables a consistent review of the population's new needs (Brasil, 2020).

Some priorities can be glimpsed, namely: a) governance and leadership for Digital Health; b) computerization of the three levels of care, with the inclusion of information policies of the health systems; c) support for the improvement of health care; c) the digital health user as the protagonist; d) training and qualification of human resources for digital health; e) interconnectivity environment and f) innovation ecosystems (Brasil, 2020).

To get an idea of the challenge of interoperability, one of the main concerns is precisely the lack of standardization of procedures for obtaining and processing health data. For this reason, the fundamental milestones of Digital Health at the governmental level have

consolidated the progressive institutionalization of services embodied in the Connect SUS Program, which implemented the National Health Data Network.

4 INTEROPERABILITY AS AN ENABLER OF THE DIGITAL SUS

Interoperability represents the central technical and managerial challenge for the integration of public health policies in Brazil. More than a technological issue, it involves the ability of different systems, developed by different suppliers at different times, to exchange information that can be used to improve patient care and subsidize the management of the system. In Brazil, this integration is guided by the Electronic Government Interoperability Standards (e-PING), which establish guidelines for the use of technology in the interaction between government and society (Brasil, 2018; Belli et al., 2024).

Interoperability in the SUS needs to be addressed on three interconnected fronts (Belli et al., 2024). This technical dimension deals with the infrastructure, communication protocols, and data formats that allow physical and logical connection between systems. In the Brazilian context, it means ensuring that the electronic medical record system of a basic health unit in a small municipality can send information to the state hospital system, which communicates with federal epidemiological surveillance systems. The adoption of international standards such as HL7 (Health Level Seven) and FHIR (Fast Healthcare Interoperability Resources) has become necessary to enable this communication. The FHIR standard has been adopted in Brazilian initiatives for its flexibility and compatibility with modern architectures, allowing structured and secure exchange of health data (Brasil, 2018). However, the adoption of these standards comes up against asymmetries of technical and financial capacity between municipalities, making technical integration, although conceptually feasible, a distributive challenge in practice.

Semantic interoperability represents the most complex challenge. It is not enough for systems to be able to exchange messages technically. The meaning of these messages must be preserved and understood uniformly by all actors involved. In the SUS, this requires standardization of clinical terminologies, disease classifications, and procedures. The International Classification of Diseases (ICD-10) and the SUS Table of Procedures are examples of controlled vocabularies that ensure that a diagnosis recorded in primary care is understood in the same way in a tertiary hospital. The absence of this standardization leads to serious consequences. A procedure code interpreted differently between systems can result in incorrect billing, inability to track procedures, and compromise clinical decisions. The construction of specific health ontologies for the Brazilian reality, considering international standards and particularities of the SUS, is still in progress. The adoption of

FAIR principles provides internationally recognized guidelines to ensure semantic interoperability of data (Schultes; Wittenberg, 2019; Brasil, 2018), although this standardization depends on continued training of health professionals in the correct application of controlled vocabularies and qualified technical supervision, resources that remain scarce in smaller municipalities.

Organizational interoperability involves aligning processes, workflows, and governance models between three spheres of government and various actors in the health system. In the SUS, with a federative structure and the participation of public and private services, this dimension presents specific complexities. It means coordinating how a municipal health department organizes referral processes with protocols for access to specialized services managed by the state.

The Electronic Government Interoperability Standards (e-PING), established in 2004 and reviewed annually, constitute the reference document that applies these three dimensions in concrete technical specifications (Brasil, 2018). For the health sector, e-PING establishes guidelines that all SUS systems must observe to ensure communication capacity. The rule, despite this, lacks an enforcement mechanism, resulting in heterogeneous compliance between federative entities.

e-PING favors the adoption of open standards and free software, a principle that became mandatory for the federal executive by Ordinance No. 92 of 2014 (Brasil, 2014). This orientation has important implications for the SUS. Open standards avoid lock-in and are a necessary condition for integrating systems from thousands of municipalities and multiple vendors. Proprietary standards can be used only when there is no open or transitory alternative in legacy systems (Brasil, 2018). In practice, however, smaller municipalities often depend on local suppliers that do not adopt open specifications, either because of initial costs perceived as more affordable, or because of lack of knowledge of the free software alternatives made available for free by the Ministry of Health, which shows a mismatch between normative guidance and effective implementation capacity.

