DATASPACE 4HEALTH
LUXEMBOURG

Dataspace4Health In the Luxembourgish Health Ecosystem

Document ID : DS4H_WP1_D1.1_D1.2

Author

Dataspace4Health Consortium

Date: 24/07/2025

Funding

This project has received funding from the Ministry of the Economy of Grand Duchy of Luxembourg under Grant agreement no 20230505RDI170010392869.

Disclaimer

The documents published by the consortium are intended solely for informational purposes and reflect the views and opinions of the consortium members at the time of publication and within the scope of the Dataspace4Health project (DS4H).

The ideas expressed herein do not necessarily reflect the official policy or position of the funding entity.

Efforts have been made to achieve the relevance of the content; however, the consortium does not make any representation regarding its completeness and accuracy.

This document may be subject to further revision.

This document is intended to be published on the Dataspace4Health website.

Table of Versions

Version n°	Issue Date	Reason for change
01		
02		
03		

CONTENTS

1. Executive Summary 7
2. Introduction 7
3. EHDS & Gaia-X: Potential for Luxembourg 8
3.1. European Health Data Space (EHDS) 8
3.1.1. Key Objectives 8
3.1.2. Components of the EHDS 9
3.1.3. Benefits of the EHDS 9
3.1.4. Long-term Vision 9
3.2. Gaia-x 10
3.2.1. Key Objectives of Gaia-X 10
3.2.2. Gaia-X for the Health Sector 10
3.2.3. Key Benefits of Gaia-X for Health 10
3.2.4. How Gaia-X Benefits Key Health Stakeholders 11
3.2.5. Conclusion 12
3.3. Relation between EHDS and Gaia-X 12
3.3.1. Common Goals 12
3.3.2. EHDS – Health-Focused Data Ecosystem 12
3.3.3. Gaia-X – The Federated Cloud Infrastructure 12
3.3.4 How EHDS *could* Leverage Gaia-X 13
3.3.5. Collaboration for Innovation 13
3.3.6. Support for the European Health Data Ecosystem 13
3.3.7. Practical Implementation 13
3.3.8. Conclusion 13
3.4. Relevance of EHDS and Gaia-X to digital health transformation 14
3.4.1. Data-Driven Healthcare 14
3.4.2. Personalized Medicine and Innovation 14
3.4.3. Interoperability Across Health Systems 14
3.4.4. Enhanced Healthcare Efficiency 14
3.4.5. Supporting Healthcare Research and Innovation 15
3.4.6. Privacy and Data Security in Healthcare 15
3.4.7. Telemedicine and Remote Healthcare 15
3.4.8. Cross-Border Healthcare and Mobility 15
3.4.9. Building Trust in Digital Health Ecosystems 15

3.4.10. Supporting the European Digital Health Vision 16
3.4.11. Conclusion 16
3.5. Context in Luxembourg 16
3.5.1. Digital Health Infrastructure in Luxembourg 16
3.5.2. Regulatory and Compliance Framework 18
3.5.3. Collaboration between Key Stakeholders 18
3.5.4. Healthcare Innovation and Research 18
3.5.5. Cross-border Healthcare 19
3.5.6. Telemedicine and Digital Health Services 19
3.5.7. Cybersecurity and Data Sovereignty 19
3.5.8. Economic Opportunities and Digital Transformation 19
3.5.9. Proof of Concept for EHDS and Gaia-X 19
3.5.10. Conclusion 20
3.6. Opportunities for Luxembourg 20
3.6.1. Advanced Digital Infrastructure and Agility 20
3.6.2. Supportive Regulatory Environment 20
3.6.3. Healthcare Innovation Hub 20
3.6.4. Cross-border Healthcare and Mobility 21
3.6.5. Leadership in Personalized Medicine and Research 21
3.6.6. Telemedicine and Digital Health Leadership 21
3.6.7. Economic Growth and Attracting Investment 21
3.6.8. Proof of Concept and Scalable Solutions 21
3.6.9. Collaboration with Key Stakeholders 21
3.6.10. Conclusion 22
3.7. Objective of the projects 22
4. Stakeholder Analysis 23
4.1. Key Stakeholders 23
4.1.1. Ministry of Health and Social Security 23
4.1.2. CNS 25
4.1.3. Agence eSanté 28
4.1.4. Key Healthcare Providers 29
4.1.6. IGSS 30
4.1.7. LNDS 30
4.1.8. CNER 30
4.1.9. Health Information Security Body (Organe de Sécurité Informatique en Santé - OSIS) 31
4.1.10. Professional Associations and Trade Unions 31
4.1.11. Patients and Patient Associations 31

4.1.12. Health Professions Council (Conseil Supérieur des Professions de Santé) 31
4.1.13. Health Scientific Council (Conseil scientifique du domaine de la santé) 32
4.1.14. Health Inspection (Division de l'Inspection Sanitaire) 32
4.1.14.2. Responsibilities 32
4.1.15. National Health Observatory (L'Observatoire national de la santé) 32
4.1.16. The Pharmaceutical Industry 32
4.1.17. Academic and Research Institutions 33
4.1.18. Public Health Institute (Direction de la Santé Publique) 33
4.1.19. Conclusion 33
4.2. Collaboration Needs 33
4.2.1. Ministry of Health and Social Security 34
4.2.2. CNS 34
4.2.3. Agence eSanté 34
4.2.4. Key Healthcare Providers 35
4.2.5. UCM 35
4.2.6. IGSS 35
4.2.7. LNDS 36
4.2.8. CNER 36
4.2.9. OSIS 36
4.2.10. Professional Associations and Trade Unions 37
4.2.11. Patient (Associations) 37
4.2.12. Health Professions Council 37
4.2.13. Health Scientific Council 38
4.2.14. Health Inspection 38
4.2.15. National Health Observatory 38
4.2.16. The Pharmaceutical Industry 39
4.2.17. Academic and Research Institutions 39
4.2.19. Public Health and Regulatory Bodies 39
4.2.20. Conclusion 39
5. Regulatory and Compliance Considerations 40
5.1. European Regulatory Framework 40
5.1.1. GDPR 40
5.1.2. NIS2 Directive 41
5.1.3. ePrivacy Directive 41
5.1.4. Directive on Patients' Rights in Cross-Border Healthcare 41
5.1.5. Data Governance Act 42
5.1.6. AI Act 42

5.1.7. Medical Device Regulation 43
5.1.8. In Vitro Diagnostic Regulation 44
5.1.9. Conclusion 44
5.2. National Regulations 44
5.2.1. Data Protection Laws in Luxembourg 44
5.2.2. Healthcare Regulations in Luxembourg 45
5.2.3. Role of National Authorities in Overseeing Compliance 46
5.2.4. Data Sovereignty and Cross-Border Healthcare 48
5.2.5. Conclusion 48
6. Challenges in Harmonizing Compliance 49
6.1. Barriers to Data Protection and Privacy 49
6.1.1. Potential Barriers 49
6.1.2. Collaborative Solutions 50
6.2. Interoperability and Data Exchange 50
6.2.1. Potential Barriers 50
6.2.2. Collaborative Solutions 50
6.3 Balancing Data Security and Accessibility 50
6.3.1. Potential Barriers 51
6.3.2. Collaborative Solutions 51
6.4. Cross-Border Data Exchange and Sovereignty 51
6.4.1. Potential Barriers 51
6.4.2. Collaborative Solutions 51
6.5. Healthcare Professionals and Digital Transformation 52
6.5.1. Potential Barriers 52
6.5.2. Collaborative Solutions 52
6.6. Conclusion 52
7. Proposed Approach 53
7.1. Establish a Self-Learning Health System 53
7.1.1. Key Actions 53
7.1.2. Benefits 54
7.2. Establish a Multi-Stakeholder Governance Framework 54
7.2.1. Key Actions 54
7.2.2. Benefits: 54
7.3. Develop a National Standard for Consent Management 54
7.3.1. Key Actions 55
7.3.2. Benefits 55
7.4. Ensure Interoperability and Secure Cross-Border Health Data Sharing 55

7.4.1. Objective 55
7.4.2. Key Actions 55
7.5. Create a Comprehensive Training Program for Stakeholders 56
7.5.1. Objective 56
7.5.2. Key Actions 56
7.5.3. Benefits 57
7.6. Establish Continuous Monitoring, Auditing and Feedback Mechanisms 57
7.6.1. Objective 57
7.6.2. Key Actions 57
7.6.3. Benefits 57
7.7. Conclusion: A Pathway for Harmonizing Compliance 58
8. Conclusion 58
Annex I 60
Annex II 61

1. EXECUTIVE SUMMARY

- **Purpose of the Document:** Outline a harmonized view and strategy between the different partners within the Dataspace4Health project to bring Health Data Space and Gaia-X innovations to Luxembourg's healthcare ecosystem and to describe the relation with the upcoming European Health Data Space. Furthermore, this document shall reflect the Luxembourgish view and perception to contribute and innovate within the Gaia-X and Data Space initiatives, including constraints and the health ecosystem itself. Finally, this document shall describe the vision and associated risk assessment on creating, building and running the new Gaia-X compliant Data Space in Production.
- **Key Objectives:** Highlight the focus areas such as regulation, compliance, technical requirements and collaboration between key stakeholders.
- **Strategic Importance:** Explain the potential benefits for Luxembourg's healthcare system, including innovation, data sharing and enhanced patient care.

2. INTRODUCTION

Dataspace4Health (DS4H) is a collaborative project between different partners to build a Health Data Space through interconnecting various stakeholders, to create an open healthcare data exchange ecosystem, focusing on secure data sharing and aiming to contribute to innovation in medical treatments. As part of this project, two concrete use-cases are under development in order to demonstrate its envisioned benefit to Luxembourg.

This document will outline a harmonized view and strategy between the different partners how to bring Health Data Space and Gaia-X innovations to Luxembourg. It takes into account elements of the European Health Data Space (EHDS) as well as Gaia-X (and its potential relation), the Luxembourgish health ecosystem (and its constraints), including the different key stakeholders and their collaboration needs.

Another aspect addressed in this document are the opportunities and potential benefits for the Luxembourgish healthcare system (and beyond) that come with the introduction of an Health Data Space, such as streamlining access to quality data to foster innovations and enhanced patient care due to timely access to accurate data to e.g., prevent insufficient as well as inappropriate care, all through secure and compliant data sharing between different institutions.

Furthermore, this document will address regulatory and compliance considerations, both on national- and European level, and describe challenges that are identified which may hinder harmonizing compliance.

Finally, this document will propose different approaches to overcome these challenges and to mitigate identified risks, in order to achieve the envisioned open health ecosystem.

3. EHDS & GAIA-X: POTENTIAL FOR LUXEMBOURG

This chapter will describe the EHDS and Gaia-X in more detail. It will also address the relation between both, as well as their relevance to digital health transformation. Additionally, this chapter will describe the Luxembourgish context and the opportunities it may bring to the country. Finally, this chapter will address the objectives of the DS4H project.

3.1. EUROPEAN HEALTH DATA SPACE (EHDS)

The EHDS, Regulation (EU) 2025/327, which entered into force on the 26th of March 2025 and has key milestones towards full implementation defined (see below for more details), is a major European Union (EU) initiative aimed at creating a framework for the secure and efficient sharing of health data within and across EU member states. It is designed to facilitate both primary use (clinical care) and secondary use (research, policymaking and innovation) of health data, while ensuring high levels of privacy and security.

3.1.1. KEY OBJECTIVES

3.1.1.1. EMPOWERMENT OF INDIVIDUALS:

- Access to Personal Health Data: EHDS ensures that individuals across the EU have the right to easily access and control their personal health data, such as electronic health records (EHR), across borders.
- Portability: Citizens can share their health data with healthcare providers, regardless of the country, improving continuity of care and reducing administrative barriers.

3.1.1.2. IMPROVED HEALTHCARE DELIVERY:

- Cross-border Healthcare: EHDS aims to create a seamless exchange of health data between healthcare providers in different EU member states, allowing for more efficient, timely and personalized care.
- Interoperability Standards: It promotes harmonization of data formats and standards to enable the exchange of data across national health systems.

3.1.1.3. DATA FOR RESEARCH AND INNOVATION:

- Secondary Use of Health Data: EHDS promotes the use of anonymized and pseudonymized health data for research, innovation and policy-making. This enables advancements in medical research, public health and the development of new treatments and technologies.
- Data-Driven Health Solutions: Researchers, companies and policymakers can leverage health data to improve public health outcomes, foster innovation and develop new digital health tools.

3.1.1.4. PRIVACY AND SECURITY:

- GDPR Compliance: EHDS is built around the principles of the General Data Protection Regulation (GDPR), ensuring that health data is handled securely and in line with strict privacy standards.
- Data Sovereignty: EHDS ensures that data remains under the control of individuals and that data protection rights are respected throughout the EU.

3.1.2. COMPONENTS OF THE EHDS

- National Health Data Access Bodies: Each member state is required to establish at least one body to facilitate access to health data for secondary purposes, such as research or policymaking.
- Interoperability Framework: EHDS requires technical standards and infrastructures to ensure that health data can flow smoothly across borders while maintaining high levels of security.
- Cross-border Services: EHDS requires services like ePrescriptions and patient summaries to allow for seamless healthcare across EU countries.

3.1.3. BENEFITS OF THE EHDS

- For Patients: Improved access to personalized healthcare services, even when traveling or living in other EU countries.
- For Healthcare Providers: Enhanced ability to offer more coordinated and efficient care by accessing patient health records in real-time and in the native language of healthcare providers.
- For Researchers and Policy Makers: Easier access to large datasets that can be used for advancing medical research, drug development and public health analysis.
- For Innovators: A supportive environment for developing digital health technologies that rely on secure access to health data.

Defined key milestones towards full implementation of the EHDS, as of the moment of writing this document are:

- **March 2025:** The EHDS Regulation enters into force, marking the beginning of the transition period.
- **March 2027:** Deadline for the Commission to adopt several key implementing acts, providing detailed rules for the regulation operationalization
- **March 2029:** Key parts of the EHDS Regulation will enter into application, including, for primary use, the exchange of the first group of priority categories of health data (Patient Summaries, ePrescriptions/eDispensations) in all EU Member States. Rules on secondary use will also start to apply for most data categories (e.g. data from electronic health records).
- **March 2031:** For primary use, the exchange of the second group of priority categories of health data (medical images, lab results, and hospital discharge reports) should be operational in all EU Member States. Rules on secondary use will also start to apply for the remaining data categories (e.g. genomic data).
- **March 2034:** Third countries and international organizations will be able to apply to join HealthData@EU, for the secondary use.

3.1.4. LONG-TERM VISION

The EHDS aims to create a unified European framework that maximizes the value of health data while safeguarding data privacy. It promotes the use of data to drive healthcare innovation, improve patient outcomes and ensures that European citizens benefit from advancements in digital health technologies and treatments.

3.2. GAIA-X

Gaia-X is a European initiative aimed at creating a federated and secure data infrastructure that ensures data sovereignty, interoperability and innovation. The project was launched in 2019 by Germany and France, with the aim of establishing a European cloud ecosystem that can compete with global tech giants while aligning with European values such as privacy, transparency and openness.

3.2.1. KEY OBJECTIVES OF GAIA-X

3.2.1.1. DATA SOVEREIGNTY

- Gaia-X empowers individuals, organizations and countries to maintain control over their own data by ensuring that it is processed and stored according to European laws and standards, such as the GDPR.
- It provides transparency about where and how data is handled, offering users full control over their information.

3.2.1.2. INTEROPERABILITY AND FEDERATION

- Gaia-X fosters interoperability between different cloud services, ensuring that data can move freely across systems, providers and borders without being locked into one proprietary platform.
- It creates a federated ecosystem where multiple cloud service providers, both large and small, can collaborate and share resources while adhering to common standards.

3.2.1.3. SECURITY AND TRUST

- Gaia-X is designed with robust security measures to protect data and ensure trust in the digital infrastructure. Participants must meet stringent security and compliance requirements.
- By offering a transparent and standardized infrastructure, Gaia-X builds trust between data providers and consumers.

3.2.1.4. INNOVATION AND COMPETITIVENESS:

- Gaia-X supports European businesses, governments and institutions in developing and using cloud services that align with European standards.
- It promotes innovation by creating an open and flexible cloud environment, allowing startups, researchers and companies to develop new digital products and services.

3.2.2. GAIA-X FOR THE HEALTH SECTOR

Gaia-X plays a crucial role in transforming the healthcare sector by providing a secure, interoperable and federated cloud infrastructure for managing and sharing health data. The health sector, which deals with highly sensitive information, could benefit greatly from the principles and technologies underpinning Gaia-X.

3.2.3. KEY BENEFITS OF GAIA-X FOR HEALTH

3.2.3.1. SECURE HEALTH DATA SHARING

- Data Sovereignty: Gaia-X ensures that health data remains under the control of the individual or organization that generates it. This is critical in healthcare, where privacy and compliance with regulations like GDPR are essential.
- Encrypted and Federated Data Exchange: Healthcare providers, researchers and institutions can share data securely across borders, enhancing collaboration and innovation without compromising patient privacy or security.

3.2.3.2. INTEROPERABILITY IN HEALTH SYSTEMS

- Gaia-X promotes the technical interoperability of health data systems, enabling seamless integration of patient records, clinical data and other health-related information between hospitals, doctors and health agencies across Europe.
- This allows trusted healthcare providers to access patient data from different systems in real-time, improving care coordination, especially in cross-border healthcare services.

3.2.3.3. ENABLING INNOVATION IN HEALTHCARE

- Research and Innovation: Through data offerings from healthcare providers, the Gaia-X framework is able to facilitate access to large datasets for medical research, public health analysis and the development of new treatments. This is crucial for areas like personalized medicine, Artificial Intelligence (AI) driven healthcare solutions and the development of digital health applications.
- Faster Medical Advancements: By creating a secure and federated platform, Gaia-X accelerates collaboration between pharmaceutical companies, universities and healthcare providers for faster drug development and clinical trials.

3.2.3.4. PRIVACY-COMPLIANT HEALTH SERVICES

- GDPR Compliance: Gaia-X ensures that all health data is handled in compliance with European data protection laws, safeguarding patient information while allowing it to be used for legitimate healthcare services and research.
- Digital Health Services: Gaia-X supports the development of secure telemedicine, remote diagnostics and e-health applications by providing a trusted infrastructure for patient data.

3.2.3.5. SUPPORT FOR THE EHDS

- Gaia-X is aligned with the goals of the EHDS, providing the underlying infrastructure for data sharing across healthcare systems in Europe.
- It enables secure access to health data for both primary use (clinical care) and secondary use (research, innovation and policymaking), fostering the vision of a unified European health data ecosystem.

