Service-oriented interoperability: governance mechanisms for the hospital-administration connection in the era of digitalization

Doina – Monica AGHEORGHIESEI,
Alexandru Ioan Cuza University of Iasi
Iasi, Romania
agheorghiesei.doina@feaa.uaic.ro

Ana-Maria BERCU,
Alexandru Ioan Cuza University of Iasi
Iasi, Romania
bercu@uaic.ro

Abstract
The digital transformation of public administration and the healthcare system redefines the way institutions collaborate and share data in order to provide efficient and secure public services. In this context, interoperability becomes a strategic infrastructure of integrated digital governance, enabling inter-institutional coordination based on trust, shared responsibility and transparency. The article proposes a conceptual and methodological framework for understanding the governance mechanisms of interoperability between hospitals and public administration, with the aim of strengthening a service-oriented digital architecture. The study aims to analyze existing models and mechanisms of interoperability governance between public institutions and the health system through national and European case studies, while adapting a conceptual and operational governance framework based on co-governance, shared responsibility, and data ethics to support the implementation of integrated digital governance in the public sector. Methodologically, the research uses a comparative analysis of best practices at the national and European level, including: Romania, through the National Strategy on the Governmental Cloud and the integration of health systems with CNAS, Estonia, through the X-Road model, which ensures the interoperability and governance of digital transactions in health, and the European network MyHealth@EU, as an example of transnational co-governance of medical data exchange. The results highlight that service-oriented interoperability is not just a technological solution, but a process of collaborative governance, which strengthens trust between institutions, optimizes information flows and supports the sustainability of digital governance in public health. The conclusions offer development directions for strengthening the normative, ethical and operational framework of interoperability in the European public administration.

Keywords: digital governance, institutional co-governance, inter-ministerial SLAs.

1. Introduction
1.1 Context of digital governance in public administration and health
The digital transformation of public administration and health systems is no longer just a technical concern, but a complex process of rethinking the way public policies and services are designed, delivered and regulated. Modern models of digital governance start from the premise that digital infrastructures and data should be treated as strategic public goods, managed through principles of transparency, accountability, interoperability and protection of citizen rights [1, 2].

In the healthcare sector, digitalization (including electronic patient records, telemedicine, and data analytics platforms) promise to increase the quality of care, operational

efficiency, and decision-making support for public policies; at the same time, they raise issues of institutional coordination, security and equity in access [2, 3].

Digital governance should be understood as a set of mechanisms, normative, institutional, technical and organizational, that facilitate the transition from information silos to interoperable service ecosystems. This includes: national and international strategic frameworks, clear responsibilities between administrative levels and healthcare providers, participation and ethics mechanisms for data reuse, and audit and compliance tools for the security and protection of personal data [2, 3].

1.2 Interoperability as a strategic infrastructure of modern public services

Interoperability, defined as the ability of systems and organizations to exchange and reuse information in a coherent, secure and meaningful way for the provision of services, is becoming a strategic infrastructure as important as the transport network or energy. In the healthcare sector, interoperability enables continuity of care (e.g., transfer of clinical information between hospitals and primary care practices), supports the response to public health emergencies, and facilitates data-driven research [4, 5].

Recent European efforts (the proposal for the European Health Data Space and supporting documents) emphasize that interoperability is both a technical challenge (standardization, formats, modern APIs such as FHIR) and a governance one: it requires legal frameworks for data access and reuse, mechanisms for certifying actors, and institutional structures to arbitrate conflicts between the public interest and the right to privacy [5, 6]. The literature also shows that technical standards are a necessary but not sufficient condition — success depends on organizational changes, digital skills of staff, and financial models that support long-term interoperability [3, 4].

1.3 The issue of inter-institutional governance in the digital age

Inter-institutional governance involves the harmonization of roles, responsibilities and information flows between entities that have partially overlapping objectives: hospitals (clinical service providers), public health authorities, local and central administrations, technology providers and, last but not least, citizens/patients. In practice, this harmonization encounters several persistent bottlenecks.

IT investments have often been made at the unit level (hospital or local network) without integrated system-wide strategies, which has generated technical and procedural incompatibilities. The lack of clear co-financing mechanisms and incentives for integration hinders the consolidation of common infrastructures [2].

Data protection requirements, consent for reuse, and security standards vary across jurisdictions and data types (primary clinical data vs. research data), complicating cross-institutional exchange. European initiatives, regarding normative and ethical divergences, emphasize specific regulations (e.g. EHDS) that create a “regulated space” for data exchange, but operational implementation remains a complex endeavor [5, 6].

Differences in IT skills, specialized human resources, and data management practices between hospitals and local governments make interoperability a difficult goal. Romania and other member states present wide variability in the digital maturity of healthcare institutions, uneven institutional capacities, which requires differentiated support policies and mechanisms for the transfer of good practices [1]

To ensure that interoperability produces real public value (not just technical connectivity), governance must be service-centric: clear definition of target public services (e.g. clinical continuity, community prevention, health crisis management), service level agreements (SLAs) between technical and operational providers, and performance indicators that include health outcomes, efficiency, and user satisfaction [2, 3].