The practical implementation of these standards faces challenges. Legacy systems, developed before the consolidation of interoperability standards, need to be adapted or replaced. Smaller municipalities, which rely on systems provided by small, local businesses, struggle when these vendors lack the technical capacity or resources to implement complex standards like FHIR. Data governance needs to balance compliance requirements with providing technical and financial support so that entities with less capacity can adhere to the standards (Belli et al., 2024).

4.1 THE RNDS AND BRAZILIAN INTEROPERABILITY INITIATIVES

The National Health Data Network (RNDS) represents the most ambitious interoperability initiative ever implemented in the Brazilian Unified Health System. Officially launched in 2020, RNDS was conceived as a national platform for the integration of health data that allows the exchange of information between various systems that make up the SUS digital ecosystem (Belli et al., 2024).

RNDS works as an integration layer that connects systems from different spheres of government and various public and private health establishments. Its technical design was based on international standards, especially FHIR, adapted to the Brazilian reality. The platform does not replace existing on-premises systems. It allows them to share information in a structured way. A municipal electronic medical record can send to the RNDS information about care performed, tests requested, medications prescribed and laboratory test results. This information is available, respecting access and privacy controls, to other points in the network that will serve the same patient.

The implementation of the RNDS was made possible by the legal framework of governance built in previous years. Decree No. 10,046 of 2019 provided a legal basis for health data to be shared between different agencies and spheres of government for public health purposes (Brasil, 2019). The General Data Protection Law established limits and safeguards for this sharing, requiring that only necessary data be shared, that there be transparency about access, and that security mechanisms be implemented (Brasil, 2018). The Supreme Court's decision on the constitutionality of data sharing, by establishing principles such as minimization and transparency, guided the technical design of the RNDS to incorporate granular access controls and audit trails (Brasil, 2022).

ConecteSUS, an application that allows citizens to access their own health data registered in the RNDS, materializes the principle of transparency and the holder's right of access provided for in the LGPD. Citizens can view vaccination history, test results, care and medications dispensed, promoting empowerment and active participation in their own health care.

The e-SUS Primary Care (e-SUS AB) strategy exemplifies how data governance operates at the primary care level. e-SUS AB is a computerized system developed by the Ministry of Health and made available free of charge to municipalities, allowing electronic registration of care following interoperability standards for integration with RNDS. The system allows not only local management but also aggregation of information for national monitoring of indicators. The free availability to municipalities, especially smaller ones that

would not have the resources to develop their own solutions, materializes the principle of interfederative coordination and the reduction of inequalities (Belli et al., 2024).

4.2 COMPARATIVE EXPERIENCES IN HEALTH AND LESSONS FOR THE DIGITAL SUS

The analysis of international experiences in health data integration offers subsidies for understanding the challenges faced by Brazil in the consolidation of the Digital SUS. The UK's experience within the National Health Service (NHS) demonstrates that interoperability in large-scale health systems depends on centralised governance and robust data protection standards. Belli et al. (2024) highlight that the UK has developed Trusted Research Environments (TREs), which have been operating for almost 20 years providing safe space for analysis of sensitive health data. In the Brazilian context, the federative structure of the SUS, which distributes competencies among the Union, states and municipalities, presents an additional challenge to the necessary technical coordination.

In Brazil, the consolidation of the Digital SUS has specificities that differentiate it from other national health systems. The Unified Health System was created by the Federal Constitution of 1988 with the principles of universality, integrality and equity (Brasil, 1988). This constitutional architecture defines that health is everyone's right and the duty of the State, establishing a universal public system that serves more than 200 million Brazilians in mainland Portugal, with regional, economic, and social inequalities.