3.2.4. HOW GAIA-X BENEFITS KEY HEALTH STAKEHOLDERS

3.2.4.1. HOSPITALS AND HEALTHCARE PROVIDERS

- Hospitals can securely share patient data across regions and countries, leading to better care coordination, especially in emergencies or when patients move across borders.
- By using a federated infrastructure, hospitals can collaborate with research institutions and other providers without compromising data security.

3.2.4.2. PHARMACEUTICAL COMPANIES AND RESEARCHERS

- Pharmaceutical companies can access anonymized and/or pseudonymized data for research purposes, speeding up clinical trials, drug discovery and personalized medicine.
- Researchers can collaborate with other institutions across Europe through secure data-sharing platforms to advance medical research.

3.2.4.3. GOVERNMENTS AND PUBLIC HEALTH AUTHORITIES

- Governments can use aggregated health data to better understand public health trends, manage pandemics and make data-driven policy decisions.

- Public health authorities can leverage Gaia-X to improve data collection, analysis and sharing between different healthcare institutions and/or different countries.

3.2.4.4. PATIENTS

- The Gaia-X framework allows to enable patients to have control over their own personal health data and can decide when and with whom to share it.
- It enhances patient experience by enabling access to digital health services and better coordination between healthcare providers.

3.2.5. CONCLUSION

Gaia-X offers a revolutionary cloud and data infrastructure that supports data sovereignty, security and innovation, making it especially valuable for the health sector. By providing a federated platform for secure data sharing and collaboration, Gaia-X enables healthcare providers, researchers and governments to deliver improved healthcare services, accelerate medical research and safeguard patient privacy in compliance with European regulations.

3.3. RELATION BETWEEN EHDS AND GAIA-X

The EHDS and Gaia-X are two complementary initiatives that aim to transform the way data is managed, shared and utilized across Europe. They share common goals in terms of ensuring data sovereignty, security and interoperability, but they focus on different aspects of the digital infrastructure. The following section describes how both initiatives relate:

3.3.1. COMMON GOALS

- Data Sovereignty: Both EHDS and Gaia-X emphasize that European citizens and organizations must have full control over their data. EHDS focuses on health data, while Gaia-X addresses a broader range of sectors (including healthcare).
- Security and Privacy: Both initiatives ensure that data is handled in compliance with European regulations, particularly the GDPR. Gaia-X provides the cloud infrastructure to manage data securely, while EHDS establishes frameworks for managing sensitive health data.
- Interoperability: Gaia-X and EHDS aim to create standardized, interoperable systems that allow seamless data exchange across borders, sectors and institutions.

3.3.2. EHDS – HEALTH-FOCUSED DATA ECOSYSTEM

- The EHDS is specifically designed to facilitate the sharing and use of health data across Europe for both primary use (patient care) and secondary use (research, policymaking).
- It focuses on enabling secure access to patient data, creating a digital health ecosystem that improves healthcare delivery and supporting research and innovation in the medical field.
- EHDS needs a robust and secure data infrastructure to manage this sensitive information, which is where Gaia-X could play a crucial role.

3.3.3. GAIA-X – THE FEDERATED CLOUD INFRASTRUCTURE

- Gaia-X could provide the underlying cloud and data infrastructure that enables secure, federated and interoperable data exchange between different systems and organizations across Europe.
- It is a cross-sector initiative designed to ensure that data flows freely, securely and in compliance with European laws. Gaia-X's infrastructure supports various industries, including healthcare, manufacturing, finance and more.

- Gaia-X for Health is one specific application of Gaia-X, providing the framework to manage and exchange health data securely within the EHDS.

3.3.4 HOW EHDS *COULD* LEVERAGE GAIA-X

- Technical Backbone: EHDS could rely on Gaia-X to provide the technical infrastructure for storing, processing and exchanging health data across borders. Gaia-X's federated architecture ensures that this data remains secure and accessible in compliance with GDPR.
- Interoperability Standards: Gaia-X offers a framework for interoperability across various cloud services and systems, which is crucial for EHDS to achieve its vision of seamless health data exchange across EU member states.
- Security and Compliance: Gaia-X's cloud infrastructure provides enhanced data security, privacy and compliance mechanisms, which are essential for managing sensitive health information under the EHDS framework.

3.3.5. COLLABORATION FOR INNOVATION

- Innovation in Healthcare: EHDS and Gaia-X both foster innovation by enabling researchers, policymakers and healthcare providers to securely access and share health data. This collaboration supports advances in fields such as personalized medicine, medical research and AI-driven healthcare solutions.
- Data-Driven Healthcare: By integrating the capabilities of Gaia-X into EHDS, health data can be analyzed and shared across borders, leading to improved healthcare outcomes and the development of innovative treatments.

3.3.6. SUPPORT FOR THE EUROPEAN HEALTH DATA ECOSYSTEM

- EHDS and Gaia-X both contribute to the creation of a unified European health data ecosystem that facilitates secure, interoperable and privacy-preserving data flows. This ecosystem enhances healthcare, research and policymaking while respecting European values such as transparency and data sovereignty.
- Gaia-X's infrastructure aligns with the EHDS vision by providing the secure, scalable and interoperable cloud services necessary for health data to be shared and used efficiently across the EU.

3.3.7. PRACTICAL IMPLEMENTATION

- In practical terms, Gaia-X could provide the cloud services and data-sharing platforms that allow healthcare providers, researchers and governments to access and analyze health data securely and efficiently within the framework set by EHDS.
- Healthcare providers would use the EHDS to share patient records across borders, while researchers could access anonymized and/or pseudonymized data for medical research, all facilitated by the Gaia-X infrastructure.

3.3.8. CONCLUSION

The EHDS and Gaia-X are closely related, with EHDS focusing on the secure and compliant sharing of health data across Europe and Gaia-X providing the underlying federated cloud infrastructure. Together, they form a powerful ecosystem that ensures European data sovereignty, privacy and security, while fostering innovation and collaboration in healthcare and beyond. The DS4H project serves as some sort of a pilot for the EHDS implementation, to create and achieve a Health Data Space on a smaller scale – namely in the Luxembourgish health ecosystem.

3.4. RELEVANCE OF EHDS AND GAIA-X TO DIGITAL HEALTH TRANSFORMATION

The EHDS and Gaia-X are pivotal to the ongoing digital health transformation in Europe. They enable a more integrated, efficient and secure approach to managing health data and delivering healthcare services. The following section will describe the relevance of both initiatives to digital health transformation:

3.4.1. DATA-DRIVEN HEALTHCARE

- EHDS enables the secure and seamless exchange of health data across borders, fostering a data-driven healthcare system where health records, lab results and diagnostic data can follow the patient across the EU. This supports continuity of care, improving patient outcomes and making healthcare more personalized.
- Gaia-X provides the infrastructure for securely managing, storing and analyzing these large datasets, making data easily accessible to healthcare providers, researchers and institutions. The ability to access comprehensive, real-time health data is crucial for improving diagnosis, treatment and care coordination.

3.4.2. PERSONALIZED MEDICINE AND INNOVATION

- Personalized Medicine: With EHDS, healthcare providers can access a patient's full medical history, genomic data and other health-related information, enabling more tailored treatments. This personalized approach to care can result in more accurate diagnoses and better outcomes.
- Gaia-X enables the secure exchange of data across different healthcare providers and research institutions, allowing for innovation in AI-driven healthcare solutions, drug development and personalized therapies. These innovations are made possible by the availability of large, secure datasets provided by EHDS, managed by Gaia-X.

3.4.3. INTEROPERABILITY ACROSS HEALTH SYSTEMS

- EHDS aims to break down silos between and within national health systems, promoting interoperability and the standardization of health data across Europe. This ensures that health information can flow freely and securely between healthcare providers, patients and researchers.
- Gaia-X plays a key role by creating a federated infrastructure that supports the technical interoperability of health systems, enabling data from various cloud providers and platforms to be accessed and shared in a standardized way. This is essential for creating a unified digital health ecosystem.

3.4.4. ENHANCED HEALTHCARE EFFICIENCY

- EHDS contributes to greater healthcare efficiency by digitizing health records, enabling telemedicine and streamlining administrative processes like ePrescriptions and cross-border patient summaries. This reduces inefficiencies in healthcare delivery and facilitates quicker, more coordinated care.
- Gaia-X ensures that healthcare data can be securely processed, stored and shared between different healthcare providers, improving collaboration, reducing redundancies and optimizing the

healthcare supply chain. This is especially relevant in managing complex healthcare systems, where multiple stakeholders need access to the same data in real time.

3.4.5. SUPPORTING HEALTHCARE RESEARCH AND INNOVATION

- Secondary Use of Health Data: EHDS enables secondary use of health data for research, innovation and policymaking. Researchers can securely access anonymized or pseudonymized data to conduct studies, develop new treatments or address public health challenges.
- Gaia-X provides the infrastructure needed for this type of large-scale data collection, exchange and analysis while ensuring that data privacy and security are maintained. Through its federated cloud, Gaia-X allows researchers from different countries to collaborate without compromising sensitive health information. This promotes innovation and the development of cutting-edge healthcare technologies.

3.4.6. PRIVACY AND DATA SECURITY IN HEALTHCARE

- Both EHDS and Gaia-X emphasize the importance of data security and privacy, critical for healthcare, where sensitive personal data is involved. GDPR compliance and data sovereignty are central tenets of both initiatives, ensuring that health data is protected while being shared and used responsibly.
- Gaia-X provides secure, GDPR-compliant cloud infrastructure that ensures health data is stored and processed in line with European regulations. This fosters trust in digital health systems, encouraging wider adoption of digital health services among healthcare providers and patients.

3.4.7. TELEMEDICINE AND REMOTE HEALTHCARE

- EHDS supports the use of telemedicine, enabling remote consultations, diagnostics and treatment. With patient data available across borders, telemedicine services can be offered with greater confidence, improving access to healthcare in rural or underserved areas.
- Gaia-X ensures that the technical infrastructure supporting telemedicine is secure, interoperable and scalable, facilitating the growth of remote healthcare solutions. This is particularly relevant post-COVID-19, as telehealth has become a vital tool for healthcare delivery.

3.4.8. CROSS-BORDER HEALTHCARE AND MOBILITY

- EHDS allows for the secure exchange of patient health data across EU borders, ensuring that healthcare providers have access to patient information, regardless of where the patient is located. This is essential for improving healthcare access and continuity for cross-border mobility within the EU.
- Gaia-X ensures that the infrastructure needed to support this cross-border data exchange is in place, providing seamless integration between different healthcare systems while maintaining the highest standards of data security.

3.4.9. BUILDING TRUST IN DIGITAL HEALTH ECOSYSTEMS

- Trust is critical in digital health transformation. EHDS and Gaia-X together create a trusted environment for data sharing and collaboration. By adhering to strict European standards for security, privacy and compliance, they provide assurance to healthcare providers, patients and regulators that health data is handled responsibly.

- This trust is essential for encouraging broader adoption of digital health technologies, from EHRs to AI-powered diagnostics and digital therapeutics.

3.4.10. SUPPORTING THE EUROPEAN DIGITAL HEALTH VISION

- The combination of EHDS and Gaia-X aligns with the broader vision of a European Health Union, where health data is shared securely and used effectively across member states to improve patient care and foster innovation.
- By providing a unified infrastructure (Gaia-X) and clear regulatory framework (EHDS), Europe can lead the world in digital health transformation, leveraging data to improve healthcare services, public health outcomes and economic growth.

3.4.11. CONCLUSION

The EHDS and Gaia-X initiatives are central to Europe's digital health transformation. By enabling secure, interoperable and innovative use of health data, they drive improvements in patient care, healthcare efficiency, research and innovation, all while ensuring data sovereignty and privacy. Together, they create a robust framework for building a future-focused, data-driven healthcare system that benefits both patients and healthcare providers across Europe.

3.5. CONTEXT IN LUXEMBOURG

In Luxembourg, the context for implementing the EHDS and Gaia-X initiatives is shaped by the country's commitment to developing a highly innovative, secure and patient-centered healthcare system. Luxembourg is positioned as a digital and financial hub in Europe, with a strong emphasis on digital transformation, data privacy and cybersecurity. This creates an ideal environment for integrating these European initiatives into its healthcare sector.

The key elements of Luxembourg's Context for DS4H, EHDS and Gaia-X in health are presented in the following chapters.

3.5.1. DIGITAL HEALTH INFRASTRUCTURE IN LUXEMBOURG

3.5.1.1. AGENCE ESANTÉ:

The central eHealth agency in Luxembourg, Agence eSanté, plays a crucial role in managing the country's health information systems, including the National eHealth Platform (eSanté), which facilitates the secure exchange of patient data between healthcare providers. Other digital health services offered by Agence eSanté include:

- Electronic Health Record (Dossier de Soins Partagé - DSP): a platform for sharing and exchanging data in the health sector including the electronic health record. Agence eSanté is in the progress of updating the DSP into a new generation (NG) in line with the EHDS regulation.
- Electronic Vaccination Record (Carnet de Vaccination Electronique - CVE)
- HealthNet: the framework for the secure interconnection network between the different actors in the health sector. It is a secure high-speed infrastructure network that provides various security services, such as Reverse Proxy, Web Proxy, Email Gateway
- Secure messaging

Additionally, Agence eSanté created a Master Plan for Health Information Systems (SDSI, currently Version 3) defining a national strategy for the interoperability of health information systems.
In regards to the EHDS, Agence eSanté has a leading role for the country's implementation in terms of primary use of data.

3.5.1.2. LUXEMBOURG'S EHEALTH STRATEGY:

In 2020 the ministry of Health and Social Security, the Agence eSanté and the Caisse Nationale de Santé (CNS) formalized a proposal for a national eHealth strategy 2021-2028 to help accelerate digitalization in the healthcare sector. The proposed national eHealth strategy 2021-2028 states: "Let's mobilize the potential of digitalization to serve healthcare professionals and patients within the framework of clear governance, to modernize our healthcare system by developing secure systems that ensure the sharing of healthcare data." It is articulated around six key strategic priorities (1 Facilitate patient follow-up for professionals, 2) Engage / involve the patient, 3) Simplify administrative procedures for all, 4) Support players as they upgrade their skills, 5) Adopt methodical, integrated governance, 6) Facilitate secure data sharing and access). Luxembourg has been actively investing in digital health technologies, with initiatives to promote telemedicine, digital health records and personalized medicine. EHDS and Gaia-X align with Luxembourg's goal to create a connected health ecosystem where health data is shared securely across systems, which the DS4H project pilots for.

3.5.1.3. LUXEMBOURG'S NATIONAL INTEROPERABILITY FRAMEWORK:

The country is working to ensure that health data can be exchanged across different healthcare providers. This framework supports the objectives of both EHDS (seamless data exchange) and Gaia-X (interoperability and secure infrastructure).

3.5.1.4. THE STATE INFORMATION TECHNOLOGY CENTER (LE CENTRE DES TECHNOLOGIES DE L'INFORMATION DE L'ÉTAT - CTIE):

The national administration responsible for IT services for the Luxembourgish government, ministries and administrations. CTIE plays a role on the Data Governance Act (DGA) and – as of writing of this document – is likely to have the EHDS technical infrastructure under them, in additional to Agence eSanté and Luxembourg National Data Service (LNDS).

3.5.1.5. NATIONAL INSTITUTE FOR HEALTH AND SOCIAL SECURITY (INSPECTION GÉNÉRALE DE LA SÉCURITÉ SOCIALE - IGSS):

The Luxembourg Microdata Platform on Labour and Social Protection (LMDP) allows for sharing of pseudonymized health data, for example with research organizations.

3.5.1.6. LUXEMBOURG IT FOR HEALTHCARE (LUXITH):

Purpose to implement and operate the shared IT services, software and infrastructures of its members. In additional, they are responsible for implementing the hospital sector's IT strategic plan, which provides for a gradual pooling of IT skills from hospital establishments towards a single system for all hospitals and, if possible, interoperable with the systems of other players in the health sector. LUXITH aims to set up a Health Content Management (HCM) system in 2026 in Luxembourg. The HCM aims to facilitate the archiving and sharing of medical and healthcare documentation, connecting existing Hospital Information Systems (HIS), offering electronic signature and protecting data against cyber-attacks. Moreover, through the HCM, hospitals should benefit from a more centralized infrastructure, connection to the DSP and the integration of medical imaging management.

3.5.1.7. DATA PROTECTION COMMISSION:

Luxembourg's Commission Nationale pour la Protection des Données (CNPD) launched a regulatory sandbox on artificial intelligence (AI), a technology whose rapid progress is raising concerns about privacy and the protection of personal data. The isolated digital environment allows innovators in the Luxembourg ecosystem to test AI systems for a limited time before they are put on the market. The aim is to help them develop AI applications that comply with the GDPR and therefore respect the privacy of the people concerned.

3.5.2. REGULATORY AND COMPLIANCE FRAMEWORK

- **GDPR Leadership:** Luxembourg, as a part of the EU, complies with the GDPR. The protection of personal data, especially sensitive health data, is a priority and both EHDS and Gaia-X align with these GDPR standards.
- **National Health Regulations:** The Ministry of Health and Social Security (Ministère de la Santé et de la Sécurité sociale) oversees the compliance of healthcare providers with both national and European regulations. The Ministry plays a key role in ensuring that the implementation of EHDS meets the necessary regulatory and security standards.
- CNPD is responsible for overseeing data privacy regulations at the national level. The CNPD will be critical in ensuring that health data sharing under EHDS and Gaia-X is compliant with data privacy laws.
- Health studies (such as clinical trials) conducted in Luxembourg are subject to ethical evaluation from the National Research Ethics Committee (Comité National d'Ethique de Recherche - CNER). The CNER operates according to the rules established by the ICH, the Grand-ducal Regulation of 30 May 2005, the law on hospitals of 18 March 2018 and in compliance with the Declaration of Helsinki.

3.5.3. COLLABORATION BETWEEN KEY STAKEHOLDERS

- **Ministry of Health and Social Security:** The Ministry drives the digital transformation of Luxembourg's healthcare system, aligning with European initiatives such as EHDS and Gaia-X to promote innovation and enhance public health services.
- **CNS:** Luxembourg's national health insurance system, CNS, manages large amounts of health data and would benefit from more streamlined data access and sharing. By integrating EHDS and Gaia-X, CNS could enhance healthcare reimbursements, patient care and policy development based on data insights.
- **Hospitals and Healthcare Providers:** Hospitals and doctors in Luxembourg need access to interoperable health data systems to improve the quality of care and patient outcomes. Gaia-X and EHDS provide a platform for secure and standardized data exchange across providers and borders.
- **Luxembourg Institute of Health (LIH) and University of Luxembourg:** Both play crucial roles in medical research and innovation. Access to shared health data through EHDS and secure infrastructure via Gaia-X enables advanced research in areas such as personalized medicine, public health and epidemiology.