In summary, the challenge of inter-institutional governance is not only technological, but is primarily a matter of orchestration: establishing rules, accountability mechanisms, and operational tools that allow diverse actors to cooperate for the continuous and secure delivery of citizen-oriented services. The pragmatic approach recommended by recent literature combines a national/regional strategic framework with pilot projects focused on critical areas (e.g. clinical data transfer between hospitals and public health authorities), mixed financial models, and a strong focus on standardization, ethics, and inclusion [3, 4, 5].

2. Concept

2.1 The notion of integrated digital governance and the role of hybrid architectures

Integrated digital governance represents a coherent framework of principles, rules, processes and institutions intended to coordinate the design, implementation and oversight of digital public services at the system level. This transcends the simple adoption of technologies: it involves aligning political strategies (national/regional strategy), administrative capacities (processes, skills, resources) and technical architecture (platforms, APIs, standards) so that public services are accessible, secure and result-oriented. In essence, integrated digital governance treats digital infrastructures and data as strategic public goods that require common planning, financing and accountability mechanisms [7].

In the context of health, integrated governance takes on an additional dimension: the interdependence between clinical service providers (hospitals, laboratories, family practices), service regulatory and payment authorities (national insurance agencies) and entities providing the technical infrastructure (platform operators, EHR solution providers). This complexity requires the adoption of hybrid architectures — deliberate combinations of centralized components (e.g., national registries, interoperability frameworks, authentication/identity services) and distributed components (local servers in hospitals, regional applications, microservices) — that allow for both scalability and respect for institutional autonomy and local requirements. Hybrid architectures offer flexibility in adopting standards (e.g. FHIR for clinical resource exchange) and allow for service orientation according to use cases (incremental transition between silos and interoperable ecosystems) [8, 9].

From a governance perspective, hybrid architectures require a specific set of coordination mechanisms: mandatory interoperability specifications at national/regional level, framework contracts and funding models covering common elements (e.g. integration bus, semantic interoperability), certification and audit mechanisms for central and local components, and dispute resolution procedures. Without these mechanisms, hybrid architectures risk reproducing technical fragmentation in a "more sophisticated" form (poor integration, ad-hoc mappings, high maintenance costs) [8, 9].

2.2 Data governance models and shared responsibility between institutions

Data governance in the public health domain is multidimensional: it includes data ownership, responsibility for quality and integrity, access authorization, semantic interoperability, and policy on reuse (research/planning/monitoring). Data governance models can be classified, simplified, into three theoretical types that coexist in practice:

1. Centralized model - a national (or regional) body holds key roles in storing, standardizing and controlling access to essential data sets. This model favors harmonization and economies of scale, but may raise concerns about excessive control and the risk of failure [5].

2. Hybrid model - data remains at the level of institutions (hospitals, clinics), but access, cataloguing and aggregation services are coordinated through standards, APIs and governance bodies that regulate access procedures. This model balances local autonomy with interoperability, but requires robust accreditation mechanisms and security controls [8, 9].

3. Decentralized data market model - access to data is achieved through markets or service portfolios where requests are assessed by automated mechanisms plus ethical review — a model that is increasingly being discussed in the context of “secondary use” of data for research and innovation (e.g. under the EHDS proposal). Its implementation requires very strict guarantees regarding pseudonymization, auditing and access control [5].

Regardless of the model, responsibility for data governance must be shared, clearly defined and contractualized: institutions producing clinical data have primary responsibility for their accuracy and maintenance; public health authorities/national agencies have responsibilities for aggregation, analysis and reporting; entities providing technical infrastructure have obligations regarding security, availability and interoperability. Shared responsibility models must be supported by explicit rules regarding the demarcation line between operational responsibilities (e.g. data retention and integrity) and decisional/ethical ones (e.g. authorizing reuse for research). Recent literature emphasizes operational tools, service level agreements (SLAs), metadata registries, retention policies, and audit procedures, as essential elements for the functioning of these models [10].

A retention policy is a set of rules created by an organization to determine how long certain data is stored. These policies apply to different types of information, from digital data to physical (paper) records. The main goal is to store data only for the period necessary for

the purposes for which they were collected, thus ensuring compliance with regulations such as GDPR.

Another critical aspect is that of legal accountability and transparency towards the citizen. National and European regulations (including the GDPR regime and specific EHDS initiatives) impose strict standards for consent, the right to portability and objection mechanisms; Concrete implementation at the hospital-administration level requires operational procedures that transform legal provisions into verifiable workflows [5].

2.3 Interoperability as a trust mechanism between hospital and administration

Operational interoperability (technical, semantic and organizational) plays a central role in establishing and maintaining mutual trust between hospitals and administration. In practical terms, trust is manifested by the ability of actors to share relevant clinical information, in a timely manner and with adequate guarantees regarding data confidentiality and integrity, so that administrative decisions (planning, financing or public health) are based on reliable data. Lack of interoperability generates friction: inconsistent data, reporting delays, coding errors, and ultimately, loss of mutual trust and public confidence [10].