SUS Digital represents the digital transformation of this complex structure. It is not just about computerizing existing processes, but about building an integrated data architecture capable of connecting thousands of systems distributed across three autonomous spheres of government. The dimension of this challenge can be understood by the numbers: there are 5,569 municipalities (Ibge, 2025), each responsible for the management of primary care, 26 states and the Federal District (DF) responsible for regional coordination and management of specialized services, in addition to the Union that establishes national policies and coordinates structuring systems.

The National Health Data Network (RNDS) is the backbone of SUS Digital. Created in 2020, RNDS does not replace local systems, but works as an integration layer that allows structured exchange of information between different points in the network. Its technical design adopts international standards, especially the FHIR, adapted to Brazilian specificities. A citizen assisted in a municipal basic health unit can have their history of care, exams, medications and vaccination accessible when they need specialized care in another municipality or hospitalization, respecting access controls and privacy. This integration

depends on the adhesion of states and municipalities, resulting in uneven implementation between entities with different technical and financial capacities.

ConecteSUS exemplifies the citizen dimension of SUS Digital. Through this application, citizens access their own health data registered in the RNDS, viewing vaccination history, test results, appointments and medications dispensed. This transparent access materializes the principle of the LGPD that guarantees the holder the right to know what data is processed about him. During the COVID-19 pandemic, ConecteSUS became a tool for presenting proof of vaccination, demonstrating the usefulness of data integration.

The e-SUS Primary Care strategy represents another dimension of the Digital SUS. The system, developed by the Ministry of Health and made available free of charge, allows electronic registration of primary care care following interoperability standards. Small municipalities, which would not have the resources to develop their own systems, can use e-SUS AB, reducing inequalities in access to technology. The system not only supports local management but also allows the aggregation of information for national monitoring of indicators such as vaccination coverage, monitoring of pregnant women, control of chronic diseases and epidemiological surveillance.

Interoperability in SUS Digital faces challenges in the Brazilian context. The diversity of legacy systems, developed over decades by different vendors and without technical coordination, creates fragmentation that makes integration difficult. Smaller municipalities rely on local vendors who don't always have the technical capacity to implement complex standards like FHIR. States with greater technical and financial capacity advance faster in digitalization, while states with fewer resources face difficulties, deepening regional inequalities that the SUS seeks to reduce.

Data governance in SUS Digital needs to balance seemingly contradictory needs. On the one hand, continuity of care requires health professionals to access information about patients treated in other services. On the other hand, the LGPD establishes that sensitive health data requires special protection and that only strictly necessary data should be shared. The design of RNDS sought to operationalize this balance through granular access controls and audit trails that allow traceability of who accessed what data, when, and for what purpose.

The experience analyzed demonstrates that interoperability in health is not limited to the adoption of technological solutions, but depends on the construction of institutional arrangements, with the definition of responsibilities, coordination between different levels of government, and mechanisms for the protection of personal data. In the context of SUS Digital, these elements become more relevant in the face of Brazilian federative complexity

and regional inequalities, reinforcing the centrality of data governance as a condition for the integration of the health system (Belli et al., 2024).

5 SECURITY, PRIVACY, AND LEGAL COMPLIANCE CHALLENGES

Despite the advanced legal framework and recent progress in the digitalization of public services, the implementation of data governance in Brazil faces structural and organizational obstacles that transcend purely technological issues. The phenomenon of digital silos remains one of the barriers, the result of decades of fragmented development of information systems in different agencies and spheres of government.

The damage of this disconnection affects multiple dimensions of public administration. The duplicity of registrations forces citizens to repeatedly provide the same information to different agencies, contrary to the principle of administrative efficiency established by the Federal Constitution (Brasil, 1988). The impossibility of cross-referencing data between different sectors limits the State's ability to identify social vulnerabilities, anticipate crises, and coordinate integrated responses. In the health sector, although advances have been achieved with initiatives such as the National Health Data Network, the historical difficulty of integrating data from different systems is still manifested in operational challenges, especially in smaller municipalities (Belli et al., 2024).