3.5.4. HEALTHCARE INNOVATION AND RESEARCH

- **Personalized Medicine:** Luxembourg is a leader in personalized medicine, with institutions like the Luxembourg Centre for Systems Biomedicine (LCSB), the Integrated Biobank of Luxembourg (IBBL) and the National Center of Translational Cancer Research (NCTCR). Additionally, Luxembourg is a front-runner in innovative health projects, such as Clinnova, CoLive Voice and Personalized Functional Profiling (PFP). EHDS can provide more robust access to health data for personalized treatment, while Gaia-X can provide the infrastructure to handle complex, sensitive datasets.

- **Clinical Research and Data Sharing:** The LIH and other research institutions rely on access to large datasets for public health studies and clinical trials. EHDS will enable them to access health data across borders, while Gaia-X ensures data security and compliance with EU standards.

3.5.5. CROSS-BORDER HEALTHCARE

- **Luxembourg's Geopolitical Position:** As a small country surrounded by larger EU countries (France, Germany and Belgium), Luxembourg's healthcare system interacts frequently with cross-border patients and care institutions. EHDS can facilitate cross-border healthcare by ensuring that patient data is accessible when citizens seek medical treatment in other EU countries.
- **Medical Tourism and Workforce Mobility:** Luxembourg experiences a high level of workforce mobility due to its proximity to neighboring countries. EHDS can support mobility of patients and healthcare professionals by making patient data accessible across EU borders, improving care coordination for cross-border workers and patients.

3.5.6. TELEMEDICINE AND DIGITAL HEALTH SERVICES

- **Adoption of Telemedicine:** The COVID-19 pandemic accelerated the adoption of and (temporarily) allowed for telemedicine in Luxembourg. EHDS and Gaia-X can further enhance telemedicine by providing secure and standardized access to health data, ensuring that healthcare professionals have the information needed to offer remote consultations in a secure environment.
- **ePrescriptions:** Luxembourg has made progress in enabling ePrescriptions, which are aligned with the EHDS' goal of creating standardized digital health services. Gaia-X may provide the technical infrastructure for securely managing and transmitting ePrescriptions across borders.

3.5.7. CYBERSECURITY AND DATA SOVEREIGNTY

- **Focus on Cybersecurity:** Luxembourg has a strong focus on cybersecurity, particularly in the financial and governmental sectors. The Cybersecurity Competence Center and national strategies support the secure handling of sensitive health data. Gaia-X's emphasis on secure cloud infrastructure aligns well with Luxembourg's cybersecurity objectives for the health sector.
- **Data Sovereignty:** Gaia-X ensures that health data remains under European control, preventing dependency on non-EU cloud providers. This is critical for Luxembourg, given its focus on data sovereignty and alignment with European privacy standards.

3.5.8. ECONOMIC OPPORTUNITIES AND DIGITAL TRANSFORMATION

- **HealthTech Industry Growth**: Luxembourg is positioning itself as a hub for HealthTech startups and companies. By adopting EHDS and Gaia-X, Luxembourg could attract new businesses and innovators focused on digital health, biotechnology and AI-driven healthcare solutions.
- **Digital Transformation in Healthcare:** With initiatives like Digital Luxembourg, the government aims to lead in digital transformation. EHDS and Gaia-X will be key enablers in digitizing the healthcare sector, making Luxembourg a model for eHealth solutions in Europe.

3.5.9. PROOF OF CONCEPT FOR EHDS AND GAIA-X

- **Luxembourg as a Testbed:** Luxembourg's size and agile digital infrastructure make it an ideal location for pilot projects and proof of concept (PoC) trials for EHDS and Gaia-X implementations, such as the DS4H project with its two concrete use-cases. The country could serve as a testing ground for large-scale health data exchange and cloud infrastructure deployment.

- **Multi-Stakeholder Collaboration:** The coordinated involvement of public institutions (Ministry of Health and Social Security, CNS), private healthcare providers and research institutions (LIH, University of Luxembourg) is key to making a PoC for EHDS and Gaia-X successful in Luxembourg.

3.5.10. CONCLUSION

Luxembourg is uniquely positioned to be at the forefront of digital health transformation by integrating EHDS and Gaia-X innovations into its healthcare system. With strong regulatory frameworks, a commitment to data security and sovereignty and a collaborative approach among key stakeholders, Luxembourg can leverage these initiatives to improve healthcare services, foster medical research and become a leader in digital health and personalized medicine within Europe.

3.6. OPPORTUNITIES FOR LUXEMBOURG

Luxembourg has a significant opportunity to become a pioneer in the implementation of EHDS and Gaia-X innovations due to its advanced digital infrastructure, supportive regulatory environment and collaborative healthcare ecosystem (and limited size thereof). By leveraging these advantages, Luxembourg can position itself as a leader in digital health transformation and reap both healthcare and economic benefits.

The key opportunities for Luxembourg to pioneer EHDS and Gaia-X innovations are presented in the following chapters.

3.6.1. ADVANCED DIGITAL INFRASTRUCTURE AND AGILITY

- Luxembourg has a highly developed digital infrastructure with strong internet connectivity, cutting-edge data centers and a commitment to secure cloud services. This makes the country well-suited for the deployment of Gaia-X infrastructure to securely manage and share health data.
- Luxembourg's small size and centralized healthcare system allow for quick implementation and integration of new technologies. This agility can enable rapid adoption of EHDS initiatives and serve as a model for larger EU countries.

3.6.2. SUPPORTIVE REGULATORY ENVIRONMENT

- Luxembourg's robust adherence to European privacy regulations, including GDPR, ensures that any health data initiative is fully compliant with data protection standards. This makes Luxembourg an ideal location for testing EHDS innovations, which require strict compliance with data privacy laws.
- With Luxembourg's government and its regulatory bodies, such as the CNPD, prioritizing data sovereignty and cybersecurity, Luxembourg can lead by example in ensuring secure and ethical management of health data under EHDS.

3.6.3. HEALTHCARE INNOVATION HUB

- Luxembourg is already home to innovative health institutions like the LIH (including the NCTCR and IBBL) and the LCSB. These institutions focus on personalized medicine, biomedical research and health data analytics. By incorporating EHDS and Gaia-X, Luxembourg can boost its research capabilities through secure and interoperable health data sharing.
- Luxembourg can attract HealthTech startups and companies by offering a secure, federated platform to test and develop new digital health solutions. This could stimulate growth in the HealthTech sector, making Luxembourg a leader in AI-driven healthcare innovations.

3.6.4. CROSS-BORDER HEALTHCARE AND MOBILITY

- Due to Luxembourg's central location in Europe and its close interaction with neighboring countries, there is a high demand for cross-border healthcare services. EHDS can facilitate seamless patient data exchange across borders, ensuring continuity of care for patients traveling or working in other EU countries.
- Luxembourg can lead the way in implementing cross-border health solutions, making it a key player in the development of a more connected and integrated European healthcare system.

3.6.5. LEADERSHIP IN PERSONALIZED MEDICINE AND RESEARCH

- Luxembourg is already pioneering personalized medicine initiatives, which rely heavily on access to big health data and secure, interoperable systems. By embracing EHDS and Gaia-X, Luxembourg can become a hub for personalized treatment, leveraging secure data sharing to enhance research on genomics, public health and chronic disease management.
- Gaia-X will enable Luxembourg to provide cloud infrastructure that allows researchers to collaborate on health data across borders, facilitating large-scale clinical trials and the development of precision medicine.

3.6.6. TELEMEDICINE AND DIGITAL HEALTH LEADERSHIP

- The rise of telemedicine in Luxembourg, accelerated by the COVID-19 pandemic, creates an opportunity for Luxembourg to lead in the development of secure and interoperable digital health services. EHDS and Gaia-X can enhance the quality and security of telemedicine, making Luxembourg a model for other EU nations.
- Luxembourg can pioneer the deployment of ePrescriptions, remote patient monitoring and AI-driven diagnostics, supported by secure data sharing between healthcare providers and patients.

3.6.7. ECONOMIC GROWTH AND ATTRACTING INVESTMENT

- By positioning itself as a leader in digital health transformation, Luxembourg can attract European funding and investment from the private sector, particularly in HealthTech, biotechnology and digital therapeutics.
- Luxembourg can become a European hub for HealthTech innovation, attracting startups, researchers and investors who want to test new technologies in a compliant and secure environment.

3.6.8. PROOF OF CONCEPT AND SCALABLE SOLUTIONS

- Luxembourg is well-suited to serve as a testbed for EHDS and Gaia-X innovations, given its small size, efficient regulatory framework and agile healthcare system. By successfully piloting projects such as cross-border data sharing, personalized medicine trials and telemedicine solutions, Luxembourg can demonstrate scalable solutions that can be expanded to larger EU countries.
- A successful PoC in Luxembourg would reinforce the country's reputation as a leader in digital health and position it as a model for the European Health Union.

3.6.9. COLLABORATION WITH KEY STAKEHOLDERS

- Luxembourg has a strong network of collaborative stakeholders in healthcare, research and government, including the Ministry of Health and Social Security, CNS, LIH, Hospitals and Agence eSanté. This makes the country ideal for fostering collaboration between public and private sectors to achieve a harmonized digital health strategy.

- The collaboration with Gaia-X's federated infrastructure will allow Luxembourg's stakeholders to lead in the secure sharing of health data, ensuring that data sovereignty and compliance are maintained while enhancing patient care and research capabilities.

3.6.10. CONCLUSION

Luxembourg's advanced digital infrastructure, commitment to data privacy, leadership in personalized medicine and its central position in Europe offer a unique opportunity for the country to pioneer the implementation of EHDS and Gaia-X innovations. By leading in digital health transformation, Luxembourg can improve healthcare services, attract investment and become a model for other EU nations, driving the future of European healthcare.

3.7. OBJECTIVE OF THE PROJECTS

The objective of establishing a harmonized strategy is to develop a PoC for the implementation of Health Data Space and Gaia-X innovations within the healthcare sector in Luxembourg, as part of the DS4H project. This will also serve as preparational work for early identification of potential barriers for future EHDS implementation and will allow to propose actions to overcome these. This strategy aims to ensure alignment across key stakeholders—including healthcare providers, government bodies, research institutions and technical experts—in terms of regulatory compliance, data security, interoperability and privacy standards. The PoC will serve as a blueprint for demonstrating how Luxembourg can leverage these innovations to enhance healthcare delivery, research capabilities and cross-border data exchange, while adhering to European data protection regulations.

4. STAKEHOLDER ANALYSIS

4.1. KEY STAKEHOLDERS

The health system in Luxembourg involves around a variety of key stakeholders, each playing a critical role in the delivery, management, innovation and regulation of healthcare services.

These stakeholders include governmental bodies, public and private healthcare providers, professional organizations, research organizations, insurance systems and patients themselves. The section below will provide a detailed overview of the main stakeholders in Luxembourg's healthcare system.

For a more concise overview in a table format, please refer to Annex I.

4.1.1. Ministry of Health and Social Security

4.1.1.1. ROLE

The Ministry of Health and Social Security is the central governmental authority responsible for setting health policy, regulating the healthcare system, overseeing public health programs and ensuring the quality and safety of healthcare services in Luxembourg.

4.1.1.2. RESPONSABILITIES

It supervises hospitals, healthcare professionals, medical products and public health campaigns. It also leads the response to health crises (e.g., pandemics) and ensures the implementation of eHealth strategies.

4.1.1.3. DETAILED INFORMATION

The Ministry of Health and Social Security in Luxembourg plays a crucial role in coordinating and overseeing the country's eHealth initiatives, including the management of health data exchange. Its responsibilities in this area align with the broader goals of improving healthcare efficiency, enhancing patient care and ensuring data privacy and security. A detailed explanation of the Ministry's role in eHealth coordination and health data management is described below.

4.1.1.4. STRATEGIC LEADERSHIP AND POLICY DEVELOPMENT

The Ministry of Health and Social Security sets the strategic direction for eHealth development in Luxembourg. This includes defining the national eHealth strategy in collaboration with other stakeholders, such as the Agence eSanté and healthcare providers.

It ensures that eHealth initiatives are aligned with national healthcare goals, such as improving access to healthcare services, streamlining operations and fostering innovation through digital technologies.

4.1.1.5. OVERSIGHT OF AGENCE ESANTÉ

Agence eSanté is the key technical and operational body responsible for implementing eHealth solutions, such as the DSP, which is the shared EHR system in Luxembourg. The Ministry of Health and Social Security provides supervisory oversight and ensures that the agency operates in accordance with national health priorities.

Through its oversight of Agence eSanté, the Ministry ensures that health data is shared securely and efficiently across the healthcare ecosystem, promoting interoperability among various healthcare providers, hospitals and institutions.

4.1.1.6. DATA PRIVACY AND SECURITY REGULATION

The Ministry ensures that health data exchange and storage systems comply with Luxembourg's strict data protection laws, including the GDPR.

It sets the regulatory framework for how personal health information is handled, ensuring that patients' rights to privacy and confidentiality are safeguarded. This involves working closely with regulatory bodies to ensure robust data security protocols are in place for all eHealth platforms.

4.1.1.7. COORDINATION OF DIGITAL HEALTH SERVICES

The Ministry of Health and Social Security coordinates the implementation of digital health services, such as telemedicine, digital prescriptions and online patient portals. It ensures that these services are integrated into the national healthcare system and are accessible to both healthcare professionals and patients.

By promoting the use of digital tools, the Ministry helps to modernize healthcare delivery, enabling more efficient communication and data exchange between patients and providers.

4.1.1.8. PROMOTING INTEROPERABILITY

One of the Ministry's key roles is to promote interoperability between different healthcare IT systems. It ensures that health data from various sources (such as hospitals, labs, general practitioners and specialists) can be shared seamlessly through the national health information exchange infrastructure.

This interoperability enables healthcare providers to access complete and accurate patient data, which is critical for effective diagnosis, treatment and continuity of care.

4.1.1.9. PUBLIC HEALTH MONITORING AND DATA ANALYSIS

The Ministry of Health and Social Security uses aggregated health data from various eHealth systems to monitor public health trends, detect outbreaks and make informed decisions on health policy.

Through data analytics and reporting, the Ministry can better allocate resources, plan public health interventions and improve the overall health system's responsiveness to emerging challenges, such as pandemics or chronic disease management.

4.1.1.10. STAKEHOLDER ENGAGEMENT AND COLLABORATION

The Ministry of Health and Social Security engages with a wide range of stakeholders, including healthcare providers, insurance providers, technology vendors and patient advocacy groups to ensure that eHealth solutions meet the needs of all users.

It plays a central role in coordinating efforts between public and private sectors to foster collaboration on eHealth projects, encouraging innovation while maintaining strict standards for quality and security.

4.1.1.11. CROSS-BORDER EHEALTH INITIATIVES

As Luxembourg is part of the EU, the Ministry of Health and Social Security also participates in EU-wide eHealth initiatives. This includes promoting cross-border health data exchange through platforms like epSOS (European Patient Smart Open Services), allowing patients to receive care in other EU countries while ensuring that their medical data is accessible and secure.

The Ministry works to harmonize Luxembourg's eHealth framework with European regulations, facilitating international cooperation in health services and research.

4.1.1.12. SUPPORT FOR RESEARCH AND INNOVATION

The Ministry encourages the use of eHealth data for health research and innovation, while ensuring that patient data is anonymized and/or pseudonymized and used ethically.

It fosters partnerships with academic and research institutions, supporting the development of new digital health technologies, data analytics tools and innovative healthcare solutions.

4.1.1.13. EDUCATION AND AWARENESS CAMPAIGNS

The Ministry plays a key role in raising awareness about the benefits of eHealth among healthcare professionals and the general public. It supports training programs for healthcare workers to ensure they are proficient in using digital health tools and it educates the public about accessing their health records and using eHealth services.

These awareness campaigns aim to increase the adoption of eHealth solutions and promote digital literacy across the healthcare sector.

4.1.1.14. SUMMARY

The Ministry of Health and Social Security in Luxembourg serves as the central authority for the coordination, oversight and regulation of eHealth initiatives. It provides strategic leadership, ensures data privacy and security, promotes interoperability and facilitates the digital transformation of healthcare. By working with agencies like Agence eSanté and aligning with European eHealth standards, the Ministry ensures that Luxembourg’s health data exchange systems are efficient, secure and patient-centered, ultimately contributing to a more modern and effective healthcare system.

4.1.2. CNS

4.1.2.1. ROLE

The CNS is the public health insurance fund in Luxembourg, covering the majority of the population under the compulsory health insurance.

4.1.2.2. RESPONSIBILITIES

It manages healthcare reimbursements for medical services, prescriptions, hospital stays and other healthcare-related expenses. The CNS also negotiates tariffs with healthcare providers and ensures that medical services remain accessible and affordable.

4.1.2.3. DETAILED INFORMATION

CNS is a key institution in Luxembourg's healthcare system, primarily responsible for managing public health insurance. It also plays a significant role in eHealth coordination and the management of health data exchange. What follows below is an in-depth explanation of the CNS's responsibilities in these areas.

4.1.2.4. HEALTHCARE REIMBURSEMENT AND FINANCING

CNS is the primary health insurance provider in Luxembourg, covering the vast majority of the population through compulsory public health insurance.

As part of its role in managing health insurance, CNS is central to digitalize healthcare reimbursement systems, ensuring that claims for medical services, medications and treatments are processed efficiently through digital platforms. This reduces paperwork and speeds up reimbursements for both patients and healthcare providers.

4.1.2.5. INTEGRATION WITH EHEALTH PLATFORMS

CNS plays a key role in integrating the eHealth infrastructure with Luxembourg's broader healthcare system, particularly with the DSP. Through this integration, CNS helps to ensure that healthcare providers can access patient data securely and efficiently while maintaining proper billing and reimbursement processes.

The CNS collaborates closely with Agence eSanté to ensure that the health data exchanged within the DSP and other digital health platforms aligns with the insurance claims and reimbursement systems.

4.1.2.6. MANAGEMENT OF HEALTH DATA FOR BILLING AND REIMBURSEMENT

The CNS is responsible for managing health data related to medical services provided, prescriptions, treatments and healthcare products in Luxembourg. This includes ensuring the secure exchange of health data between healthcare providers and the CNS for the purpose of billing and reimbursement.

CNS works with healthcare providers to automate data exchange, minimizing manual processing. It uses digital solutions to verify services rendered, ensuring that healthcare providers receive payment and that patients are reimbursed correctly for services covered by insurance.