Mechanisms through which interoperability builds trust include:

- Standardization and certification: the use of common technical and clinical standards (e.g. FHIR, SNOMED CT) and certification processes for IT solutions, which reduce uncertainty about the meaning and quality of the data exchanged [6].
  - FHIR (Fast Health Interoperability Resources) [11].
  - The main purpose of SNOMED CT is to encode the meanings used in medical information and to support efficient clinical data recording, with the aim of improving patient care. SNOMED CT provides the general basic terminology for electronic health records. SNOMED CT ensures consistent information exchange and is fundamental to an interoperable electronic health record [12] .
- Clear contracting and SLAs: institutional agreements that define responsibilities, response times, minimum data quality levels and remediation procedures. These tools translate technical interoperability into verifiable administrative obligations [13].
- Transparency and audit: access registers and independent audit mechanisms for all data flows involving public authorities, elements that increase accountability and citizen confidence [10].

In the Romanian context, where the healthcare system still remains very hospital-centric and characterized by regional differences in IT capacity, interoperability can function both as a driver of efficiency (e.g., reducing duplication, improving continuity of care) and as a tool for strengthening institutional relationships: sharing valid data allows authorities to allocate resources based on up-to-date information, and hospitals to receive prompt operational and financial feedback. However, in the short term, this relationship of trust requires clear policy interventions —joint investments, binding national standards, and support mechanisms for low-capacity units [14].

From a conceptual perspective, integrated digital governance, data governance models and interoperability are not separate concepts, but interdependent parts of the same socio-technical system. Hybrid architectures allow for balancing local autonomy with the need for a common data exchange space; data governance models delineate responsibilities and control mechanisms; and functional interoperability builds operational trust between hospitals and authorities. For practitioners, the implications are direct: interoperability projects must be designed concurrently with governance tools (rules, contracts, coordination bodies) and with plans to compensate for capacity inequalities (technical assistance, conditional funding, regional microservice centers) [8, 9].

3. Methodology — comparative analysis of good practices and institutional modeling

3.1 Methodological objective and research design

Analyzing existing models and mechanisms of governance of interoperability between public institutions and the healthcare system, through national and European case studies (Romania, Estonia, MyHealth@EU), in order to identify good practices applicable to the Romanian context.

The objective of the article is to analyze existing models and mechanisms of governance of interoperability between public institutions and the healthcare system, through national and European case studies (Romania, Estonia, MyHealth@EU), in order to identify good practices applicable to the Romanian context.

The method is a comparative documentary analysis of official reports, national strategies, European guidelines and academic studies (TEHDAS, EHDS analyses, OECD, WHO, national strategies, the sources being selected for relevance (public policies, government reports, technical analyses), timeliness (2020–2025) and open-access accessibility [8, 9].

The comparative analysis methodology included: extracting key governance elements (actors, roles, decision-making and financing mechanisms), operational procedures (SLA, accreditation/recertification processes), and performance indicators used in the analyzed practice.

3.2 Criteria for selecting good practices

The criteria used for including an example as a “good practice” were:

- Scalability and replicability: solutions implemented at national or regional level that can be adapted to contexts with institutional heterogeneity (e.g. Estonia, Denmark) [15].
- Service-oriented interoperability: initiatives that prioritize operational flows (clinical continuity, public health reporting) rather than abstract technical connectivity [8, 9].
- Demonstrated governance and accountability mechanisms: existence of coordination bodies, SLAs or certification processes for IT solutions [2].
- Transparency and legal data protection: GDPR-compliant solutions and EHDS proposals for secondary data reuse [6].

- Information accessibility: open documentation, public reports and technical material available for download [16].

3.3 Methodological limitations

The analysis is based on official documents and publicly available reports (2020–2025) and their translation into operational solutions for Romania. Limitations include: (1) contextual differences between countries (size, regime financial), (2) ongoing legislative developments (EHDS) that may modify the requirements, and (3) lack of primary data from detailed Romanian operational implementations in open access. I recommend implementing pilot projects to validate the hypotheses [6].

3.4 Comparative analysis — selection of good practices (synthesis)

We compared 3 exemplary models frequently cited in the European literature as relevant for service-oriented interoperability: Estonia (national integrated model), Denmark (standards catalogue and controlled distribution architecture) and the conceptual offers for the European Health Data Space (EHDS / TEHDAS). The comparative summary highlights the replicable elements for Romania.

1. Estonia — integrated national registry and digital trust

Features: interoperable national EHR registry, electronic identity infrastructure, consent-based control and access logging; implemented clinical standards; central infrastructure with nodes at providers. Estonia offers a centralized infrastructure model with distributed access components, facilitating rapid access by authorities (in authorized situations) to aggregated clinical data for public health and planning [17, 18].

2. Estonia — The X-Road Model for Digital Transaction Governance in Health

X-Road (X-tee) is an open-source secure data exchange platform that provides connectivity and interoperability between public and private systems. The X-Road architecture functions as a transaction assurance layer: each participant (institution) keeps data in its own system, but uses secure gateways for requests and responses; communications are encrypted and audited, and access is controlled according to national policies. X-Road was the central element in the construction of e-Estonia and is used in many areas, including e-Health [19, 20].