Administrative discontinuity represents another structural challenge. Linked to electoral cycles, especially at the municipal level, this discontinuity is manifested in the constant risk of abandonment of ongoing initiatives, discontinuation of systems and loss of investments already made. Digital transformation projects that require long-term implementation and maturation face the challenge of surviving management changes. Smaller municipalities face challenges due to a shortage of trained teams, poor connectivity infrastructure in rural areas, and limited budgets.

The human and organizational dimension aggravates this scenario of fragmentation and discontinuity. The implementation of data governance depends on empowered and engaged people. The shortage of qualified professionals represents one of the most critical bottlenecks. The complexity of interoperability requires expertise that goes beyond technical competence in information technology, encompassing data standards, ontologies, cybersecurity, and personal data protection. In the healthcare sector, professionals need to master specific standards such as HL7 and FHIR, in addition to the clinical and epidemiological specificities of the data.

The rotation of technical positions, many occupied by political appointment and not by public tender, compromises the sustainability of digital transformation projects. Initiatives that

require accumulated knowledge and operational continuity suffer from the loss of institutional memory with each change in management. The lack of continuous training of public servants aggravates this scenario.

Cultural resistance to change is another organizational challenge. Digital transformation is not just a matter of replacing legacy systems with new technologies, but of redesigning work processes, changing consolidated operational flows, and modifying organizational cultures established over decades. In the healthcare industry, the transition from paper records to integrated digital systems faces resistance ranging from privacy concerns to fears related to changing work routines (Belli et al., 2024).

The implementation of interoperability in the Brazilian public sector faces critical challenges related to cybersecurity and the protection of personal data. Recent literature on cybersecurity has emphasized the need for socio-technical approaches that integrate technological, procedural, and human aspects of security (van den Berg, 2020). Government data, especially those classified as sensitive by the LGPD, such as health data, require special protection (Brasil, 2018). Contemporary perspectives on cybersecurity have shifted the traditional focus on infrastructure and systems to the centrality of people and the human impacts of digital threats (Whyte, 2022).

The challenge of cybersecurity has become pressing in a context where public systems are frequent targets of increasingly sophisticated attacks. Incidents involving ransomware, which can completely paralyze services such as hospitals, transportation networks, or pension systems, demonstrate the vulnerability of public digital infrastructure. Data leaks can expose sensitive information, compromising the privacy of millions of citizens and undermining society's trust in public institutions.

The General Data Protection Law establishes requirements for the processing of personal data in the public sector, determining that this processing has a legitimate public purpose and is indispensable for legal attributions or the provision of public services (Brasil, 2018). The principle of minimization, reinforced by the understanding of the Federal Supreme Court in ADI No. 6,649/DF, establishes that only strictly necessary data should be shared (Brasil, 2022). This requirement creates a technical and operational challenge: how to ensure that interoperable systems allow granular information sharing, where each agency or professional only accesses data relevant to their specific attributions, without indiscriminate access to the entire database? (Carvalho, 2023)

Transparency is another requirement of the LGPD. Data subjects have the right to know who has accessed their information, when, for what purpose, and on what legal basis. Interoperable systems in the public sector therefore need to include mechanisms for auditing

and traceability of access. This requirement, while necessary to protect rights, adds technical complexity to systems and requires investments in log infrastructure, audit trails, and monitoring tools. Balancing the need for data sharing for administrative efficiency with the protection of privacy requires sophisticated technical solutions and governance, especially in sensitive areas such as health, social assistance, and public safety (Brasil, 2022; Belli et al., 2024).