4.1.2.7. DIGITAL TOOLS FOR PATIENTS

CNS provides digital tools and platforms for patients to access their insurance information, submit claims and track their reimbursements online. This includes platforms like MyGuichet, where patients can access health data, check reimbursement status and submit claims electronically.

These digital services are integrated with Luxembourg’s eHealth infrastructure, allowing patients to manage their health insurance and interact with the healthcare system more efficiently.

4.1.2.8. DATA SECURITY AND PRIVACY

Given the sensitive nature of health data, CNS is deeply involved in ensuring that the health data exchanged for insurance purposes complies with GDPR and other national data protection laws.

CNS enforces strict data privacy protocols, ensuring that patient information, medical records and insurance data are handled securely. It works to ensure that all digital transactions and data exchanges are encrypted and that only authorized personnel have access to sensitive information.

4.1.2.9. PROMOTING EHEALTH ADOPTION

CNS plays a crucial role in promoting the adoption of eHealth solutions among both healthcare providers and patients. By supporting the digitalization of claims processing and medical billing, CNS encourages healthcare professionals to adopt EHRs and digital platforms for their daily operations.

For patients, CNS encourages the use of digital portals for managing health insurance claims, which complements the broader push towards digital health management in Luxembourg.

4.1.2.10. COLLABORATION WITH AGENCE ESANTÉ

CNS collaborates closely with Agence eSanté to ensure the smooth integration of health data exchange systems with the insurance framework. This collaboration ensures that health data is shared securely and in a standardized manner, promoting interoperability across healthcare providers, insurance systems and the eHealth platform.

The CNS also works with Agence eSanté to ensure that new eHealth technologies and innovations, such as telemedicine and digital prescriptions, are integrated into the reimbursement framework.

4.1.2.11. HEALTH DATA ANALYTICS AND PUBLIC HEALTH INSIGHTS

CNS contributes to the national healthcare system by analyzing the data it collects on healthcare usage and expenses. These insights can be used to improve healthcare efficiency, control costs and develop better health policies.

By participating in public health data initiatives, CNS helps provide anonymized data for use in public health planning and research. This data can inform national strategies on healthcare resource allocation, prevention programs and healthcare quality improvements.

4.1.2.12. SUPPORT FOR CROSS-BORDER HEALTHCARE

Luxembourg residents often seek healthcare services in neighboring countries under the European Health Insurance Card (EHIC) or other cross-border health agreements. CNS manages the cross-border health data exchange and reimbursement processes for these services, ensuring that Luxembourg patients can access care abroad and that the corresponding health data and payments are processed efficiently.

CNS ensures that data exchanged for cross-border healthcare remains compliant with both Luxembourg's national regulations and EU healthcare directives.

4.1.2.13. EPRESCRIPTIONS

CNS supports the digital ePrescription system, which allows physicians to issue prescriptions electronically and pharmacies to process them through an integrated eHealth platform.

This digital system reduces administrative work, improves the accuracy of prescriptions and facilitates the automatic linkage between prescribed medications and the CNS reimbursement system.

4.1.2.14. MANAGING COSTS AND SUSTAINABILITY

CNS uses health data to monitor the costs of healthcare services and evaluate the sustainability of healthcare expenditures. By analyzing data from eHealth systems, CNS can make informed decisions about how to allocate resources efficiently, negotiate tariffs with healthcare providers with the aim to control rising healthcare costs.

This data-driven approach ensures that Luxembourg's healthcare system remains financially sustainable while continuing to provide high-quality services to its citizens.

4.1.2.15. INNOVATION IN HEALTHCARE PAYMENT MODELS

The CNS works to integrate innovative payment models into the eHealth ecosystem, such as value-based care, which links reimbursement to the quality of care delivered rather than just the quantity of services. Through data exchange and analysis, CNS can assess health outcomes and adjust payment models to encourage more effective and efficient care.

4.1.2.16. SUMMARY

The CNS plays a critical role in Luxembourg's eHealth coordination and health data exchange, ensuring that the health insurance and reimbursement systems are tightly integrated with the country's eHealth platforms. It supports the digital transformation of healthcare by managing the exchange of health data for billing, reimbursement and public health planning. CNS ensures that both healthcare providers and patients benefit from efficient, secure and transparent digital processes while maintaining compliance with data protection regulations and promoting the adoption of eHealth solutions across the healthcare system.

4.1.3. AGENCE ESANTÉ

4.1.3.1. ROLE

The national eHealth agency coordinates and manages the digital infrastructure of Luxembourg's healthcare system, including the DSP.

4.1.3.2. RESPONSIBILITIES

It oversees the secure exchange of patient health data, facilitates interoperability between healthcare systems, ensures data privacy and supports eHealth initiatives like telemedicine. In regards to the EHDS, Agence eSanté is responsible for the primary use of data.

4.1.3.3. DETAILED INFORMATION

The Agence eSanté is the national eHealth agency of Luxembourg, established to coordinate and manage the digitalization of healthcare and the exchange of health data across the country. Its role is central to improving the efficiency, security and accessibility of health services through a digital infrastructure. Key aspects of its role in eHealth coordination and the management of health data exchange are described below.

4.1.3.4. DEVELOPMENT AND MANAGEMENT OF THE EHEALTH PLATFORM

Agence eSanté is responsible for developing and maintaining Luxembourg’s national eHealth platform, known as eSanté. This platform enables the secure sharing and exchange of health information among healthcare professionals, hospitals, laboratories and other healthcare stakeholders. It ensures interoperability between different healthcare systems to facilitate the transfer of patient data and electronic medical records (EMRs).

4.1.3.5. CENTRALIZED PATIENT DATA EXCHANGE (DSP)

A core service managed by the Agence eSanté is the DSP. The DSP allows patients and healthcare providers to access a comprehensive EHR that includes medical history, prescriptions, test results and other critical health data. It enhances care coordination by making the information easily accessible in real-time, reducing redundant procedures and improving patient safety.

4.1.3.7. SECURITY AND DATA PRIVACY

The agency plays a critical role in ensuring that health data is exchanged securely and in compliance with Luxembourg’s strict data protection laws, including the GDPR. Agence eSanté implements robust security protocols, such as encryption and access controls, to ensure that sensitive patient data is protected while being shared across various healthcare entities.

4.1.3.8. INTEROPERABILITY AND STANDARDIZATION

Agence eSanté promotes interoperability by developing and enforcing standards for the exchange of health information. This involves ensuring that various healthcare software systems, EHRs and digital

tools can communicate with each other effectively. It also ensures that medical data is standardized across different platforms, facilitating seamless data flow between healthcare providers.

4.1.3.9. SUPPORT FOR HEALTHCARE PROVIDERS

The agency supports healthcare providers by offering tools and training to help them integrate eHealth solutions into their practice. This includes helping physicians, hospitals and pharmacies connect to the national health data exchange platform, use digital prescriptions and manage electronic patient records.

4.1.3.10. PUBLIC HEALTH AND RESEARCH

In addition to supporting healthcare delivery, Agence eSanté facilitates public health monitoring and research by enabling aggregated health data analytics. The availability of centralized health data can be used to monitor trends, manage public health initiatives and support clinical research, all while ensuring the anonymity and protection of personal patient information.

4.1.3.11. EMPOWERMENT OF PATIENTS

Agence eSanté also focuses on patient empowerment by providing patients with direct access to their health records. Through the DSP system, patients can view their own medical data, manage permissions for healthcare providers to access their information and actively participate in their healthcare management.

4.1.3.12. COORDINATION OF EHEALTH PROJECTS

The agency coordinates national eHealth projects and initiatives in collaboration with the Ministry of Health and Social Security, healthcare institutions and other stakeholders. This includes launching innovative digital health solutions, such as telemedicine services and mobile health apps and promoting the adoption of new technologies in healthcare.

4.1.3.13. EMERGENCY MEDICAL DATA

The agency has also developed solutions for emergency medical data sharing. This ensures that in the case of an emergency, healthcare professionals can access critical medical information, such as allergies, current treatments and pre-existing conditions, even if the patient is unable to provide it.

4.1.3.14. SUMMARY

Agence eSanté plays a pivotal role in transforming Luxembourg's healthcare system through digitalization. It ensures secure and efficient management of health data, improves coordination between healthcare providers and empowers patients to have greater control over their health information. Its efforts are focused on creating a more connected, efficient and patient-centered healthcare system.

4.1.4. KEY HEALTHCARE PROVIDERS

- **Public and Private Hospitals:** Luxembourg has a mix of public and private hospitals and other specialized centers (e.g., rehabilitation centers, center for radiotherapy) that provide secondary and tertiary care services and are grouped within the Federation of Luxembourgish Hospitals (Fédération des Hôpitaux Luxembourgeois – FHL).
- **Primary Care Physicians (General Practitioners):** GPs are often the first point of contact for patients in Luxembourg's healthcare system. They play a critical role in diagnosing and referring patients to specialists or hospitals.
- **Specialists:** Various medical specialists, including cardiologists, neurologists and surgeons, provide secondary care either within hospitals or in private practices.
- **Pharmacies:** Pharmacists are responsible for dispensing medications, providing advice on drug use and contributing to public health efforts such as vaccinations.

- **Laboratories:** the National Health Laboratory (Laboratoire National de Santé – LNS), as well as the private laboratories grouped within the Luxembourgish Federation of Medical Analysis Laboratories (Fédération Luxembourgeoise des Laboratoires d'Analyses Médicales – FLLAM): Laboratoires Réunis, Ketterthill and BIONEXT, all responsible for taken and analyzing clinical specimens to obtain information about the health of a patient to aid in diagnosis, treatment, and prevention of disease.
- Different institutions grouped within COPAS, such as for elderly care, for people with disabilities etc. e.g., responsible to assist with activities of daily living, such as bathing, dressing, and medication management.
- **The Grand Ducal Fire and Rescue Corps (Corps grand-ducal d'incendie et de secours - CGDIS)**: providing emergency medical assistance services.
- Other healthcare professionals, such as physiotherapists, nurses, laboratory assistants, etc. to carry out various tasks to contribute to the healthcare system.

4.1.5. UNION OF SICKNESS FUNDS (UNION DES CAISSES DE MALADIE - UCM)

4.1.5.1. ROLE

The UCM coordinates the different sickness funds in Luxembourg.

4.1.5.2. RESPONSIBILITIES

It helps negotiate the terms of care, reimbursement and tariffs between healthcare providers and insurance funds, contributing to the financial sustainability of the healthcare system.

4.1.6. IGSS

4.1.6.1. ROLE

The IGSS oversees the functioning of the social security system, including healthcare.

4.1.6.2. RESPONSIBILITIES

It monitors the financial stability and performance of the healthcare system, ensuring compliance with national regulations and standards in health and social protection.

4.1.7. LNDS

4.1.7.1. ROLE

Created by the Luxembourg Government to implement Luxembourg's strategies in research, innovation, and digitalization.

4.1.7.2. RESPONSIBILITIES

LNDS enables value creation from secondary use of data, for public and private partners and supports the sharing and re-use of public sector data, in a trustable manner.

In regards to the EHDS, LNDS has a leading role for the country's implementation in terms of secondary use of data.

4.1.8. CNER

4.1.8.1. ROLE

The national ethics body for evaluating health studies.

4.1.8.2. RESPONSIBILITIES

The CNER is responsible for protecting persons participating in a health study by providing an opinion concerning the ethical acceptability of projects (such as clinical trials) submitted to it. This opinion may be positive (approval), negative (rejection) or an exemption (possible in case of anonymous retrospective studies). The CNER is thus of significant importance for the DS4H project due to its – by law defined – involvement concerning secondary use of health data.

4.1.9. HEALTH INFORMATION SECURITY BODY (ORGANE DE SÉCURITÉ INFORMATIQUE EN SANTÉ - OSIS)

4.1.9.1. ROLE

OSIS was created by the Ministry of Health within a national cybersecurity framework. Its goal is to facilitate discussions on cybersecurity and the various entities involved.

4.1.9.2. RESPONSIBILITIES

It's missions are to define both general- and specific cybersecurity guidelines for hospitals, as well as so-called "transversal" structures (such as LUXITH or eSanté).

4.1.10. PROFESSIONAL ASSOCIATIONS AND TRADE UNIONS

- Luxembourg Medical Association (Association des Médecins et Médecins-Dentistes - AMMD): Represents doctors and dentists and is involved in negotiations regarding tariffs and working conditions.
- FHL: Represents the interests of hospitals and healthcare institutions in Luxembourg.
- Healthcare Workers' Unions: Represent various healthcare professionals, such as nurses, midwives and allied health workers, advocating for their working conditions, salaries and professional development.

4.1.11. PATIENTS AND PATIENT ASSOCIATIONS

4.1.11.1. PATIENTS

Patients are at the center of the healthcare system, with rights to access high-quality care, reimbursement for medical services and involvement in healthcare decisions.

4.1.11.2. PATIENT ASSOCIATIONS

Various organizations represent patients with specific health conditions, advocating for better care, support and research. For example, associations for cancer, diabetes and rare diseases provide support and raise awareness.

4.1.11.3. NATIONAL HEALTH INFORMATION AND MEDIATION SERVICE

To provide information, advice, as well as conflict prevention and resolution between healthcare providers and patients.

4.1.12. HEALTH PROFESSIONS COUNCIL (CONSEIL SUPÉRIEUR DES PROFESSIONS DE SANTÉ)

4.1.12.1. ROLE

This body is responsible for regulating the licensing, qualifications and ethical practices of healthcare professionals, including doctors, nurses and pharmacists.

4.1.12.2. RESPONSIBILITIES

It ensures that healthcare providers meet the required standards for professional practice and patient safety.

4.1.13. HEALTH SCIENTIFIC COUNCIL (CONSEIL SCIENTIFIQUE DU DOMAINE DE LA SANTÉ)

4.1.13.1. ROLE

An independent organization composed of medical professionals whose mission is to develop and contribute to the implementation of standards of good medical practice.

4.1.13.2. RESPONSIBILITIES

To promote high-quality care, to guide healthcare professionals in the development of good practices and to make optimal use of available resources.

4.1.14. HEALTH INSPECTION (DIVISION DE L'INSPECTION SANITAIRE)

4.1.14.1. ROLE

Part of the Ministry of Health and Social Security, this division is responsible for inspecting and ensuring the hygiene, safety and compliance of healthcare institutions.

4.1.14.2. RESPONSIBILITIES

It oversees the licensing of healthcare facilities, investigates complaints and enforces public health laws.

4.1.15. NATIONAL HEALTH OBSERVATORY (L'OBSERVATOIRE NATIONAL DE LA SANTÉ)

4.1.15.1. ROLE

As an administrative body under the authority of the Ministry of Health and Social Security, the purpose of the National Health Observatory is to guide health decisions and policies and assess their impact by networking data.

4.1.15.2. RESPONSIBILITIES

To evaluate the population health status, publish and disseminate these findings and to propose improvements to the population's health status and the health system.

4.1.16. THE PHARMACEUTICAL INDUSTRY

Innovative Medicine for Luxembourg (IML) is the association of the biopharmaceutical industries active in Luxembourg and bring together the expertise of more than 60 laboratories involved in the research and development of innovative medicines, who’s members account for around 90% of medicines imported into Luxembourg.

In addition, recently bill 8491 passed in Luxembourg to establish a new Luxembourgish Agency for Medicines and Health Products (Agence luxembourgeoise des médicaments et produits de santé - ALMPS)

4.1.16.1. ROLE

Pharmaceutical companies, both local and international, provide medications and treatments to healthcare providers in Luxembourg.

4.1.16.2. RESPONSIBILITIES

They are involved in research, development, manufacturing and the distribution of pharmaceutical products, as well as negotiating pricing and reimbursement conditions with the CNS.

4.1.17. ACADEMIC AND RESEARCH INSTITUTIONS

4.1.17.1. ROLE

Institutions like the University of Luxembourg (including the LCSB) and research organizations like the LIH (including the NCTCR and IBBL) contribute to medical research, healthcare innovation and the training of healthcare professionals.

4.1.17.2. RESPONSIBILITIES

They engage in research activities in areas like biotechnology, health data and medical science, often collaborating with hospitals and the government.

4.1.18. PUBLIC HEALTH INSTITUTE (DIRECTION DE LA SANTÉ PUBLIQUE)

4.1.18.1. ROLE

Focuses on public health promotion, disease prevention and health monitoring by defining public health objectives and contribute to the national health strategy.

4.1.18.2. RESPONSIBILITIES

To develop and manage national health plans and interact with all healthcare system partners. To provide awareness, screening, and surveillance services. To ensure access, quality, and safety of healthcare. To guarantees compliance with applicable laws, regulations, and standards. To support the development of effective public health policies.

4.1.19. CONCLUSION

The healthcare system in Luxembourg operates with a multi-stakeholder approach, where governmental bodies regulate and fund healthcare, providers deliver services and patients have a say in their care. Research institutions introduce health innovations. The system is built on the principles of universal health coverage, with significant emphasis on data privacy, patient rights and quality healthcare delivery. These stakeholders work collaboratively to ensure that healthcare services in Luxembourg are efficient, equitable and accessible to all.

4.2. COLLABORATION NEEDS

Achieving a unified and efficient eHealth strategy in Luxembourg requires close collaboration among various stakeholders in the healthcare ecosystem. These stakeholders include government bodies, healthcare providers, insurance funds, professional organizations, patients and research institutions.

Each plays a specific role and their collaboration is essential for balancing regulatory, technical and operational aspects of the health system. The section below describes in detail how these stakeholders will need to work together.

Annex I provides a concise overview.

4.2.1. MINISTRY OF HEALTH AND SOCIAL SECURITY

4.2.1.1. ROLE

Strategic leadership, regulation and public health policies.

4.2.1.2. COLLABORATION NEEDS

The Ministry must provide clear leadership and policy direction while ensuring that regulations related to data privacy, security and public health are enforced. It works with CNS, Agence eSanté and Healthcare Providers to integrate these policies into day-to-day healthcare operations. The Ministry also needs to collaborate with Professional Associations, Patients' Associations and Pharmaceutical Industry to ensure that the needs of all stakeholders are considered when setting eHealth policies.

4.2.1.3. BALANCING ASPECTS

The Ministry balances regulatory compliance with innovation, ensuring that Luxembourg's healthcare system embraces new technologies without compromising on quality and safety.

4.2.2. CNS

4.2.2.1. ROLE

Management of health insurance and reimbursement.

4.2.2.2. COLLABORATION NEEDS:

CNS needs to work with Healthcare Providers, the Ministry of Health and Social Security and the UCM to streamline health data exchange for accurate billing and reimbursements. Collaboration with Agence eSanté is necessary to integrate health data into eHealth platforms like the DSP, ensuring that financial and clinical data are synchronized. CNS also interacts with Patients' Associations to improve access to digital tools for managing insurance claims.