For the healthcare sector, X-Road offers governance benefits that are worth analyzing as best practices:

- Decentralization with centralized rules: Data remains at the level of the holders (hospitals, providers), but the exchange follows uniformly applied rules, certificates and policies (entity certificates, authentication/authorization functions), which ensures local autonomy combined with operational interoperability [15].
- Access control and auditability: every transaction is logged; in healthcare this means transparency regarding who accessed what information and for what purpose, an essential element for trust between hospitals and administration [17, 18].

- Certification ecosystem and institutional support: the Estonian model includes institutions that certify X-Road nodes and provide support for onboarding, testing and monitoring. This reduces the barriers to entry for small organizations [19, 20].
- Estonia's experience shows that an X-Road infrastructure accelerates cross-institutional services (e.g. rapid release of public health information, cross-sectoral access to administrative data), contributing to data-driven decisions and streamlining reimbursement/monitoring processes. For countries with fragmented hospital networks, the lesson is clear: a secure and standardized exchange network reduces integration costs and increases institutional trust. However, implementation requires investments in digital certificates, data standards (clinical terminologies) and audit procedures [19, 20].

3. Denmark — catalogue of standards and strategy for digital health services
Characteristics: clear national digital health strategy (national catalogue of standards, mandatory requirements for providers), focus on semantic interoperability and technical SLAs; emphasis on regional hubs and shared services (microservices) that can be used by hospitals. The model emphasizes central coordination of standards + local operational autonomy [21].

4. TEHDAS / EHDS — European model for reuse and governance
Features: proposals for roles of Health Data Access Bodies (HDABs), federated options for services and access mechanisms for secondary uses; recommends a mix of central components (catalogue, policies) and data federation at the holder level. Supports hybrid models and coordinating institutions at national/regional level [8, 9].

Key lessons for modeling highlight that hybrid models, which combine central governance components with distributed regional services, provide an effective balance between standardization and local autonomy; that technical and semantic standards, together with certification mechanisms, are essential for increasing trust and ensuring operational interoperability; and that institutional roles — such as data access bodies, metadata registries, and the national interoperability office — must be clearly defined both contractually and legally [8, 9, 16].

4. Romania — EU: governance mechanisms in the MyHealth@EU network (eHDSI / eHDSI services)

4.1. Romania — National Strategy on Government Cloud and integration with CNAS

Romania introduced a legal and programmatic framework for “cloud-first” in administration through Emergency Ordinance no. 89/2022 on the establishment, management and development of cloud computing infrastructures and services used by public authorities and institutions, followed by strategic documents and operational plans detailing the architecture of the Government Cloud (Government Cloud Platform). The stated goal is to consolidate digital public infrastructures, reduce fragmentation, increase resilience and ensure conditions for interoperable services on a national scale. This framework provides a legal basis for hosting critical public health components (registries, catalogs, sandboxes) and for integrating CNAS (Health Insurance Informatics Platform — PIAS) services into the government cloud ecosystem. CNAS manages PIAS, the

integrated health insurance information system that includes the key components: the insured person registry, electronic prescription, electronic health record and settlement reports (PIAS). Implementing a government cloud architecture offers practical opportunities: consolidating databases (elasticity, backup and disaster recovery), facilitating standardized API interfaces for exchange with hospitals and authorities (REST/FHIR services), and the possibility of operating sandboxes for interoperable testing. The PNRR documents and the financing guidelines for the modernization of PIAS explicitly mention the need to standardize and optimize the platform to enable interoperability of clinical and administrative services [22, 23].

Good practices derived from the Romanian approach include: (1) consolidating the physical architecture in a controlled government cloud (reducing the risk of silos), (2) clearly defining legal responsibilities (data owner — hospitals/CNAS, cloud operator — public/contracted entity), (3) designing APIs and semantic profiles (e.g. FHIR) as mandatory requirements for any solution integrated into the ecosystem, and (4) including mixed financing mechanisms (European funds for CAPEX, operational subscriptions for OPEX).

Relevant risks are: dependency on suppliers, security vulnerabilities at scale, and the possibility that excessive centralization reduces local innovation capacity; therefore the recommended model is hybrid (centralized components + regional/local nodes) to maintain the balance between control and operational autonomy [23].

4.2 Institutional governance mechanisms

"MyHealth@EU" is the branded name for cross-border electronic healthcare services provided through the European Commission's eHealth Digital Service Infrastructure (eHDSI). Initial services include ePrescription and Patient Summary exchange, and expansion plans include lab results, imaging, and discharge reports. Implementation is based on a set of technical specifications, conformance testing processes and national registration mechanisms (mapping, adaptation to standards), coordinated by the eHealth Network and national agencies [24, 25].

Participation in MyHealth@EU requires Member States to have the following governance mechanisms, which constitute good practices for the hospital-administration link: National connection authority/technical contact point: each state designates entities responsible for the national connection to eHDSI (national nodes) and for managing the necessary semantic mappings. This ensures clear responsibilities between ministries, national agencies (e.g. CNAS/Ministry of Health in Romania) and service providers [25].