5.1 FEDERATIVE GOVERNANCE

The Brazilian federative structure, with its three spheres of government endowed with constitutional autonomy, presents specific challenges for the implementation of interoperable data governance. Coordinating the Union, states and municipalities in the adoption of interoperability standards throughout the national territory requires institutional mechanisms that respect the autonomy of each federative entity while ensuring the necessary uniformity for data integration. Strengthening interfederative coordination becomes necessary: the Union needs to play an inducing role, providing technical and financial support to states and municipalities, without which digital transformation can deepen, rather than reduce, existing regional inequalities.

The absence of specific and institutionalized governance structures for data in the Brazilian public sector represents a gap (Belli et al., 2024). Establishing Data Governance Offices in each public administration, bringing together data openers, LGPD protection officers, and information security chiefs, could create focal points to coordinate initiatives, mediate conflicts over use and sharing, ensure legal compliance, and promote evidence-based management. In sensitive sectors such as health, these offices should include professionals who understand the technical, clinical and epidemiological specificities of the data.

The creation of national data governance committees for strategic sectors, bringing together representatives from the three spheres of government, specialized professionals, technology experts, and representatives of civil society, could contribute to coordinating efforts, defining and maintaining interoperability standards, guiding investments in digital infrastructure, and ensuring compliance with the LGPD consistently throughout the territory. These committees would need to have independence, plurality, and democraticity, as determined by the STF in the decision on the Central Data Governance Committee, for their deliberations to have legitimacy (Brasil, 2022).

To consolidate the advances already achieved in the digital transformation of the Brazilian public sector and overcome the structural challenges identified, an articulated set

of strategic recommendations is required, in line with the constitutional principle of administrative efficiency (Brasil, 1988). This support should include not only financial resources, but also training, knowledge transfer, and the provision of technological solutions that can be adapted and reused by smaller entities. The institutionalization of Data Governance Offices would establish focal points to coordinate initiatives, mediate conflicts, and ensure legal compliance.

Ensuring the protection of sensitive data requires strengthening the National Data Protection Authority, ensuring its technical and budgetary independence. The ANPD must develop specific regulations for the processing of data in interoperability contexts in the public sector, establishing clear guidelines that balance the need for sharing with the protection of rights. Investing in the standardization of concepts, vocabularies, and ontologies across different sectors is necessary for exchanged data to be truly intelligible and useful, allowing not only technical integration, but the semantic interoperability necessary for evidence-based analysis and decisions.

Investment in training and building a data culture is another central strategic recommendation. It is necessary to train public managers capable of managing information with ethics, strategic vision and understanding of the ethical aspects of data use, through permanent training programs. Data governance must be structured in a plural and democratic way, including representation of civil society, sectoral councils, and citizens in committees and decision-making bodies. This inclusion builds the legitimacy and social trust necessary for the sharing of sensitive data to be accepted by the population.

The establishment of Trusted Research Environments would allow researchers to access aggregated and anonymized government data for studies, policy evaluation, and development of innovative solutions, under ethical and legal oversight. Seeking greater technological autonomy should guide investment decisions in critical digital infrastructure, reducing dependence on external proprietary solutions and fostering the development of safe and sustainable national technologies. The preferential adoption of open standards and free software, as recommended by e-PING and made mandatory in 2014, contributes to this autonomy and to the long-term sustainability of the systems, avoiding technological lock-in and facilitating interoperability (Brasil, 2014).

The implementation of new sharing initiatives must include data protection impact assessment mechanisms, as required by the LGPD. The Data Privacy and Ethics Impact Assessment (AIPED) is a central tool to operationalize this requirement, allowing the identification and mitigation of risks before the implementation of new treatments (Belli, 2020). Conducting these assessments preemptively ensures that benefits for administrative

efficiency outweigh privacy risks, allowing for adjustments that prevent rights violations (Belli et al., 2024).

Thus, data governance enables interoperability in SUS Digital through the structuring of technical standards, legal framework, and interfederative coordination, but faces structural challenges related to the fragmentation of systems, scarcity of qualified human resources, and complexity of federative coordination in the context of deep regional inequalities.