4.2.2.3. BALANCING ASPECTS

CNS must balance operational efficiency in healthcare reimbursements with maintaining affordability and accessibility for patients, while aligning with regulatory frameworks for data protection.

4.2.3. AGENCE ESANTÉ

4.2.3.1. ROLE

Coordination and implementation of eHealth infrastructure.

4.2.3.2. COLLABORATION NEEDS

Agence eSanté must collaborate with all stakeholders, particularly CNS, Healthcare Providers and the Ministry of Health and Social Security, to build and maintain a robust, secure and interoperable eHealth platform. It ensures that different systems (clinical, financial and administrative) can communicate with each other. Close cooperation with Professional Associations and Health Professions Council is also necessary to ensure healthcare providers are trained in and using the eHealth systems effectively.

4.2.3.3. BALANCING ASPECTS

Agence eSanté must balance technical demands for system's interoperability and data security with the operational needs of healthcare providers and regulatory compliance.

4.2.4. KEY HEALTHCARE PROVIDERS

4.2.4.1. ROLE

Provision of medical care and services.

4.2.4.2. COLLABORATION NEEDS

Healthcare providers must collaborate with the Ministry of Health and Social Security, CNS and Agence eSanté to ensure that health data is accurately recorded, securely shared and accessible for patient care. Providers work closely with Professional Associations and Patients' Associations to ensure the medical community's interests are aligned with patient safety and satisfaction. Cooperation with Pharmaceutical Industry is also necessary to ensure the smooth digital integration of prescription and medication data.

4.2.4.3. BALANCING ASPECTS

Providers must balance patient care with compliance to eHealth protocols, using technology to improve service delivery while safeguarding patient data.

4.2.5. UCM

4.2.5.1. ROLE

Coordination of sickness funds and insurance.

4.2.5.2. COLLABORATION NEEDS

UCM coordinates with CNS, Healthcare Providers and the Ministry of Health and Social Security to standardize health insurance policies, reimbursement procedures and rates. This collaboration ensures consistency across different insurance funds and smooth integration with the broader eHealth infrastructure. UCM must also work with Patients' Associations to ensure that reimbursement and insurance systems are patient-friendly.

4.2.5.3. BALANCING ASPECTS

UCM must balance the financial sustainability of the insurance system with ensuring equitable access to healthcare for all citizens.

4.2.6. IGSS

4.2.6.1. ROLE

Oversight of social security and healthcare funding.

4.2.6.2. COLLABORATION NEEDS

IGSS works with CNS, UCM and the Ministry of Health and Social Security to ensure financial oversight and that healthcare and social security systems are functioning efficiently. Collaboration with Healthcare Providers and Agence eSanté ensures that accurate data is collected for reporting, analysis and policy-making.

4.2.6.3. BALANCING ASPECTS

IGSS must balance financial oversight with operational flexibility to adapt to new healthcare models, while ensuring the long-term sustainability of the social security system.

4.2.7. LNDS

4.2.7.1. ROLE

To implement Luxembourg's strategies in research, innovation, and digitalization.

4.2.7.2. COLLABORATION NEEDS

LNDS collaborates closely with government, (healthcare) industry, research institutions and citizens to create impactful data projects.

4.2.7.3. BALANCING ASPECTS

LNDS must balance the need for open and accessible data with the requirement to protect personal data and ensure privacy. This involves implementing robust data protection measures and adhering to regulations such as the GDPR.

4.2.8. CNER

4.2.8.1. ROLE

The national ethics body for health studies.

4.2.8.2. COLLABORATION NEEDS

The CNER collaborates with the CNPD, as well as with Research Organizations and Key Healthcare Providers (who act as Principal Investigator within clinical trial studies).

4.2.8.3. BALANCING ASPECTS

The CNER needs to balance ethical considerations by protecting individuals who are participating in health studies, while allowing medical research to advance.

4.2.9. OSIS

4.2.9.1. ROLE

To define both general- and specific cybersecurity guidelines.

4.2.9.2. COLLABORATION NEEDS

OSIS works closely with other government agencies, such as the Ministry of Health, CNS, eSanté, FHL and LUXITH, to coordinate cybersecurity efforts and share best practices.

4.2.9.3. BALANCING ASPECTS

OSIS must balance the need for stringent data protection measures with the requirement to keep health information accessible to authorized personnel. This involves implementing security protocols that do not hinder the day-to-day operations of healthcare providers.

4.2.10. PROFESSIONAL ASSOCIATIONS AND TRADE UNIONS

4.2.10.1. ROLE

Representation of healthcare professionals.

4.2.10.2. COLLABORATION NEEDS:

Professional associations (e.g., AMMD for doctors) must work with Healthcare Providers, the Ministry of Health and Social Security and Agence eSanté to ensure that the needs and concerns of healthcare professionals are reflected in eHealth policies. They play a crucial role in training healthcare professionals to use eHealth systems effectively and in advocating for working conditions that support eHealth adoption.

4.2.10.3. BALANCING ASPECTS

These associations must balance advocacy for professionals' rights with supporting the integration of eHealth innovations to improve healthcare outcomes.

4.2.11. PATIENT (ASSOCIATIONS)

4.2.11.1. ROLE

Representation of patient interests.

4.2.11.2. COLLABORATION NEEDS

Patients and their associations need to work with the Ministry of Health and Social Security, CNS and Healthcare Providers to ensure patient rights, privacy and safety are protected. They also provide feedback on eHealth tools, such as patient portals and digital records and collaborate with Agence eSanté to improve user-friendliness and accessibility.

4.2.11.3. BALANCING ASPECTS

Patients' associations balance advocacy for better healthcare services with supporting digital transformation efforts that improve convenience and efficiency for patients.

4.2.12. HEALTH PROFESSIONS COUNCIL

4.2.12.1. ROLE

Regulation of healthcare professionals.

4.2.12.2. COLLABORATION NEEDS

The Health Professions Council collaborates with the Ministry of Health and Social Security, Healthcare Providers and Professional Associations to ensure that healthcare professionals meet training standards for using eHealth systems. It also ensures that regulations governing the use of digital tools by healthcare professionals are in place.

4.2.12.3. BALANCING ASPECTS

The Council balances the need for high standards in healthcare with the adoption of new technologies that require ongoing professional development.

4.2.13. HEALTH SCIENTIFIC COUNCIL

4.2.13.1. ROLE

To develop and contribute to the implementation of standards of good medical practice.

4.2.13.2. COLLABORATION NEEDS:

Collaboration with various government departments and agencies to ensure policies are evidence-based, working with healthcare providers to implement best practices as well as partnering with research institutions to foster innovation and scientific advancements.

4.2.13.3. BALANCING ASPECTS

Ensuring that new medical technologies and treatments are safe and effective before widespread use.

4.2.14. HEALTH INSPECTION

4.2.14.1. ROLE

Ensuring compliance with health standards.

4.2.14.2. COLLABORATION NEEDS

Health Inspection works with Healthcare Providers, the Ministry of Health and Social Security and Agence eSanté to ensure that health facilities comply with eHealth regulations, data security standards and hygiene protocols. It also ensures that any newly introduced eHealth solution meets public health standards.

4.2.14.3. BALANCING ASPECTS

It must balance regulatory enforcement with supporting the adoption of eHealth innovations in clinical settings.

4.2.15. NATIONAL HEALTH OBSERVATORY

4.2.15.1. ROLE

To guide health decisions and policies and assess their impact by networking data.

4.2.15.2. COLLABORATION NEEDS

Collaboration with health ministries and other government agencies to ensure data is used effectively in policymaking, working with healthcare providers to gather accurate and timely data and partnering with research institutions to conduct studies and analyses.

4.2.15.3. BALANCING ASPECTS

Balancing the need for comprehensive data analysis with the need for timely reporting as well as ensuring that both local and national health trends are adequately addressed.

4.2.16. THE PHARMACEUTICAL INDUSTRY

4.2.16.1. ROLE

Provision of medications and health products.

4.2.16.2. COLLABORATION NEEDS

The pharmaceutical industry collaborates with Healthcare Providers, CNS and Agence eSanté to integrate digital solutions such as ePrescriptions into the healthcare system. It must also work with the Ministry of Health and Social Security and regulatory bodies to ensure compliance with drug safety and digital health regulations.

4.2.16.3. BALANCING ASPECTS

The industry must balance innovation in digital healthcare (e.g., digital drug tracking) with ensuring safety and regulatory compliance in a highly sensitive industry.

4.2.17. ACADEMIC AND RESEARCH INSTITUTIONS

4.2.17.1. ROLE

Research, innovation and education.

4.2.17.2. COLLABORATION NEEDS

Research institutions collaborate with the Ministry of Health and Social Security, Healthcare Providers and Agence eSanté to develop and test new digital health technologies and analyze health data. They work with Healthcare Providers and the population directly to obtain health data. They also provide the educational support necessary for healthcare workers to adopt eHealth solutions effectively.

4.2.18.3. BALANCING ASPECTS

Institutions must balance innovation and research with practical applications of new eHealth technologies in real-world healthcare settings.

4.2.19. PUBLIC HEALTH AND REGULATORY BODIES

4.2.19.1. ROLE

Monitoring and ensuring public health.

4.2.19.2. COLLABORATION NEEDS

Public health bodies work with the Ministry of Health and Social Security, CNS and Healthcare Providers to gather data from eHealth systems for public health monitoring, disease surveillance and crisis response. These bodies ensure that eHealth solutions are used effectively for public health purposes, such as managing pandemics.

4.2.19.2. BALANCING ASPECTS

These bodies balance real-time health surveillance with protecting patient privacy and data security.

4.2.20. CONCLUSION

The success of a unified eHealth strategy in Luxembourg relies on collaboration across all stakeholders, each contributing their expertise to balance regulatory compliance, technical requirements and operational needs. By working together, these stakeholders ensure that eHealth solutions are secure and lead to overall better health outcomes.

5. REGULATORY AND COMPLIANCE CONSIDERATIONS

This chapter will highlight the different regulatory aspects, both on European- and National level.

For a more concise overview, refer to Annex II.

5.1. EUROPEAN REGULATORY FRAMEWORK

The EU has established a comprehensive regulatory framework to ensure the protection of personal data, with specific focus on health data through various regulations, including the EHDS and the GDPR. These regulations aim to balance data protection and sovereignty with the need for secure and efficient data sharing, particularly in the context of eHealth and cross-border healthcare. Below is an outline of the key requirements of these frameworks.

The EHDS will not be discussed in detail once more, as this as already addressed in subchapter 3.1.

5.1.1. GDPR

The GDPR, Regulation (EU) 2016/679, which came into effect in May 2018, is the cornerstone of EU data protection law. It applies to all organizations processing personal data within the EU, including health data.

5.1.1.1. KEY REQUIREMENTS/ASPECTS

- Lawfulness, Fairness and Transparency: Personal data, including health data, must be processed lawfully, fairly and in a transparent manner. Data subjects (in this context: patients) must be informed about how their data is collected and used.
- Data Minimization: Only the data that is necessary for a specific purpose should be collected and processed. This principle is crucial when dealing with sensitive data like health information.
- Consent and Legal Basis: Processing of personal health data requires explicit consent from the individual, unless other legal bases apply (e.g., public health, medical research or vital interest).
- Data Security and Confidentiality: Organizations must implement technical and organizational measures to protect personal data against unauthorized access, breaches or other security risks. This includes encryption and strict access controls for sensitive health data.
- Right of Access, Rectification and Erasure: Data subjects have the right to access their health data, correct inaccuracies and request its deletion under certain conditions (e.g., where the data is no longer necessary for the purpose for which it was collected).
- Data Portability: Patients have the right to transfer their health data between healthcare providers, ensuring continuity of care, especially in cross-border contexts.
- Data Sovereignty and Local Laws: GDPR ensures that EU member states retain some sovereignty over specific types of data, such as health data, through derogations that allow national laws to apply in specific contexts (e.g., public health emergencies).
- Data Protection Officer (DPO): Organizations processing significant amounts of personal data, including health data, must appoint a DPO to oversee compliance with GDPR requirements.

5.1.1.2. RELEVANCE FOR EHEALTH

For eHealth systems, GDPR ensures that patients' personal health data is processed securely and transparently. It emphasizes obtaining explicit consent from patients for the use of their data, particularly when sharing data across healthcare providers or borders.

5.1.2. NIS2 DIRECTIVE

The Network and Information Security (NIS)2 Directive, Directive (EU) 2022/2555, adopted in 2022, updates the previous NIS Directive (2016) to strengthen cybersecurity in key sectors, including healthcare.

5.1.2.1. KEY REQUIREMENTS/ASPECTS

- Cybersecurity Measures: Health organizations must implement adequate cybersecurity measures to protect digital infrastructures against cyber threats. This includes incident response, encryption, access controls and data backups.
- Incident Reporting: Organizations are required to report any cybersecurity incidents (e.g., data breaches) that could affect the availability, confidentiality or integrity of personal health data to relevant authorities.
- Risk Management and Governance: Healthcare providers and eHealth platforms must have appropriate governance frameworks to ensure they can manage cybersecurity risks effectively.

5.1.2.2. RELEVANCE FOR EHEALTH

The NIS2 Directive ensures that the digital infrastructure supporting eHealth is secure, minimizing the risk of cyberattacks that could compromise sensitive health data or disrupt healthcare services.

5.1.3. EPRIVACY DIRECTIVE

The ePrivacy Directive, Directive (EU) 2002/58/EC, which passed in 2002 and was amended in 2009, is a set of rules for data protection and privacy in the EU. It regulates cookie usage, email marketing, data minimization, and other aspects of data privacy.

The ePrivacy Directive has a significant impact on the healthcare sector by emphasizing the confidentiality of communications, requiring consent for cookie usage, promoting data minimization and ensuring transparency in data processing. It also aligns with the GDPR to provide a robust framework for data protection in the EU.

5.1.4. DIRECTIVE ON PATIENTS' RIGHTS IN CROSS-BORDER HEALTHCARE

This EU Directive (2011/24/EU) facilitates patients' access to cross-border healthcare and reinforces patients' rights in relation to receiving healthcare services in other EU countries.

5.1.4.1. KEY REQUIREMENTS/ASPECTS

- Access to Health Data Across Borders: Patients have the right to receive healthcare in another EU country and access their health data from that country. This directive is closely aligned with GDPR and EHDS principles, ensuring that data protection rules are respected even when health data is transferred across borders.
- Reimbursement: The directive establishes rules for the reimbursement of cross-border healthcare services, ensuring that citizens from one EU country can receive care in another EU country and have costs reimbursed by their home country's healthcare system.

5.1.4.2. RELEVANCE FOR EHEALTH

The directive supports the exchange of medical data and the continuity of care for patients traveling or living in multiple EU countries. It is closely connected with the goals of the EHDS and GDPR in terms of data portability and security.

5.1.5. DATA GOVERNANCE ACT

The DGA, Regulation (EU) 2022/868 and adopted in 2022, complements the GDPR by promoting trustworthy mechanisms for data sharing within and across sectors, including healthcare.

5.1.5.1. KEY REQUIREMENTS/ASPECTS

- Data Intermediaries: Organizations that facilitate data sharing, such as eHealth platforms, must operate under strict rules to ensure the security and privacy of the data being exchanged.
- Data Sovereignty: The Act emphasizes that data sharing must respect national laws, ensuring that EU countries retain sovereignty over critical data, including health data.

5.1.5.2. RELEVANCE FOR EHEALTH

The DGA supports the governance of health data exchange, particularly for research and innovation, while ensuring that data protection principles are maintained.

5.1.6. AI ACT

The AI Act, Regulation (EU) 2024/1689 that came into force on the 1st of August 2024, is a comprehensive legal framework introduced by the EU to regulate the development and use of AI systems. It aims to foster innovation while protecting individuals from the potential harms of AI.

5.1.6.1. KEY REQUIREMENTS/ASPECTS

- Risk Classification: The AI Act classifies AI systems into different risk categories, including prohibited, high-risk, and those subject to transparency obligations. High-risk AI systems are subject to stringent requirements, while minimal-risk systems have fewer obligations.
- Transparency and Disclosure: The Act mandates transparency in AI use, requiring that AI systems interacting with humans be clearly identified as such. This ensures that users are informed about AI involvement in decisions that affect them.
- Risk Management: Providers of high-risk AI systems must implement a risk management system that spans the entire life cycle of the AI system. This includes iterative updates and assessments to ensure ongoing compliance and safety.
- Conformity Assessments: AI systems must undergo conformity assessments to verify compliance with the Act's standards. These assessments can be conducted through self-assessment or by third-party notifying bodies, depending on the risk level of the AI system.
- Prohibited Practices: The AI Act outlines specific AI practices that are deemed unacceptable due to their potential risks to European values and fundamental rights. This includes systems that manipulate human behavior, exploit vulnerabilities, or engage in social scoring.
- AI Literacy: Organizations are required to implement AI literacy measures to ensure that individuals and entities understand their rights and obligations under the Act. This includes considering the impact of AI systems on different groups of people.
- Governance and Compliance: The Act establishes a governance framework that includes the European Artificial Intelligence Board and national supervisory authorities. These bodies are responsible for overseeing compliance and providing guidance on the implementation of the Act.

In relation to the healthcare sector, the AI Act has significations implications, including the regulation of high-risk AI systems, the need for transparency and patient consent, and the integration with existing regulations. It aims to promote innovation while ensuring the safe and ethical use of AI in healthcare.

5.1.7. MEDICAL DEVICE REGULATION

The Medical Device Regulation (MDR), Regulation (EU) 2017/745, which entered into force in 2017, has as effective date the 26th of May 2021 and transitional provisions until the 31st of December 2028, is a comprehensive framework introduced by the EU to ensure the safety and efficacy of medical devices. As an example, Clinical Decision Support Systems are considered to be medical devices.