Testing and validation processes (conformance & interoperability testing): interoperability requirements include sandbox testing and technical compliance requirements prior to implementation, reducing the risk of malfunctions at deployment [26].

Legal mechanisms and cross-border liability agreements: to enable exchange, policies on liability for errors, incident notification and data protection (GDPR + EU specifications)

need to be agreed. These agreements build trust between hospitals and administrations of different countries [27].

4.3 Lessons for Romania and hospital–administration networks

Romania's involvement (through CNAS/Ministry of Health) in MyHealth@EU offers concrete governance lessons applicable at national level: Clarification of national roles: designation of a national coordination point (technical and political) to manage onboarding and conformance testing; this practice ensures that hospitals are integrated systematically, not ad-hoc [27].

Adopt common profiles (FHIR, CDA, ePrescription/eDispensation profiles) for semantic interoperability, together with local certification processes reflecting eHDSI requirements. Using regional networks (CRIs / regional nodes) to reduce hospital-level complexity and provide centralized technical support for compliance. This replicates lessons from Denmark/Estonia and is compatible with MyHealth@EU requirements [15, 26].

The comparative analysis (Romania cloud + CNAS, Estonia X-Road, MyHealth@EU) reveals the following common and transferable elements:

1. Hybrid architecture (central components + regional nodes/locations): balances central control with local autonomy (lesson from Romania & Estonia) [23].
2. Technical standardization, sandboxing and mandatory testing: FHIR/CDA profiles, semantic mapping and pre-production testing (MyHealth@EU requirement) [26].
3. Clear accountability and certification model: accreditation procedures for nodes/services and SLA contracts between hospitals, CRIs and central authorities (recommended practice in all examples) [19, 20].
4. Transparency and auditing: mandatory logging of accesses and aggregated public reports to maintain citizen trust [17, 18].

As key practical recommendations for the hospital-administration link, materialized, we find in the studied literature:

1. Adopting a hybrid model: hosting central services (catalogs, sandboxes, metadata registries) on the Government Cloud Platform, maintaining regional nodes (CRI) for integration with hospitals [23].
2. Implementing mandatory certification procedures for any solution that exchanges data with CNAS or with national nodes (compliance testing, security audit) [26].
3. Convert interfaces to common profiles (FHIR/CDA) and publish a catalogue of national profiles adapted to the requirements of MyHealth@EU [26].
4. Establish a national coordination office (ONIS-like) to manage policies, certification and representation in EU networks (equivalent to ONIS/point of contact for eHDSI) [25].
5. Mixed financing plan: clear CAPEX requirement from PNRR/EU for infrastructure + OPEX model based on differentiated subscriptions and cross-subsidy schemes for vulnerable hospitals [28].

The analyzed good practices show that efficient interoperability between hospitals and administration relies on hybrid architectures that combine the government cloud with regional nodes, robust certification and audit mechanisms (inspired by X-Road and

MyHealth@EU), and institutional clarity (national connection points and responsibility roles). For Romania, the operationalization of these good practices involves adapting legislation, investing in the Cloud Platform and PIAS, defining certification and onboarding procedures, and active participation in the cross-border interoperability mechanisms offered through MyHealth@EU. Coherent implementation will increase both administrative efficiency and citizens' trust in digital health services [23].

5. Governance mechanisms for hospital-administration interoperability

Hospital-administration interoperability requires an explicit governance framework that allocates roles, establishes responsibilities, provides for operational contracts (SLAs), and secures data use through ethics, confidentiality, and auditability policies. The following proposals combine general principles (OECD; EIF) with European and Romanian experiences (EHDS/TEHDAS, X-Road, Cloud Platform/OUG 89/2022 and PIAS/CNAS) to provide a coherent set of mechanisms applicable in the Romanian context [29].

5.1. Roles, responsibilities and decision-making levels

An effective governance framework clearly differentiates at least four fundamental institutional roles: the strategic/regulatory actor (Ministry of Health / ONIS at national level), the platform/infrastructure operator (Government Cloud Platform / CRI), the operational data holders (hospitals/clinical units) and the access/authorization entities for reuse (Health Data Access Body at national/regional level according to EHDS). This separation reflects the TEHDAS recommendations and the EHDS framework, which prescribe distinct roles for access management, certification and oversight [9].

The decision-making levels (strategic–operational–technical) include the strategic (political) level, where national objectives are defined, budgets are allocated and governance standards and policies are approved, the entities involved being the Ministry of Health, the Ministry of Digitalization/Ministry of Research, Innovation and Digitalization and the Ministry of Finance, mainly involved in co-financing mechanisms and budgetary control, and the strategic decisions cover the accession to the EHDS, the allocation of PNRR/EU funds and the "cloud-first" policies; the institutional/operational level, where interoperable services are implemented and monitored (PIAS management, regional nodes/CRI), SLAs and accreditation processes are administered, the actors involved being CNAS (PIAS), ONIS (or a national equivalent), CRI and hospital units; and the technical level, which involves daily operation, performance monitoring, cybersecurity and compliance testing (sandbox), being managed by certified IT providers, hospital IT teams and cloud operators, where technical mechanisms such as certification, logging and sandbox testing are essential for the practical implementation of policies [19, 20, 23, 30, 31, 32].