6 CONCLUSION

Data governance is a structuring element to enable interoperability in SUS Digital. The analysis carried out demonstrates that the digital transformation of the Brazilian health system is not limited to the adoption of technologies, but requires articulation between technical, normative, and organizational dimensions.

Interoperability in SUS Digital is made possible by data governance through three pillars. The first is the structuring of technical standards, represented by e-PING and the adoption of international standards such as HL7 FHIR, which guarantee communication capacity between heterogeneous systems. The second is the legal framework, consolidated by the LGPD, Decree No. 10,046/2019, and the decisions of the Federal Supreme Court, which establishes limits and safeguards for the sharing of sensitive data. The third is interfederative coordination, materialized in initiatives such as RNDS and e-SUS AB, which seek to integrate systems distributed across three spheres of government and 5,569 municipalities (Ibge, 2025).

The implementation of this governance faces structural challenges. Digital silos, the result of decades of fragmented development, prevent the citizen's single vision. Administrative discontinuity, linked to electoral cycles, compromises the sustainability of long-term projects. The shortage of qualified professionals represents a bottleneck, as interoperability requires specialized knowledge in data standards, cybersecurity, and personal data protection. Cultural resistance to change makes it difficult to transition from entrenched processes to new digital flows.

The challenges of cybersecurity and personal data protection add complexity. Public systems face sophisticated attacks that can bring services to a standstill. The LGPD establishes principles such as minimization and transparency that need to be operationalized in interoperable systems, ensuring that only necessary data is shared and that audit trails allow access traceability.

The Brazilian federative structure presents specific challenges. Coordinating the Union, states and municipalities in a context of regional inequalities requires the Union to

play an inducing role, providing technical and financial support so that entities with less capacity can adhere to interoperability standards.

The consolidation of the Digital SUS depends on articulated measures. Strengthening the ANPD, establishing Data Governance Offices, creating plural national committees, investing in permanent training, developing Reliable Research Environments, and seeking technological autonomy through open standards are recommendations that emerge from the analysis carried out.

The analysis indicates that public health managers need to face the challenge of data governance and interoperability, considering the specificities of Brazilian federalism and the asymmetries of capacity between entities. At the federal level, it is necessary to establish specific financing mechanisms for health information infrastructure that consider the fixed costs of computerized systems, avoiding penalizing smaller municipalities, as well as strengthening continuing technical training programs for professionals who work with information systems. State managers can prioritize the regional coordination of systems, technically supporting municipalities with lower capacity and facilitating integration with the National Health Data Network.

At the municipal level, especially in small and medium-sized municipalities, the priority adoption of systems made available free of charge by the Ministry of Health, such as e-SUS AB, which meet interoperability standards, is a viable alternative, combined with investment in training of civil servants for appropriate use. The creation of permanent instances of data governance in the three spheres, with the participation of managers, health professionals and user representatives, would allow technical decisions on information systems to consider care needs and respect the principles of social control that characterize the SUS.

Data governance enables interoperability in SUS Digital through the structuring of technical standards, legal framework, and interfederative coordination, but faces structural challenges related to system fragmentation, shortage of qualified human resources, and complexity of federative coordination in the context of regional inequalities. Overcoming these challenges requires long-term institutional commitment, sustained investments, and building technical and organizational capacities at all levels of government.

REFERENCES

Belli, L. (2020). Como implementar a LGPD por meio da avaliação de impacto sobre privacidade e ética de dados (AIPED). In L. S. Mendes, D. Doneda, I. W. Sarlet, & O. L. Rodrigues Junior (Coords.), Tratado de proteção de dados pessoais (pp. 393–422). Forense.

Belli, L., et al. (2024). Governança de dados no setor público: Abertura de dados governamentais, proteção de dados pessoais e segurança da informação para uma transformação digital sustentável. Lumen Juris.