5.1.7.1. KEY REQUIREMENTS/ASPECTS

- Classification of Devices: Medical devices are classified into four risk categories: Class I, Class IIa, Class IIb, and Class III. The classification determines the level of scrutiny and regulatory requirements each device must meet.
- Unique Device Identifier: Each medical device must have a Unique Device Identifier (UDI) to enable better identification, traceability and accountability throughout the supply chain.
- General Safety and Performance Requirements: The MDR includes 23 General Safety and Performance Requirements that cover various aspects of device safety, performance, and risk management. These requirements are more extensive than the previous Essential Requirements under the Medical Device Directive.
- Clinical Evaluation and Post-Market Clinical Follow-Up: Manufacturers must conduct clinical evaluations and post-market clinical follow-ups to demonstrate the safety and performance of their devices. This includes gathering and analyzing data from the use of the device in real-world conditions.
- Quality Management System: Manufacturers must implement a quality management system that ensures compliance with MDR requirements. This system must be maintained and updated throughout the lifecycle of the device.
- Notified Bodies: Notified Bodies are third-party organizations that assess the conformity of medical devices with MDR requirements. Manufacturers must work with Notified Bodies to obtain certification for their devices.
- Technical Documentation: Manufacturers must maintain comprehensive technical documentation for their devices, including design specifications, risk management plans, and clinical evaluation reports. This documentation must be readily available for review by Notified Bodies and regulatory authorities.
- Vigilance and Post-Market Surveillance: Manufacturers are required to implement systems for vigilance and post-market surveillance to monitor the performance of their devices after they are placed on the market. This includes reporting serious incidents and field safety corrective actions.
- EUDAMED Database: The European Database on Medical Devices (EUDAMED) is a central repository for information on medical devices. Manufacturers must register their devices and report relevant data to EUDAMED.
- Transparency and Traceability: The MDR emphasizes transparency and traceability in the supply chain, ensuring that all stakeholders, including healthcare providers and patients, have access to relevant information about medical devices.
- Increased Scrutiny on High-Risk Devices: Devices classified as high-risk (Class III) are subject to more stringent regulatory requirements, including more frequent assessments and closer monitoring by Notified Bodies.

The introduction of the MDR resulted in strict regulatory and approval processes, classification and regulatory control, quality and safety regulations, innovation and compliance, a global regulatory landscape, post-market surveillance and interdisciplinary collaboration. These aspects aim to enhance the safety, efficacy, effectiveness and quality of medical devices, ensuring that patients and healthcare providers have access to high-quality, reliable medical devices.

5.1.8. IN VITRO DIAGNOSTIC REGULATION

The In Vitro Diagnostic Regulation (IVDR), Regulation (EU) 2017/746, entered force in 2017 replacing Directive 98/79/EC and became fully applicable on the 26th of May 2022. The IVDR is a comprehensive set of regulations that govern the clinical investigation, production, and distribution of in vitro diagnostic medical devices in Europe.

5.1.8.1. KEY REQUIREMENTS/ASPECTS

- Classification and Risk Management: The IVDR introduces a risk-based classification system with four risk classes (A, B, C, and D) for in vitro diagnostic medical devices. This classification determines the level of scrutiny and regulatory requirements for each device. Technical documentation and performance evaluation are crucial for conformity assessment. Manufacturers must provide comprehensive technical files and design dossiers for their devices.
- Quality Management and Post-Market Surveillance: Implementing a quality management system (QMS) is essential for ensuring that IVD products are safe and effective. Continuous monitoring of medical device performance through post-market surveillance is crucial for compliance with IVDR standards. This helps in identifying and addressing any issues that arise after the device has been placed on the market.
- UDI: IVD products must comply with specific labeling requirements. This includes proper labeling for human use and ensuring that the labels are accurate and informative. The IVDR emphasizes the importance of UDI for tracking and tracing devices throughout their lifecycle. This helps in improving transparency and safety.
- Clinical Evidence and Performance Evaluation: Manufacturers must provide clinical evidence to support the performance and safety of their IVD devices. This includes data from clinical investigations and performance evaluations. Good Clinical Practice requirements must be followed for data submitted from clinical investigations for IVD device premarket submissions.

Similar to the MDR, the introduction of the IVDR resulted in strict regulatory and approval processes, classification and regulatory control, quality and safety regulations, labeling requirements as well as post-market surveillance. These aspects aim to enhance the safety, efficacy, effectiveness and quality of in vitro diagnostic devices.

5.1.9. CONCLUSION

The GDPR, EHDS and other EU regulations like the NIS2, DGA, AI Act, IVDR and MDR create a strong legal and operational framework for data protection, sovereignty and secure (usage of) health data (exchange) in the EU. Together, they balance the need for efficient and accessible healthcare across the EU with the protection of sensitive health data, ensuring that patients' rights to privacy and security are upheld while enabling innovation and improved healthcare outcomes.

5.2. NATIONAL REGULATIONS

Luxembourg's legal framework concerning data protection, healthcare regulations and the role of national authorities in overseeing compliance is multifaceted and deeply interconnected with both national laws and broader EU directives. The legal context in Luxembourg places significant emphasis on protecting personal health data, ensuring healthcare quality and promoting interoperability within the digital health ecosystem. Below, a more detailed view is described.

5.2.1. DATA PROTECTION LAWS IN LUXEMBOURG

Luxembourg strictly follows the GDPR, which is binding across all EU member states. The country has also enacted specific laws to adapt to the national context and to address specific healthcare-related issues, especially concerning the management and exchange of sensitive health data.

The key regulations and features are documented in the following chapters.

5.2.1.1. GDPR - EU REGULATION 2016/679

Lawfulness of Processing Health Data:

- Health data is classified as sensitive data under GDPR, requiring special protection.
- Processing health data is only lawful under specific conditions, such as explicit consent, when necessary for public health reasons or when required for medical purposes (e.g., patient care, diagnosis, treatment).
- Explicit patient consent is essential, particularly for data sharing in cross-border health scenarios or with third-party providers.

Key Patient Rights Under GDPR:

- Right to Access and Portability: Patients can access their health data and Luxembourg must ensure that data is easily portable (e.g., via eHealth platforms like DSP).
- Right to Erasure (Right to be Forgotten): Patients can request the deletion of their data, although exceptions exist for public health or legal reasons (e.g., long-term medical record retention).
- Data Minimization and Purpose Limitation: Only the necessary amount of data should be collected and used for specific, clear and pre-defined healthcare purposes.

Data Security and Safeguards:

- Encryption and anonymization or pseudonymization of health data are required to protect patient information during electronic exchanges, particularly through eHealth platforms or cross-border data sharing.
- Data Breach Notification: Healthcare providers in Luxembourg must notify the National Commission for Data Protection (CNPD) within 72 hours of any data breach that could jeopardize patient confidentiality.

5.2.1.2. LUXEMBOURG DATA PROTECTION LAW (LAW OF 1 AUGUST 2018)

This law complements the GDPR and adapts specific provisions for Luxembourg's legal context, providing additional national-level enforcement and guidance.

- Specific Provisions on Health Data:
  - The law includes derogations for the processing of health data for research, public health and archival purposes under strict conditions.
  - Healthcare institutions must ensure that DPOs are appointed to oversee compliance and regularly audit data-handling procedures.
- Enforcement and Penalties:
  - The CNPD has the authority to impose significant fines for non-compliance. Penalties can be severe, especially in the case of mishandling sensitive health data.

5.2.1.3. LAW ON ELECTRONIC COMMUNICATIONS AND DATA SECURITY (LAW OF 30 MAY 2005, AS AMENDED)

Confidentiality of Electronic Communications:

- This law ensures that all electronic communication involving health data (e.g., telemedicine, remote monitoring) maintains strict confidentiality.
- Providers offering telehealth or digital consultations must adhere to secure communication standards to protect sensitive health information during remote exchanges.

5.2.2. HEALTHCARE REGULATIONS IN LUXEMBOURG

Luxembourg's healthcare system is governed by several laws and regulations that aim to guarantee high standards of care, patient safety and efficient healthcare delivery. These laws are also crucial for

maintaining the security and privacy of health data, especially as digital health solutions like eHealth and telemedicine become more prominent.

5.2.2.1. LAW ON HOSPITALS AND MEDICAL ESTABLISHMENTS (LAW OF 8 MARCH 2018)

Healthcare Facility Oversight:

- This law regulates the organization, operations and inspection of hospitals and medical institutions. It ensures that hospitals have appropriate digital systems in place to manage patient data securely and comply with Luxembourg's data protection standards.
- Hospitals must integrate with national eHealth systems like the DSP to ensure that patient data can be shared securely across the healthcare network for better coordination of care.

Data Sharing Within Hospitals:

- The law mandates that hospitals adopt standardized EHR systems that are interoperable with national eHealth infrastructure. This ensures seamless sharing of patient records between healthcare professionals.

5.2.2.2. LAW ON PATIENT RIGHTS AND OBLIGATIONS (LAW OF 24 JULY 2014)

Right to Information and Access to Health Records:

- Patients in Luxembourg have the right to access their personal health records, including electronic records. This applies to data stored in national systems like the DSP or in individual hospitals.
- Patients can request that healthcare providers provide information on how their health data is being used, ensuring transparency.

Consent for Data Processing:

- This law reinforces the principle that patients must give informed consent before their health data is processed or shared, except in emergency situations where patient consent cannot be obtained.
- The law also mandates that patients are informed about their rights regarding their data, including how to request access or correction.

5.2.2.3. LAW ON HEALTH PROFESSIONS (LAW OF 10 AUGUST 1991, AS AMENDED)

Professional Standards and Data Management:

- This law governs the licensing and regulation of healthcare professionals in Luxembourg, ensuring that they are qualified to handle sensitive patient data in accordance with the law.
- Healthcare professionals must be trained in data protection practices, particularly when using eHealth systems or accessing shared health records.

5.2.3. ROLE OF NATIONAL AUTHORITIES IN OVERSEEING COMPLIANCE

Several national authorities in Luxembourg are responsible for ensuring that the legal and regulatory frameworks concerning healthcare and data protection are properly implemented and followed.

5.2.3.1. CNPD

Oversight of Data Protection:

- The CNPD is Luxembourg’s independent data protection authority responsible for enforcing GDPR and the national data protection law. It plays a crucial role in overseeing how healthcare providers and institutions manage patient data.
- Responsibilities include:
    - Investigating complaints and ensuring that health data is processed lawfully and securely.

- Auditing healthcare providers, hospitals and eHealth platforms like Agence eSanté to ensure GDPR compliance.
- Imposing penalties for violations of data protection laws, particularly for data breaches or unauthorized sharing of sensitive health information.

- Guidance and Best Practices:
  - CNPD regularly issues guidelines to healthcare providers on data security measures, such as encryption, anonymization and access control systems.

5.2.3.2. MINISTRY OF HEALTH AND SOCIAL SECURITY

Policy and Regulation:

- The Ministry of Health and Social Security is responsible for developing national health policy and ensuring that healthcare providers comply with national laws and regulations. This includes overseeing digital health infrastructure, such as the DSP and coordinating eHealth projects to improve healthcare delivery.
- Responsibilities include:
  - Overseeing the implementation of eHealth solutions across the healthcare sector, ensuring they are interoperable, secure and compliant with both GDPR and national laws.
  - Collaborating with the CNPD and other regulatory bodies to ensure health data is processed in line with legal requirements.
  - Providing public health guidelines that emphasize the safe use of digital health technologies, such as telemedicine and ePrescriptions.

5.2.3.3. IGSS

Supervision of Health Insurance and Social Security:

- The IGSS is responsible for overseeing Luxembourg's social security system, including health insurance and the financial aspects of healthcare. It ensures the smooth operation of reimbursement systems and the secure exchange of health data between insurance providers (like CNS) and healthcare institutions.
- Responsibilities include:
  - Ensuring that data related to healthcare financing, such as patient claims and reimbursements, is securely exchanged between institutions and patients.
  - Auditing the use of health data within insurance claims to prevent fraud and ensure compliance with national regulations on data privacy.

5.2.3.4. AGENCE ESANTÉ

eHealth Infrastructure Coordination:

- Agence eSanté plays a pivotal role in managing Luxembourg's eHealth infrastructure. It oversees the DSP, the national shared health record system and ensures its secure operation in compliance with national and European laws.
- Responsibilities include:
  - Coordinating the integration of healthcare providers into the national eHealth system, ensuring interoperability and secure data sharing across different healthcare systems.
  - Ensuring that health data exchanged through eHealth platforms complies with GDPR and local data protection laws, including encryption and user access control.
  - Supporting the Ministry of Health and Social Security in implementing digital health strategies and promoting the adoption of telemedicine, ePrescriptions and other eHealth innovations.

5.2.3.5. LUXEMBOURG HEALTH PROFESSIONS COUNCIL

Regulation of Healthcare Professionals:

- The Health Professions Council regulates healthcare professionals and ensures that they meet the required standards for handling sensitive health data.
- Responsibilities include:
    - Licensing healthcare providers and ensuring they are trained in data protection practices, particularly in the context of eHealth and telemedicine.
    - Ensuring that healthcare professionals adhere to ethical standards for protecting patient confidentiality and securing health records.

5.2.4. DATA SOVEREIGNTY AND CROSS-BORDER HEALTHCARE

Given Luxembourg's proximity to other EU countries, cross-border healthcare and the secure exchange of health data with neighboring countries are critical concerns.

5.2.4.1. DIRECTIVE 2011/24/EU ON PATIENTS' RIGHTS IN CROSS-BORDER HEALTHCARE

Access to Cross-Border Healthcare:

- Luxembourgish citizens have the right to seek healthcare in other EU countries and their health data can be transferred securely across borders, especially for continuity of care.
- Healthcare providers in Luxembourg must comply with GDPR when transferring patient data across borders and ensure that it is securely exchanged and processed in the receiving country.

Integration with European Systems:

- Luxembourg will need to comply to the EHDS, including the MyHealth@EU aspect, which will facilitate the secure exchange of health data across EU countries, such as ePrescriptions and patient summaries. This requires interoperability between Luxembourg's eHealth platforms and other EU member states' systems.
- National regulations ensure that any cross-border data exchanges respect both Luxembourg's and the EU's strict data protection laws.

5.2.5. CONCLUSION

Luxembourg's legal framework for data protection and healthcare regulations is well-developed, integrating both national laws and EU directives. The framework ensures that health data is processed securely, patients' rights are protected and healthcare providers comply with stringent data security and privacy standards. National authorities like the CNPD, Ministry of Health and Social Security and IGSS play critical roles in overseeing compliance, while healthcare providers, insurance bodies and eHealth platforms like Agence eSanté are required to maintain high levels of data protection and operational efficiency.

6. CHALLENGES IN HARMONIZING COMPLIANCE

Harmonizing compliance in Luxembourg's healthcare system, especially with regard to data protection and eHealth regulations, presents several challenges. These arise primarily from the need to align national regulations with EU regulations and directives, ensure smooth cross-border healthcare and data exchange and manage the complexities of implementing interoperable digital health systems.

Additionally, healthcare providers, regulators, insurers and eHealth platforms must coordinate closely to ensure the lawful and efficient handling of sensitive health data.

A detailed look at the (regulatory) barriers and challenges in harmonizing compliance will be outlined in the next subchapters.

6.1. BARRIERS TO DATA PROTECTION AND PRIVACY

Challenge: Complexity of GDPR implementation and obtaining ethical approval for (usage of) health data.

The GDPR sets high standards for data protection, particularly for sensitive health data, but applying these standards consistently across various healthcare providers, insurers and eHealth platforms can be difficult. GDPR requires:

- Explicit consent from patients for health data processing.
- Strict rules around data minimization and purpose limitation.
- Right to be forgotten and right to portability, which are harder to manage with complex health records.

6.1.1. POTENTIAL BARRIERS

- Interpretation of GDPR Across Sectors: Different healthcare entities (e.g., hospitals, insurance providers) may interpret the application of GDPR requirements differently, leading to inconsistent compliance practices.
- Data Access and Control: Patients may demand control over their health data, but managing access control across multiple healthcare providers can lead to technical and operational complexities.
- Anonymization and Pseudonymization: Ensuring that health data is properly anonymized or pseudonymized for research or public health purposes without compromising patient privacy is difficult.

In addition to the abovementioned challenges in regards to complying with and implementation/interpretation of GDPR requirements, for the secondary usage of health data, ethical approval (or exemption) is required. The process to request an opinion for a new study, or for an

amendment of an existing study is a manual effort and can be rather time-consuming, complex and requires large amounts of paperwork.

While ethical considerations to protect an individual involved in a clinical study is of great importance, timely access to health data for research purposes is equally important and crucial to enhance medical innovations. Both aspects need to be well balanced.

6.1.2. COLLABORATIVE SOLUTIONS

- Joint Guidelines and Standards: Collaborative development of standardized guidelines by CNPD, Agence eSanté, CNER and healthcare providers will ensure uniform GDPR implementation. These guidelines should clarify key aspects like consent management, data retention and anonymization and pseudonymization processes.
- Shared Training Initiatives: Healthcare providers, insurers and tech companies could create joint training programs for staff to ensure a unified understanding of GDPR compliance when handling health data.
- Centralized Consent Management Platforms: Developing a centralized consent management tool within the DSP system would allow patients to easily manage their consent, ensuring GDPR-compliant data access across the system.
- Automate the process to request, review and grant, reject or exempt ethical assessments to new clinical research studies to make it less cumbersome. Create a link to the Centralized Consent Management Platform within the DSP, where individual citizens can consent to sharing their data, also for secondary research purposes, either in anonymized or pseudonymized form. Allow for a broad consent, that the individual consents that their data can be used for any future medical research project, without having to consent for each specific research project.

6.2. INTEROPERABILITY AND DATA EXCHANGE

Challenge: Achieving interoperability across healthcare systems

One of the most significant challenges in eHealth is achieving interoperability between disparate systems. Luxembourg must ensure that health data can be shared securely and efficiently between healthcare providers, insurers and across borders, particularly through platforms like MyHealth@EU.

6.2.1. POTENTIAL BARRIERS

- Different Data Standards: Variations in the data formats and standards used by healthcare providers make it difficult to ensure interoperability between hospitals, clinics and national health databases.
- Cross-Border Healthcare Data Exchange: Differences in regulations and infrastructure between Luxembourg and neighboring countries may slow down cross-border healthcare data sharing.
- Technical Barriers to Integrating Legacy Systems: Older systems used by some healthcare providers may not be easily integrated with new eHealth platforms, requiring significant investments in infrastructure upgrades.

6.2.2. COLLABORATIVE SOLUTIONS

- National Interoperability Framework: Agence eSanté should lead the development of a national interoperability framework in collaboration with Ministry of Health and Social Security, CNS and IT providers. This would standardize data formats, exchange protocols and ensure that all systems can communicate with each other.
- Cross-Border Healthcare Agreements: Luxembourg should actively collaborate with neighboring countries to create specific bilateral agreements that facilitate data exchange under GDPR and cross-border healthcare directives.
- Funding and Support for Legacy System Upgrades: The Ministry of Health and Social Security and IGSS could provide incentives or funding programs for smaller healthcare providers to upgrade outdated systems, ensuring they are compatible with national and EU-level eHealth infrastructures.

6.3 BALANCING DATA SECURITY AND ACCESSIBILITY

Challenge: Ensuring data security while maintaining accessibility for patients and providers

Healthcare data is highly sensitive and maintaining robust security measures (such as encryption and access control), while ensuring that healthcare providers have timely access to data, can be difficult. Cybersecurity risks are increasing, particularly as the reliance on digital health platforms grows.