The responsibilities proposed within the governance scheme are distributed among several institutions and main actors. The Ministry of Health, through ONIS, has the role of strategic coordination, approving clinical and procedural standards, applying sanctions in case of non-compliance and representing Romania at the European Union level in the field of e-health. The Ministry of Digitalization manages the Government Cloud Platform, according to the framework established by GEO no. 89/2022, and deals with the technical

policies of the public infrastructure, including aspects related to hosting, resilience and continuity. The Ministry of Finance has responsibilities regarding the allocation, supervision and approval of financial instruments, ensuring co-financing and balance between funding sources. The National Health Insurance House, through the PIAS operator, maintains the functionality of the insurance platform and manages administrative-financial interoperability with medical units. Regional interoperability centers provide shared microservices, testing spaces, support for system integration and semantic translations, and are responsible for operational monitoring at the local level. Hospitals and other clinical providers own and manage medical data, ensure its quality, and comply with service level agreements established through contracts [33].

5. 2. Recommended KPIs for hospital–administration governance

The set of key performance indicators (KPIs) constitutes an essential strategic tool for assessing the efficiency, data quality and public value generated by the interoperable health system. Indicators must be clearly defined, measured periodically and reported at an aggregate level to strengthen institutional accountability, transparency and citizen trust. According to European practices and recommendations from the OECD (2021) and the European Parliament Research Service (2022), four categories of KPIs are mentioned [2, 6].

The first category targets the technical and operational performance of the digital infrastructure, including KPIs such as interoperable service uptime, average API response time, MTTR (Mean Time to Restore) for critical incidents, and the percentage of requests successfully processed (throughput). These are monitored daily or weekly by the Regional Interoperability Centers and Cloud operators, ensuring the functional continuity and reliability of digital services [19, 20, 21].

The second category refers to data quality and semantic compliance, with indicators such as the rate of completeness of mandatory clinical fields, the rate of coding errors (ICD/SNOMED mismatches), and the percentage of records validated through automatic or manual reconciliation. These indicators, tracked monthly or quarterly by hospitals and ONIS, are fundamental for maintaining data accuracy, consistency and integrity, critical aspects for administrative decisions and clinical analyses [34].

Governance and compliance categories include KPIs that monitor security incidents reported and resolved within the GDPR timeframe and the percentage of data reuse requests processed according to the HDAB SLA. Assessing these indicators quarterly or annually supports institutional accountability and ensures compliance with the legal framework in the field of data protection [8].

The last category, on public impact and value, measures the reduction of redundant medical visits, the average time for data-based administrative decisions and the percentage of research access requests approved, reflecting the efficiency of decision-making processes and the transparency of data reuse. Annual monitoring of these KPIs allows the assessment of the tangible benefits of interoperability and contributes to the optimization of public health policies [6].

6. Data governance policies: ethics, confidentiality and auditability

All data governance procedures should be anchored in principles such as respect for patient autonomy, data minimization, transparency of use, and fairness. At the legal level, the framework is determined by the GDPR (data subject rights, data controller/processor responsibilities) and, specifically for health, by the EHDS provisions that introduce Health Data Access Bodies and specific rules for secondary reuse. National policies must reflect these principles and translate legal obligations into clear operational flows (consent, portability, complainants) [25].

Mandatory technical and organizational measures include pseudonymization and anonymization in test environments and for certain reuse requests, along with clear criteria and standards regarding the level of pseudonymization, as well as the use of secure processing environments for secondary reuse, compliant with EHDS, with role-based access control and continuous auditing; It is also necessary to implement robust logging and provenance mechanisms, which provide complete records of accesses (who, when, for what purpose), metadata regarding the line of provenance of the data and independent audit procedures, these registers having a dual role — security and public transparency, including through aggregated reports in addition, incident response and breach notification processes must oblige operators to notify internally and to competent authorities, including ANSPDCP, within the legal deadlines, as well as to communicate to affected persons, in accordance with the GDPR; and for the reuse of data for research or public policy purposes, it is necessary to establish, at national level, a commission to evaluate complex requests from an ethical perspective — social impact, risk of re-identification, equity in access — as TEHDAS recommends including civil society and patient representatives in such structures to ensure democratic legitimacy [9, 19, 35].

7.Conclusions and recommendations

Interoperability is not just a technical element of digital infrastructure, but is the foundation that makes possible the coherent functioning of health services and public administration in the data age. The analysis of the entire material demonstrates that interoperability represents the minimum condition for institutional coordination, administrative efficiency, continuity of medical care and protection of the public interest, being today equivalent to a national critical infrastructure, comparable to transport or energy networks [5].

Interoperability ensures the ability of healthcare and administrative institutions to communicate in real time, reduce errors, eliminate redundancies, and produce informed decisions. European models — Estonia, Denmark and MyHealth@EU — show that interoperability not only streamlines processes, but also creates a climate of trust between institutions, an essential element for good governance. At the same time, interoperability is directly linked to ethical values such as fairness, transparency and respect for patient autonomy, as coherent digital structures reduce the risk of data abuse and facilitate citizen control over their own information [5, 8, 19, 20].