Belli, L., & Guglielmi, G. J. (2022). L'État digital: Numérisation de l'administration publique et administration publique du numérique. Berger-Levrault.

Brasil. (1988). Constituição da República Federativa do Brasil. Presidência da República.

Brasil. (2019, 9 de outubro). Decreto nº 10.046: Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Diário Oficial da União.

Brasil. (2022, 10 de fevereiro). Emenda Constitucional nº 115: Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Diário Oficial da União.

Brasil. (2014, 23 de abril). Lei nº 12.965: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União.

Brasil. (2018, 14 de agosto). Lei nº 13.709: Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União.

Brasil. (2019, 8 de julho). Lei nº 13.853: Altera a Lei nº 13.709/2018 para dispor sobre a Autoridade Nacional de Proteção de Dados. Diário Oficial da União.

Brasil. (1990, 19 de setembro). Lei nº 8.080: Dispõe sobre as condições para a promoção, proteção e recuperação da saúde e a organização dos serviços correspondentes. https://www.planalto.gov.br/ccivil_03/leis/l8080.htm

Brasil. (1990, 28 de dezembro). Lei nº 8.142: Dispõe sobre a participação da comunidade na gestão do Sistema Único de Saúde (SUS). https://www.planalto.gov.br/ccivil_03/leis/l8142.htm

Brasil. (2018). Padrões de interoperabilidade de governo eletrônico (e-PING). Ministério do Planejamento, Desenvolvimento e Gestão.

Brasil. (2014, 24 de dezembro). Portaria nº 92: Institui a arquitetura e-PING (Padrões de Interoperabilidade de Governo Eletrônico). Diário Oficial da União.

Brasil. Supremo Tribunal Federal. (2026). Ação Direta de Inconstitucionalidade n. 6.649/DF (Incidente 6079238). https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238

Carvalho, L. B. (2023). O poder público e a proteção de dados pessoais no Brasil: Novos desafios, velhas práticas administrativas. Revista de Direito Administrativo, 282(2), 133–162.

Haddad, A. E., & Lima, N. T. (2024). Saúde digital no Sistema Único de Saúde (SUS). Interface (Botucatu), 28, e230597. https://doi.org/10.1590/interface.230597

IBGE – Instituto Brasileiro de Geografia e Estatística. (2025, 26 de agosto). Um país com quase seis mil municípios. https://educa.ibge.gov.br/jovens/materias-especiais/22754-um-pais-com-quase-seis-mil-municipios.html

IEPS – Instituto de Estudos para Políticas de Saúde. (2022). Desafios da estratégia de saúde digital para o Brasil 2020–2028. Veredas. https://www.veredas.org/wordpveredas/wp-content/uploads/2023/07/IEPS_desafiosESD28.pdf

Organização Mundial da Saúde. (2020). Global strategy on digital health 2020–2025. https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf

Saldanha, R. F., Pedroso, M. M., & Magalhães, M. (2023). Acesso aos dados agregados e microdados do SUS. In Avaliação de impacto nas políticas de saúde (pp. 418–434). Ministério da Saúde. https://bvsms.saude.gov.br/bvs/publicacoes/avaliacao_impacto_politicas_saude_guia_sus.pdf

Schultes, E., & Wittenburg, P. (2019). FAIR principles and digital objects: Accelerating convergence on a data infrastructure. In Y. Manolopoulos & S. Stupnikov (Eds.), Data analytics and management in data intensive domains (Vol. 1003). Springer.

Van den Berg, J. (2020). A basic set of mental models for understanding and dealing with the cyber-security challenges of today. Journal of Information Warfare, 19(1), 26–47.

Whyte, C. (2022). The human turn in cybersecurity: Towards a politics of truth and subject. European Journal of International Security, 7(3), 343–362.

Zeleti, F. A., Ojo, A., & Curry, E. (2016). Exploring the economic value of open government data. Government Information Quarterly, 33(3), 535–551.