6.3.1. POTENTIAL BARRIERS

- Striking a Balance Between Security and Usability: Implementing stringent security protocols (e.g., multi-factor authentication, encryption) can slow down access to health records in emergency situations or for cross-border care.
- Cybersecurity Threats: Healthcare organizations are increasingly targeted by cyberattacks. Complying with the NIS2 Directive to ensure cybersecurity is a complex and resource-intensive process.

6.3.2. COLLABORATIVE SOLUTIONS

- Cybersecurity Best Practices Across the Sector: Ministry of Health and Social Security, in collaboration with CNPD and Agence eSanté, should establish national cybersecurity guidelines for healthcare providers, ensuring they adopt secure systems while maintaining usability. This could include minimum encryption standards, threat detection systems and secure data-sharing practices.
- Emergency Access Protocols: Develop specific protocols that allow healthcare providers to quickly access patient records during emergencies, while maintaining GDPR and security compliance. This could include specific exemptions for data access during critical care.
- Sector-Wide Cybersecurity Response Teams: Establish cybersecurity response teams within Luxembourg's healthcare sector, consisting of representatives from CNS, hospitals and Agence eSanté. These teams would coordinate efforts to prevent, detect and respond to cybersecurity incidents.

6.4. CROSS-BORDER DATA EXCHANGE AND SOVEREIGNTY

Challenge: Aligning national data protection rules with EU-wide frameworks

While the GDPR provides a unified framework for data protection across the EU, individual countries like Luxembourg may implement certain derogations (exceptions) for national data sovereignty. Coordinating health data exchange for cross-border healthcare (under Directive 2011/24/EU) with varying national interpretations of GDPR poses a challenge.

6.4.1. POTENTIAL BARRIERS

- Differing National Data Laws: While GDPR applies EU-wide, individual member states have different interpretations or national laws that can affect cross-border data sharing, particularly for healthcare.
- Fragmentation in Cross-Border Healthcare Reimbursement Systems: Differences in healthcare reimbursement rules between countries can make it difficult for patients to access care abroad and have their data and treatment reimbursed smoothly.

6.4.2. COLLABORATIVE SOLUTIONS

- Bilateral and Multilateral Data-Sharing Agreements: Luxembourg should work closely with neighboring countries to establish bilateral agreements that outline clear rules for cross-border data exchange. These agreements should also include provisions for aligning healthcare reimbursement systems.
- Standardizing Cross-Border eHealth Systems: Adherence to the EHDS, including MyHealth@EU will ensure that Luxembourg's eHealth platforms are interoperable with other EU member states. This will streamline data exchange for cross-border care, particularly in managing ePrescriptions and patient summaries.

- Regular Dialogue on Sovereignty Issues: Establish regular dialogues between Luxembourg's CNPD and the Ministry of Health and Social Security with their counterparts in neighboring countries to address data sovereignty concerns and ensure that GDPR is interpreted consistently, especially in cross-border care scenarios.

6.5. HEALTHCARE PROFESSIONALS AND DIGITAL TRANSFORMATION

Challenge: Ensuring healthcare providers are adequately trained and supported

The adoption of eHealth platforms, telemedicine and other digital health solutions requires that healthcare providers are well-versed in using these technologies, while ensuring compliance with complex legal and regulatory frameworks.

6.5.1. POTENTIAL BARRIERS

- Resistance to Adoption: Healthcare professionals may be hesitant to adopt new digital tools due to a lack of training or concerns about the time and effort required to comply with digital data entry and security procedures.
- Varying Levels of Digital Literacy: Different levels of digital literacy among healthcare workers can lead to inconsistent implementation of eHealth solutions and may create potential compliance gaps, particularly in terms of data security.

6.5.2. COLLABORATIVE SOLUTIONS

- Comprehensive Training Programs: Agence eSanté and professional bodies such as the Health Professions Council should develop comprehensive training and certification programs on the use of eHealth platforms, telemedicine and data protection compliance. These programs should be mandatory for healthcare workers to ensure consistent digital literacy across the sector.
- Integration of Digital Tools in Clinical Practice: Healthcare providers should collaborate with digital health providers and CNS to ensure that eHealth tools are seamlessly integrated into daily workflows. This reduces the burden on healthcare professionals and increases adoption.

6.6. CONCLUSION

Harmonizing compliance in Luxembourg's healthcare system, particularly around data protection, interoperability and eHealth adoption, presents several challenges. These challenges are rooted in balancing GDPR requirements, national sovereignty and the operational needs of healthcare providers.

Through collaboration among stakeholders — including the Ministry of Health and Social Security, CNPD, CNS, Agence eSanté, healthcare providers and patients — Luxembourg can overcome these barriers. Coordinated efforts in training, data-sharing agreements, cybersecurity and interoperability standards will ensure a unified, compliant and secure digital healthcare system that aligns with both national and European regulations.

7. PROPOSED APPROACH

Harmonizing compliance across all stakeholders in Luxembourg's healthcare system, particularly concerning data privacy, consent management and cross-border health data sharing, requires a structured pathway that integrates regulatory frameworks, technological solutions and collaborative governance. The goal is to align the operations of healthcare providers, insurers, government bodies and patients with both Luxembourg's national laws and EU regulations, ensuring that health data is securely handled, accessible when needed and properly managed across borders.

The proposed approach for harmonizing compliance is descript in the next sections.

7.1. ESTABLISH A SELF-LEARNING HEALTH SYSTEM

Objective: Create a self-leaning healthcare system, in which high-quality health data is (securely and in adherence with all relevant regulations) transferred from care- to research institutions, accelerating medical innovation and returning new insights back to the healthcare providers to enhance patient wellbeing.

The two concrete use-cases as part of the DS4H PoC, for diabetes and oncology respectively, intend to demonstrate how exchange of health data from care- to research institutions allows for data-driven (AI) innovations, from which the actual patient seen in the care institute can ultimately benefit (in the future).

7.1.1. KEY ACTIONS

1. Promote a Culture of Continuous Learning:
   - Foster a culture of continuous learning and improvement among healthcare providers.
   - Encourage the use of data and analytics to drive decision-making and improve patient care.
2. Engage Stakeholders in the Self-Learning Process:
   - Involve healthcare providers, researchers and patients in the self-learning process.
   - Create feedback loops to continuously gather and apply evidence in real-time to guide care.
3. Enhance Data Governance and Security:
   - Strengthen data governance policies to ensure the secure and ethical use of health data.
   - Implement robust security measures to protect patient data and maintain compliance with regulatory standards.
4. Foster Collaboration and Innovation:
   - Encourage collaboration among healthcare providers, researchers, and technology partners.

- Support innovative projects that leverage data-driven insights to improve healthcare delivery and patient outcomes.

7.1.2. BENEFITS

This will close the loop between primary use of health data on one hand, and secondary use of health data on the other hand – and thus goes beyond EHDS.

7.2. ESTABLISH A MULTI-STAKEHOLDER GOVERNANCE FRAMEWORK

Objective: Create a centralized governance structure to oversee the alignment of data privacy, consent management and cross-border data sharing across all stakeholders, ensuring transparency, accountability and consistency.

7.2.1. KEY ACTIONS

7.2.1.1. FORM A NATIONAL EHEALTH STEERING COMMITTEE

Members: Ministry of Health and Social Security, CNS, Agence eSanté, CNPD, Healthcare Providers, Patients' Associations and Professional Councils.

Role: Oversee the harmonization of regulatory compliance, propose unified standards and ensure continuous alignment between national and EU regulations (e.g., GDPR, EHDS).

Responsibilities:

- Develop a national roadmap for eHealth compliance, including data privacy, consent management and cross-border sharing.
- Monitor the integration of digital health tools and ensure ongoing collaboration between stakeholders.

7.2.1.2. APPOINT A COMPLIANCE TASK FORCE

Role: Ensure GDPR and EHDS compliance across all sectors.

Responsibilities: Provide recommendations on how to integrate best practices on data protection into daily healthcare operations, oversee audits and address potential regulatory barriers.

7.2.2. BENEFITS:

This centralized governance framework will streamline decision-making and ensure that all stakeholders work together under a unified approach, preventing fragmented compliance efforts.

It is expected that over time, in line with the EHDS implementation, this will be addressed (to a certain extend).

7.3. DEVELOP A NATIONAL STANDARD FOR CONSENT MANAGEMENT

Objective: Implement a centralized consent management system that complies with GDPR requirements and allows patients to control access to their health data across different healthcare providers and systems, both nationally and cross-border.

7.3.1. KEY ACTIONS

7.3.1.1. IMPLEMENT A CENTRALIZED CONSENT MANAGEMENT SYSTEM (CMS)

Lead: Agence eSanté in collaboration with CNPD and Ministry of Health and Social Security.
Role: Enable patients to manage their consent for data access in real-time, through an online platform (integrated with the DSP).
Functionality:

- Patients can view, grant or withdraw consent for healthcare providers to access specific health records. Also for secondary usage of their health data, patients should have the possibility within the CMS to content (or not) to sharing their data for research purposes, either in anonymized or pseudonymized form, as well as being able to choose to give consent for a specific research project, or rather a broad consent.
- Patients can give consent for cross-border sharing of health data in compliance with Directive 2011/24/EU.
- Consent status is updated across all healthcare providers in real-time to ensure that only authorized personnel has access to patient data.

7.3.1.2. STANDARDIZE CONSENT FORMS AND PROCEDURES

- Develop standardized, multilingual consent forms (aligned with GDPR) for both national and cross-border healthcare.
- Ensure that patients understand their rights and the scope of data sharing, with simple opt-in/opt-out mechanisms.

7.3.1.3. CREATE AWARENESS CAMPAIGNS FOR PATIENTS AND PROVIDERS

- Run public awareness campaigns to educate patients on how to manage their health data and rights under GDPR.
- Train healthcare providers on how to integrate the CMS into their workflows.

7.3.2. BENEFITS

A centralized consent management system provides transparency for patients, enhances their control over personal data and ensures legal compliance across national and cross-border healthcare environments.

Although patient consent will be a central aspect of the EHDS, this proposal will go beyond the expected minimal requirements from the regulation.

7.4. ENSURE INTEROPERABILITY AND SECURE CROSS-BORDER HEALTH DATA SHARING

7.4.1. OBJECTIVE

Enable interoperable and secure health data exchange within Luxembourg and across EU borders, ensuring that healthcare providers can access and share patient data securely when needed, particularly for cross-border healthcare services.

7.4.2. KEY ACTIONS

7.4.2.1. ADOPT COMMON DATA STANDARDS FOR INTEROPERABILITY

Lead: Agence eSanté and Ministry of Health and Social Security, in collaboration with EU bodies (e.g., MyHealth@EU)

- Implement EU-wide health data standards (HL7 FHIR, ICD, SNOMED CT) for EHRs to ensure interoperability and compatibility with cross-border health systems.
- Ensure that all healthcare providers in Luxembourg adopt these standards for easy data sharing across systems.

7.4.2.2. STRENGTHEN CROSS-BORDER DATA EXCHANGE INFRASTRUCTURE

- Integrate Luxembourg's national eHealth systems (DSP, ePrescriptions) with the MyHealth@EU platform to facilitate secure cross-border data sharing.
- Ensure real-time exchange of patient summaries, ePrescriptions and diagnostic data with healthcare providers in other EU member states, ensuring compliance with GDPR and EHDS.
- Adopt EU Digital COVID Certificate infrastructure as a model for future cross-border health data sharing.

7.4.2.3. ESTABLISH CROSS-BORDER DATA-SHARING AGREEMENTS

- Work with neighboring countries to establish bilateral or multilateral agreements that define clear protocols for secure data sharing in line with GDPR and national data sovereignty laws.
- These agreements should include specific provisions on data handling, consent requirements and secure data transfer protocols.

7.4.2.4. ENHANCE DATA SECURITY MEASURES

- Implement end-to-end encryption for all cross-border data exchanges, ensuring secure data transmission and storage.
- Adopt multi-factor authentication (MFA) and role-based access control for healthcare providers accessing patient data from other EU countries.
- Regularly audit cross-border data-sharing processes to identify vulnerabilities and ensure compliance with NIS2 Directive on cybersecurity.

7.4.3. BENEFITS

Interoperable and secure data sharing ensures that patients receive seamless healthcare, whether in Luxembourg or abroad. This approach promotes continuity of care while maintaining stringent data protection standards.

It is expected that this proposal is within the scope of the future EHDS implementation.

7.5. CREATE A COMPREHENSIVE TRAINING PROGRAM FOR STAKEHOLDERS

7.5.1. OBJECTIVE

Equip healthcare providers, administrative staff and IT personnel with the knowledge and skills required to manage patient data securely, comply with GDPR and utilize cross-border health data sharing systems effectively.

7.5.2. KEY ACTIONS

7.5.2.1 DEVELOP EHEALTH COMPLIANCE TRAINING MODULES

Lead: Health Professions Council and CNPD, in collaboration with Agence eSanté**.**

- Develop tailored training programs for different stakeholder groups (healthcare providers, insurers, IT staff) on topics such as:
  - GDPR compliance for health data.
  - Use of the centralized consent management system.
  - Secure data-sharing practices, both nationally and cross-border.
  - Cybersecurity protocols for protecting health data.

7.5.2.2. CONDUCT MANDATORY WORKSHOPS AND CERTIFICATIONS

- Ensure that all healthcare providers undergo mandatory training and certification on data privacy, consent management and cross-border data sharing.
- IT professionals responsible for maintaining eHealth platforms should receive specialized training on cybersecurity and data encryption technologies.

7.5.2.3. CONTINUOUS EDUCATION AND UPDATES

- Provide regular updates and refresher courses on emerging trends in data protection and new regulatory requirements (e.g., updates to EHDS or GDPR amendments).
- Collaborate with EU bodies to ensure alignment with new cross-border healthcare protocols.

7.5.3. BENEFITS

This ensures that all stakeholders are equipped with the necessary skills to manage patient data responsibly, comply with regulations and use digital health tools effectively, minimizing compliance risks. It is expected that this goes beyond the EHDS Implementation.

7.6. ESTABLISH CONTINUOUS MONITORING, AUDITING AND FEEDBACK MECHANISMS

7.6.1. OBJECTIVE

Set up continuous monitoring and auditing processes to ensure that data privacy, consent management and cross-border data-sharing protocols are followed consistently and adjusted as necessary.

7.6.2. KEY ACTIONS

7.6.2.1. IMPLEMENT A COMPLIANCE MONITORING SYSTEM

Lead: CNPD in collaboration with the Ministry of Health and Social Security and Agence eSanté**.**

- Develop a real-time monitoring system that tracks data access, consent updates and data-sharing activities to detect non-compliance or security risks.
- Set up automated alerts for unauthorized access attempts or breaches of GDPR rules.

7.6.2.2. CONDUCT REGULAR AUDITS AND ASSESSMENTS

- Perform annual audits of healthcare providers, insurers and eHealth platforms to ensure adherence to GDPR, EHDS and cross-border data-sharing regulations.
- Use audit findings to make continuous improvements to the consent management system, data security protocols and interoperability standards.

7.6.2.3. FEEDBACK LOOPS WITH STAKEHOLDERS

- Create regular feedback sessions with patients, healthcare providers and regulators to gather insights on the effectiveness of the compliance framework.
- Use feedback to refine data-sharing protocols, update consent management tools and address emerging compliance challenges.

7.6.3. BENEFITS

Continuous monitoring, auditing and feedback mechanisms ensure that the system remains compliant with evolving regulations and that stakeholders are consistently aligned with best practices in data privacy and security.

It is expected that over time, in line with the EHDS implementation, this will be addressed (to a certain extend).

7.7. CONCLUSION: A PATHWAY FOR HARMONIZING COMPLIANCE

By establishing a self-learning healthcare system and a centralized governance framework, implementing a centralized consent management system, ensuring interoperability and secure cross-border data sharing, providing comprehensive training and setting up monitoring mechanisms, Luxembourg can harmonize compliance across all stakeholders. This approach not only ensures GDPR and EHDS compliance but also fosters trust and collaboration among healthcare providers, patients and national authorities, enabling efficient and secure healthcare delivery.

8. CONCLUSION

This concluding chapter summarizes the key outcomes, opportunities and proposed approaches to overcome challenges, which will ensure the successful implementation of the DS4H project and *may* lay the grounds for the future EHDS implementation.

The DS4H project represents a significant step forward in Luxembourg's journey towards a more integrated, efficient and secure healthcare system. By leveraging the EHDS and Gaia-X initiatives, the project aims to create a harmonized Health Data Space that facilitates secure data exchange, enhances healthcare delivery and fosters medical innovation.

The EHDS and Gaia-X have common goals, notably in regards to data sovereignty, security and privacy and interoperability aspects. EHDS *could* rely on Gaia-X to be the technical backbone by providing the technical infrastructure for storing, processing and exchanging health data across borders.

In the context of Luxembourg, both in regards to the digital health infrastructure as well as relevant stakeholders, there is a large variety of entities, both public and private, with different roles and responsibilities, collaborative needs and balancing aspects. The limited size of the country allows for shorter lines of communication (and constructive collaboration), making Luxembourg uniquely positioned to pioneer in creating the Health Data Space.

Even though there are numerous European- and Luxembourgish regulations that need to be adhered to, also through the upcoming EHDS, there is a significant paradigm shift to in a secure, sensible, ethical and meaningful way create value from usage of health data with the aim to ultimately improve patient care.

Identified challenges include barriers to data protection and privacy, interoperability and data exchange, balancing data security and accessibility, cross-border data exchange and sovereignty as well as healthcare professionals within the digital transformation.

Approaches to overcome these challenges consist of establishing a self-learning health system as well as a multi-stakeholder governance framework, developing a national standard for consent management, ensuring national interoperability and secure cross-border health data sharing, creating a comprehensive training program for stakeholders and finally by establishing continuous monitoring, auditing and feedback mechanisms.

In conclusion, there is a large long-tern potential for Luxembourg(‘s healthcare system) by creating a Health Data Space in Luxembourg with a clear governance and by adhering to all relevant regulations. The Health Data Space stimulates and allows for constructive collaboration between both care institutions amongst each other (and thus primary use of health data), between care- and research institutions (and thus secondary use of health data) and finally returning medical innovation from research- to care institutions (and thus closing the loop between primary- and secondary use of health data). This not only has the potential to ultimately improve patient care, but also to foster innovation and thus allows economic growth and attracting investment.