Interoperability has immediate applicability in all key processes of the healthcare and administrative system, as it facilitates continuity of care through the fluent transfer of

clinical data between hospitals, practices and public health authorities, supports financial efficiency through rapid and standardized settlement processes between CNAS and hospitals, enables informed public policy planning through access to quality data for epidemiological analyses and prioritization of investments, supports research and ethical data reuse through secure processing areas, pseudonymization and clear access mechanisms, and strengthens risk management and cybersecurity through complete auditability and prompt notification of incidents; this applicability is amplified by European frameworks, as MyHealth@EU demonstrates that interoperability can work coherently and across borders, confirming the maturity and relevance of hybrid models [3, 19, 22, 25, 35].

For Romania, interoperability is not only useful, but absolutely necessary. The fragmentation of IT infrastructures, the large differences in digital maturity between hospitals and the difficulties of coordination between central institutions make administrative modernization impossible in the absence of a mandatory interoperability framework. The "cloud-first" policy and the modernization of PIAS offer a real opportunity to consolidate a coherent digital ecosystem, but success depends on the implementation of hybrid architectures, technical standardization (FHIR/CDA) and a strong certification and audit system [23, 26].

From an ethical perspective, interoperability is the mechanism by which the state demonstrates that it can manage sensitive data in a responsible, transparent and public interest-oriented manner. It thus becomes an expression of administrative well-being: if a state cannot integrate its own data, it can neither protect its citizens nor design effective public policies.

The implementation of the proposed strategic recommendations would have significant effects on the coordination and efficiency of digital health systems. Establishing a strong national body for interoperability, expanding the role of ONIS, would ensure a unified framework for system certification, defining semantic profiles and representing Romania in international forums. This would allow accelerating the adoption of compatible solutions, reducing fragmentation of the medical IT market and increasing access to European funds and good practices. Also, adopting a hybrid architectural model, combining centralized cloud infrastructure with regional nodes, would provide the optimal balance between centralized control and local autonomy, ensuring better application performance and flexibility in implementing solutions adapted to the local context. The introduction of unified SLA procedures for hospital-administration flows would clarify expectations regarding the level of services, standardize their quality and reduce bottlenecks caused by the lack of clear standards.

On a technical and operational level, mandatory testing in sandbox environments for all systems before integration into production would reduce the risk of errors and incidents, guaranteeing compliance with security and interoperability standards. The creation of a national catalog of FHIR profiles and an interoperable metadata registry would facilitate the rapid integration of new applications and systems, ensuring data consistency and reporting quality.

Acknowledgement
The European Commission's (EACEA) support to produce this publication, through Jean Monnet Module. Project 101127556 — EU Resilience Digital Skills - EU-ReDiSkills — ERASMUS-JMO-2023-HEI-TCH-RSCH, does not constitute an endorsement of the contents, which reflect the views only of the authors. Neither the European Union nor the granting authority can be held responsible for them.

References

[1] OECD, "The OECD digital government policy framework," *OECD Publishing*, 2020.

[2] OECD, "Empowering the health workforce to make the most of the digital revolution," *OECD Publishing*, 2021.

[3] World Health Organization, Global strategy on digital health 2020-2025, World Health Organisation, 2021.

[4] A. Torab-Miandoab, T. Samad-Soltani , A. Jodati and P. Rezaei-Hachesu , "Interoperability of heterogeneous health information systems: a systematic literature review," *BMC Medical Informatics and Decision Making*, vol. 23, no. 1, January 2023.

[5] European Commission, "The European Health Data Space: What it is and why it matters," *EPRS*, 2022.

[6] European Parliament Research Service, "The European Health Data Space- analysis and perspectives," 2022. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740054/IPOL_STU(2022) 740054_ EN.pdf. [Accessed 20 November 2025].

[7] Government of Romania- General Secretariat of the Government, "National Plan / Documents on the Digital Agenda and the Digital Decade," 2024. [Online]. Available: https://sgg.gov.ro/1/wp-content/uploads/2024/09/ANEXA-1-13.pdf. [Accessed 9 November 2025].

[8] TEHDAS, "Options for the services and infrastructure for secondary use of data in the EHDS," 2023. [Online]. Available: https://tehdas.eu/app/uploads/2023/07/tehdas-options-for-the-services-and-services-architecture-and-infrastructure.pdf. [Accessed 11 November 2025].

[9] TEHDAS Consortium, "Options for governance models for the European Health Data Space," 2023. [Online]. Available: https://tehdas.eu/app/uploads/2023/01/tehdas-options-for-governance-models-for-the-european-health-data-space.pdf. [Accessed 20 November 2025].

[10] World Bank, "Interoperability in health- analytical report. Digital in Health Flagschip Program, Public Disclosure Authorized, Implementation know-how," 2021.

[11] I. Bossenko, R. Randmaa, G. Piho and P. Ross, "Interoperability of health data using the FHIR Mapping Language: Transforming HL7 CDA to FHIR with reusable visual components," *Frontiers in Digital Health*, vol. 6, 2024.

[12] M. Marquis, I. Bossenko and P. Ross, "RadLex and SNOMED CT integration: a pilot study for standardization of radiological classification," *Insights into Imaging*, vol. 16, no. 58, 2025.

[13] A. Gyrard, S. Abedian, P. Gribbon, G. Manias, R. van Nuland, K. Zatloukal, I. E. Nicolae, G. Danciu, S. Nechifor, L. Marti-Bonmati, P. Mallol, S. Dalmiani, S. Autexier, M. Jendrossek, I. Avramidis, E. Garcia Alvarez, P. Holub, I. Blanquer, A. Boden, R. Hussein and , "Lessons learned from European health data projects with cancer use cases: Implementation of health standards and Internet of Things semantic interoperability," *Journal of Medical Internet Research*, vol. 27, 2025.

[14] National Health Insurance House, "Projects and decision-making transparency- PIAS, the electronic health record," 2023-2024. [Online]. Available: https://cnas.ro/category/proiecte/. [Accessed 23 October 2025].

[15] X-Road e-Estonia, "Interoperability services," [Online]. Available: https://e-estonia.com / solutions/ interoperability-services/x-road/. [Accessed 11 November 2025].

[16] European Commission, "European Interoperability Framework (EIF) Guidance and recommendations," 2017. [Online]. Available: https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/european-interoperability-framework. [Accessed 20 11 2015].

[17] e-Estonia, "e-Health records," n.d. [Online]. Available: https://e-estonia.com/solutions/e-health-2/e-health-records/. [Accessed 17 October 2025].

[18] e-Estonia, "This is the story of the world's most advanced digital society," n.d. [Online]. Available: https://e-estonia.com/story. [Accessed 12 November 2025].

[19] X-Road Global, "X-Road documentation and case studies," n.d. [Online]. Available: https://docs.x-road.global/. [Accessed 11 November 2025].

[20] X-Road Global, "X-Road history & case studies," n.d. [Online]. Available: https://x-road.global/xroad-history. [Accessed 20 11 2025].

[21] Sundhedsdatastyrelsen, "Digital Health Strategy 2018–2022," 2018. [Online]. Available: https://english.sundhedsdatastyrelsen.dk/Media/638657841521943752/Digital_Health_Strategy_2018_2022.pdf. [Accessed 9 November 2025].

[22] National Health Insurance House, "Communiqué – PIAS Platform will be replaced with a modern, secure and accessible IT system," 15 October 2025. [Online]. Available: https://cnas.ro/2025/10/15/comunicat-platforma-pias-va-fi-inlocuita-cu-un-sistem-informatic-modern-sigur-si-accesibil/ . [Accessed 10 November 2025].

[23] Emergency Ordinance no. 89/2022, *The National Action Plan for the Digital Decade includes measures for the development of cloud services used by public institutions,* Government of Romania, 2022-2024.

[24] European Commission, "eHealth Digital Service Infrastructure (eHDSI) MyHealth@EU — technical and governance specifications," 2024. [Online]. Available: https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/eu-cooperation/ehealth-network_en. [Accessed 11 Novmeber 2025].

[25] European Commission, "European Health Data Space (EHDS)," n.d. [Online]. Available: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en. [Accessed 11 November 2025].

[26] eHealth Ireland; IHE Europe, "MyHealth@EU – Building digital health services across Europe," 2022. [Online]. Available: https://www.ihe-europe.net/sites/default/files/PDF%20EXP%2022/7-IHE_ExP_DAY_PPT_kJirakova_2022%20%28002%29.pdf. [Accessed 29 October 2025].

[27] European Commission, "Country Health Profile: Romania," 2023. [Online]. Available: https://health.ec.europa.eu/system/files/2023-12/2023_chp_ro_english.pdf. [Accessed 2 November 2025].

[28] Ministry of Health, "Beneficiary Guide- Realization of the eHealth and Telemedicine System (PIAS)," 2022. [Online]. Available: https://oldsite.ms.ro/wp-content/uploads/2022/11/Ghidul-beneficiarului.-Realizarea-sistemului-de-eHealth-si-telemedicina.pdf. [Accessed 10 November 2025].

[29] General Secretariat of the Government, *OECD Report – 01.2025-002,* 2025.

[30] Government of Romania / Legislative Portal, *Emergency Ordinance no. 89/2022 on public cloud computing infrastructures and services,* 2022.

[31] Ministry of Health, *National Health Strategy 2023–2030 (Annex 1),* 2023.

[32] Ministry of Health, *Annex for amending the annex to Order no. 2.300/2023 on the approval of the Financing Guide for the specific investment,* Official Gazette of Romania, 2023.

[33] National Health Insurance House CNAS-PIAS Portal, *Integrated Health Insurance Platform,* n.d.

[34] OECD, "Health data governance for the digital age," *OECD Health Policy Studies,* 2022.

[35] Joint Action TEHDAS, *Options for governance models for the European Health Data Space*, 2023.