ANNEX I

Who	Role	Responsibility	Collaboration Needs	Balancing aspects
Ministry of Health and Social Security	The central governmental authority responsible for setting health policy, regulating the healthcare system, overseeing public health programs and ensuring the quality and safety of healthcare services in Luxembourg.	To supervises hospitals, healthcare professionals, medical products and public health campaigns. It also leads the response to health crises (e.g., pandemics) and ensures the implementation of eHealth strategies.	The Ministry must provide clear leadership and policy direction while ensuring that regulations related to data privacy, security and public health are enforced. It works with CNS, Agence eSanté and Healthcare Providers to integrate these policies into day-to-day healthcare operations. The Ministry also needs to collaborate with Professional- and Patient Associations and the Pharmaceutical Industry to ensure that the needs of all stakeholders are considered when establishing eHealth policies.	The Ministry balances regulatory compliance with innovation, ensuring that Luxembourg's healthcare system embraces new technologies without compromising on quality and safety.
CNS	The national public health insurance fund, covering the majority of the population under the compulsory health insurance.	To manage healthcare reimbursements for medical services, prescriptions, hospital stays and other healthcare-related expenses. The CNS also negotiates tariffs with healthcare providers and ensures that medical services remain accessible and affordable.	CNS needs to work with Healthcare Providers, the Ministry of Health and Social Security and the UCM to streamline health data exchange for accurate billing and reimbursements. Collaboration with Agence eSanté is necessary to integrate health data into eHealth platforms like the DSP, ensuring that financial and clinical data are synchronized. CNS also interacts with Patients' Associations to improve access to digital tools for managing insurance claims.	CNS must balance operational efficiency in healthcare reimbursements with maintaining affordability and accessibility for patients, while aligning with regulatory frameworks for data protection.
Agence eSanté	The national eHealth agency that coordinates and manages the digital infrastructure of Luxembourg's healthcare system, including the DSP.	To oversee the secure exchange of patient health data, facilitate interoperability between healthcare systems, ensure data privacy and support eHealth initiatives like telemedicine. In regards to the EHDS, Agence eSanté is responsible for the primary use of data.	Agence eSanté must collaborate with all stakeholders, particularly CNS, Healthcare Providers and the Ministry of Health and Social Security, to build and maintain a robust, secure and interoperable eHealth platform. It ensures that different systems (clinical, financial and administrative) can communicate with each other. Close cooperation with Professional Associations and Health Professions Council is also necessary to ensure healthcare providers are trained in and using the eHealth systems effectively.	Agence eSanté must balance technical demands for system's interoperability and data security with the operational needs of healthcare providers and regulatory compliance.
Key healthcare providers	Public and private hospitals, specialized centres	To provide secondary and tertiary care services.	Healthcare providers must collaborate with the Ministry of Health and Social Security, CNS and Agence eSanté to ensure that health data is accurately recorded, securely shared and accessible for patient care. Providers work closely with Professional- and Patient Associations to ensure the medical community's interests are aligned with patient safety and satisfaction. Cooperation with Pharmaceutical Industry is also necessary to ensure the smooth digital integration of prescription and medication data. Finally, healthcare providers collaborate with the Health Professions Counsil for licensing and qualifications and with the Health Scientific Council for good medical practices.	Providers must balance patient care with compliance to eHealth protocols, using technology to improve service delivery while safeguarding patient data.
	Primary Care Physicians (GPs)	To act as the first point of contact for patients. To play a critical role in diagnosing and referring patients to specialists or hospitals.		
	Specialists	To provide secondary care either within hospitals or in private practices.		
	Pharmacies	To dispense medications, provide advice on drug use and contribute to public health efforts such as vaccinations.		
	Private and public laboratories	To take and analyse clinical specimens to obtain information about the health of a patient to aid in diagnosis, treatment, and prevention of disease.		
	Different institutions (elderly care, disabilities etc.)	To assist with activities of daily living, such as bathing, dressing, and medication management.		
	Other healthcare professionals	To carry out various tasks to contribute to the healthcare system.		
UCM	To coordinate the different sickness funds in Luxembourg.	To negotiate the terms of care, reimbursement and tariffs between healthcare providers and insurance fund and to contribute to the financial sustainability of the healthcare system.	UCM coordinates with CNS, Healthcare Providers and the Ministry of Health and Social Security to standardize health insurance policies, reimbursement procedures and rates. This collaboration ensures consistency across different insurance funds and smooth integration with the broader eHealth infrastructure. UCM must also work with Patients' Associations to ensure that reimbursement and insurance systems are patient-friendly.	UCM must balance the financial sustainability of the insurance system with ensuring equitable access to healthcare for all citizens.
IGSS	To oversee the functioning of the social security system, including healthcare.	To monitor the financial stability and performance of the healthcare system, ensuring compliance with national regulations and standards in health and social protection.	IGSS works with CNS, UCM and the Ministry of Health and Social Security to ensure financial oversight and that healthcare and social security systems are functioning efficiently. Collaboration with Healthcare Providers and Agence eSanté ensures that accurate data is collected for reporting, analysis and policy-making.	IGSS must balance financial oversight with operational flexibility to adapt to new healthcare models, while ensuring the long-term sustainability of the social security system.
LNDS	To implement Luxembourg's strategies in research, innovation, and digitalization.	To enable value creation from secondary use of data, for public and private partners and support the sharing and re-use of public sector data, in a trustable manner. In regards to the EHDS, LNDS has a leading role for the country's implementation in terms of secondary use of data.	LNDS collaborates closely with government, (healthcare) industry, research institutions and citizens to create impactful data projects.	LNDS must balance the need for open and accessible data with the requirement to protect personal data and ensure privacy. This involves implementing robust data protection measures and adhering to regulations such as the GDPR.
CNER	The national ethics body for health studies.	To protect persons participating in a health study by providing an opinion concerning the ethical acceptability of projects (such as clinical trials) submitted to it.	The CNER collaborates with the CNPD, as well as with Research Organizations and Key Healthcare Providers (who act as Principal Investigator within clinical trial studies).	The CNER needs to balance ethical considerations by protecting individuals who are participating in health studies, while allowing medical research to advance.
OSIS	OSIS was created by the Ministry of Health within a national cybersecurity framework. Its goal is to facilitate discussions on cybersecurity and the various entities involved.	To define both general- and specific cybersecurity guidelines for hospitals and "transversal" structures (such as LUXITH or eSanté).	OSIS works closely with other government agencies, such as the Ministry of Health, CNS, eSanté, FHL and LUXITH, to coordinate cybersecurity efforts and share best practices.	OSIS must balance the need for stringent data protection measures with the requirement to keep health information accessible to authorized personnel. This involves implementing security protocols that do not hinder the day-to-day operations of healthcare providers.
Professional Associations and Trade Unions	AMMD	To represents doctors and dentists and involved in negotiations regarding tariffs and working conditions.	Professional associations and Trade Unions must work with Healthcare Providers, the Ministry of Health and Social Security and Agence eSanté to ensure that the needs and concerns of healthcare professionals are reflected in eHealth policies. They play a crucial role in training healthcare professionals to use eHealth systems effectively and in advocating for working conditions that support eHealth adoption.	These associations must balance advocacy for professionals' rights with supporting the integration of eHealth innovations to improve healthcare outcomes.
	FHL	To represents the interests of hospitals and healthcare institutions in Luxembourg,		
	Healthcare Workers' Unions	To represent various healthcare professionals, advocating for their working conditions, salaries and professional development.		
Patient (Associations)	Patients	At the centre of the healthcare system, with rights to access high-quality care, reimbursement for medical services and involvement in healthcare decisions.	Patients and their associations need to work with the Ministry of Health and Social Security, CNS and Healthcare Providers to ensure patient rights, privacy and safety are protected. They also provide feedback on eHealth tools, such as patient portals and digital records and collaborate with Agence eSanté to improve user-friendliness and accessibility.	Patients' associations balance advocacy for better healthcare services with supporting digital transformation efforts that improve convenience and efficiency for patients.
	Patient Associations	To represent patients with specific health conditions, advocating for better care, support and research.		
	National Health Information and Mediation Service	To provide information, advice, as well as conflict prevention and resolution between healthcare providers and patients.		
Conseil Supérieur des Professions de Santé	Regulating the licensing, qualifications and ethical practices of healthcare professionals, including doctors, nurses and pharmacists.	To ensure that healthcare providers meet the required standards for professional practice and patient safety.	The Health Professions Council collaborates with the Ministry of Health and Social Security, Healthcare Providers and Professional Associations to ensure that healthcare professionals meet training standards for using eHealth systems. It also ensures that regulations governing the use of digital tools by healthcare professionals are in place.	The Council balances the need for high standards in healthcare with the adoption of new technologies that require ongoing professional development.
Conseil scientifique du domaine de la santé	To develop and contribute to the implementation of standards of good medical practice.	To promote high-quality care, to guide healthcare professionals in the development of good practices and to make optimal use of available resources.	Collaboration with various government departments and agencies to ensure policies are evidence-based, working with healthcare providers to implement best practices as well as partnering with research institutions to foster innovation and scientific advancements.	Ensuring that new medical technologies and treatments are safe and effective before widespread use.
Division de l'Inspection Sanitaire	Responsible for inspecting and ensuring the hygiene, safety and compliance of healthcare institutions.	To oversee the licensing of healthcare facilities, investigate complaints and enforce public health laws.	Health Inspection works with Healthcare Providers, the Ministry of Health and Social Security and Agence eSanté to ensure that health facilities comply with eHealth regulations, data security standards and hygiene protocols. It also ensures that any newly introduced eHealth solution meets public health standards.	It must balance regulatory enforcement with supporting the adoption of eHealth innovations in clinical settings.
L'Observatoire national de la santé	To guide health decisions and policies and assess their impact by networking data.	To evaluate the population health status, publish and disseminate these findings and to propose improvements to the population's health status and the health system.	Collaboration with health ministries and other government agencies to ensure data is used effectively in policymaking, working with healthcare providers to gather accurate and timely data and partnering with research institutions to conduct studies and analyses.	Balancing the need for comprehensive data analysis with the need for timely reporting as well as ensuring that both local and national health trends are adequately addressed.
The Pharmaceutical Industry	To provide medications and treatments to healthcare providers in Luxembourg,	Involvement in research, development, manufacturing and the distribution of pharmaceutical products, as well as negotiating pricing and reimbursement conditions with the CNS.	The pharmaceutical industry collaborates with Healthcare Providers, CNS and Agence eSanté to integrate digital solutions such as ePrescriptions into the healthcare system. It must also work with the Ministry of Health and Social Security and regulatory bodies to ensure compliance with drug safety and digital health regulations.	The industry must balance innovation in digital healthcare (e.g., digital drug tracking) with ensuring safety and regulatory compliance in a highly sensitive industry.
Academic and Research Institutions	To contribute to medical research, healthcare innovation and the training of healthcare professionals.	To engage in research activities in areas like biotechnology, health data and medical science.	Research institutions collaborate with the Ministry of Health and Social Security, Healthcare Providers and Agence eSanté to develop and test new digital health technologies and analyse health data. They work with Healthcare Providers and the population directly to obtain health data. They collaborate with CNER to obtain ethical approval. They also provide the educational support necessary for healthcare workers to adopt eHealth solutions effectively.	Institutions must balance innovation and research with practical applications of new eHealth technologies in real-world healthcare settings.
Direction de la Santé Publique	To define public health objectives and contribute to the national health strategy.	To develop and manage national health plans and interact with all healthcare system partners. To provide awareness, screening, and surveillance services. To ensure access, quality, and safety of healthcare. To guarantees compliance with applicable laws, regulations, and standards. To support the development of effective public health policies.	Public health bodies work with the Ministry of Health and Social Security, CNS and Healthcare Providers to gather data from eHealth systems for public health monitoring, disease surveillance and crisis response. These bodies ensure that eHealth solutions are used effectively for public health purposes, such as managing pandemics.	These bodies balance real-time health surveillance with protecting patient privacy and data security.

ANNEX II

Level	What	Brief description	Key Requirements/aspects	Relevance for eHealth
European	EHDS - European Health Data Space, Regulation (EU) 2025/327	To create a framework for the secure and efficient sharing of health data within and across EU member states. It is designed to facilitate both primary use (clinical care) and secondary use (research, policymaking and innovation) of health data, while ensuring high levels of privacy and security.	Empowerment of Individuals (access to portable personal health data), Improved Healthcare Delivery (cross-border healthcare and interoperability standards), Data for Research and Innovation (secondary use of health data and data-driven health solutions) and Privacy and Security (GDPR compliance and data sovereignty)	The EHDS plays a pivotal role in advancing eHealth by creating a secure, interoperable and patient-centric framework for health data exchange across the EU.
European	GDPR - General Data Protection Regulation, (EU) 2016/679	The cornerstone of EU data protection law. It applies to all organizations processing personal data within the EU, including health data	Lawfulness, Fairness and Transparency, Data Minimization, Consent and Legal Basis, Data Security and Confidentiality, Right of Access, Rectification and Erasure, Data Portability, Data Sovereignty and Local Laws and requirement of an Data Protection Officer	To ensure that patients' personal health data is processed securely and transparently. To emphasize obtaining explicit consent from patients for the use of their data, particularly when sharing data across healthcare providers or borders
European	NIS2 - Network and Information Security 2 Directive, (EU) 2022/2555	Directive to strengthen cybersecurity in key sectors, including healthcare	Cybersecurity Measures, Incident Reporting and Risk Management and Governance	The NIS2 Directive ensures that the digital infrastructure supporting eHealth is secure, minimizing the risk of cyberattacks that could compromise sensitive health data or disrupt healthcare services.
European	ePrivacy Directive, (EU) 2002/58/EC	Directive focused on privacy and electronic communications, complementing the GDPR by specifically addressing the confidentiality of communications and the tracking of user behaviour online	Explicit User Consent for cookie usage, email marketing, data minimization and other aspects of data privacy	To emphasize the confidentiality of communications, requiring consent for cookie usage, promoting data minimization and ensuring transparency in data processing. It also aligns with the GDPR to provide a robust framework for data protection in the EU.
European	Patients' Rights in Cross-Border Healthcare, Directive 2011/24/EU	Directive to facilitate patients' access to cross-border healthcare and to reinforce patients' rights in relation to receiving healthcare services in other EU countries	Access to Health Data Across Borders and reimbursements for cross-border healthcare services	The directive supports the exchange of medical data and the continuity of care for patients traveling or living in multiple EU countries. It is closely connected with the goals of the EHDS and GDPR in terms of data portability and security.
European	DGA - Data Governance Act, Regulation (EU) 2022/868	Regulation that complements the GDPR by promoting trustworthy mechanisms for data sharing within and across sectors, including healthcare	Data Intermediaries and Data Sovereignty	The DGA supports the governance of health data exchange, particularly for research and innovation, while ensuring that data protection principles are maintained.
European	AI Act, Regulation (EU) 2024/1689	A comprehensive legal framework introduced by the EU to regulate the development and use of AI systems. It aims to foster innovation while protecting individuals from the potential harms of AI.	Risk Classification, Transparency and Disclosure, Risk Management, Conformity Assessments, Prohibited Practices, AI Literacy and Governance and Compliance	In relation to the healthcare sector, the AI Act has significations implications, including the regulation of high-risk AI systems, the need for transparency and patient consent, and the integration with existing regulations. It aims to promote innovation while ensuring the safe and ethical use of AI in healthcare.
European	MDR - Medical Device Regulation, (EU) 2017/745	A comprehensive framework introduced by the EU to ensure the safety and efficacy of medical devices.	Classification of Devices, Unique Device Identifier, General Safety and Performance Requirements, Clinical Evaluation and Post-Market Clinical Follow-Up, Quality Management System, Notified Bodies, Technical Documentation, Vigilance and Post-Market surveillance, EUDAMED Database, Transparency and Traceability and Increased Scrutiny on High-Risk Devices	The introduction of the MDR resulted in strict regulatory and approval processes, classification and regulatory control, quality and safety regulations, innovation and compliance, a global regulatory landscape, post-market surveillance and interdisciplinary collaboration. These aspects aim to enhance the safety, efficacy, effectiveness and quality of medical devices, ensuring that patients and healthcare providers have access to high-quality, reliable medical devices.
European	IVDR - In Vitro Diagnostic Regulation, (EU) 2017/746	The In Vitro Diagnostic Medical Devices Regulation (EU) 2017/746 (IVDR) governs the placing on the market and use of in vitro diagnostic devices within the European Union. It replaces Directive 98/79/EC and aims to enhance patient safety by introducing stricter requirements for clinical evidence, risk classification, transparency, and post-market surveillance.	The IVDR introduces a risk-based classification system, stricter conformity assessments, and reinforced clinical performance evaluation. It requires EUDAMED registration and post-market surveillance. In-house devices are allowed under specific conditions if no CE-marked equivalent exists.	The IVDR applies to diagnostic software, including AI tools. Hospital-developed digital tests fall under Article 5(5). The regulation promotes traceability, security, and interoperability with health IT systems,
National	Luxembourg Data Protection Law (Law of 1 August 2018)	Law that complements the GDPR and adapts specific provisions for Luxembourg's legal context, providing additional national-level enforcement and guidance.	The law includes derogations for the processing of health data for research, public health and archival purposes under strict conditions. Healthcare institutions must ensure that DPOs are appointed to oversee compliance and regularly audit data-handling procedures. The CNPD has the authority to impose significant fines for non-compliance. Penalties can be severe, especially in the case of mishandling sensitive health data.	
National	Law on Electronic Communications and Data Security (Law of 30 May 2005, as amended)	Law that ensures that all electronic communication involving health data (e.g., telemedicine, remote monitoring) maintains strict confidentiality.	Providers offering telehealth or digital consultations must adhere to secure communication standards to protect sensitive health information during remote exchanges.	
National	Law on Hospitals and Medical Establishments (Law of 8 March 2018)	Law that regulates the organization, operations and inspection of hospitals and medical institutions. It ensures that hospitals have appropriate digital systems in place to manage patient data securely and comply with Luxembourg's data protection standards.	Hospitals must integrate with national eHealth systems like the DSP to ensure that patient data can be shared securely across the healthcare network for better coordination of care. The law furthermore mandates that hospitals adopt standardized EHR systems that are interoperable with national eHealth infrastructure. This ensures seamless sharing of patient records between healthcare professionals	
National	Law on Patient Rights and Obligations (Law of 24 July 2014)	Law that allows patients to access their personal health records, including electronic records. This applies to data stored in national systems like the DSP or in individual hospitals. Patients can request that healthcare providers provide information on how their health data is being used, ensuring transparency	This law reinforces the principle that patients must give informed consent before their health data is processed or shared, except in emergency situations where patient consent cannot be obtained. The law also mandates that patients are informed about their rights regarding their data, including how to request access or correction	