Building a Resilient European Health Data Space: Advancing Interoperability and Cybersecurity for a Safe and Innovative Health Union

Introduction

The European healthcare landscape is undergoing a profound transformation, driven by digital health technologies and an increasing reliance on data-driven approaches. With the implementation of the European Health Data Space (EHDS) on the horizon, interoperability and cybersecurity have emerged as critical pillars when it comes to ensuring the effective and secure exchange of health data across borders. The EHDS represents a significant leap forward in the integration and utilisation of health data across the European Union, potentially serving as a global model for data transfer and healthcare digitalisation.

COCIR recognises the vital role that interoperability and cybersecurity play in that transformation. Health systems increasingly rely on digital technologies to enhance patient care, streamline operations and foster innovation. Therefore, ensuring seamless data exchange (interoperability) while safeguarding sensitive information and availability of systems (cybersecurity) is of utmost importance and cannot be overstated.

Rapid advancements in health technologies, including the adoption of Application Programming Interfaces (APIs) and emerging standards, offer unprecedented opportunities for enhancing interoperability across a range of health IT solutions. However, such opportunities come with significant challenges, particularly regarding preventing the fragmentation of healthcare systems and ensuring that data and systems remain secure against the growing threats posed by cyberattacks.

This position paper addresses the intersection between interoperability and cybersecurity within the context of the EHDS. We explore the main trends in the interoperability landscape, the challenges posed by cybersecurity and how standards can serve as the bridge between those two crucial aspects. By focusing on the need for international technical consensus, standards and coordinated policies, this position outlines strategic recommendations to guide the implementation of effective interoperability and cybersecurity measures within the EHDS framework.

Through such efforts, COCIR contributes to the realisation of a European Health Union where health data can be shared securely and efficiently, ultimately leading to improved patient outcomes and a stronger, more resilient healthcare system.

Main Trends in the Interoperability Landscape

Interoperability across diverse health technologies is fundamental to enabling multi-site and multi-disciplinary collaboration, ensuring that patients receive a continuum of care across different settings within health and social care systems. The rapid evolution of Application Programming Interface (API) platform standards has provided a powerful set of interoperability services that facilitate collaboration and information exchange among various health IT solutions at multiple levels (citizen/patient – provider – regional level).

One of the most significant advancements in interoperability is the emergence of standard specifications, such as the widely accepted HL7 FHIR (Fast Healthcare Interoperability Resources). Such a standard has the potential to become the preferred platform API standard for healthcare IT solutions. It promises to break down existing information silos by creating open ecosystems where a range of health IT systems can communicate seamlessly if the creation of e.g. HL7 FHIR-based interoperability specifications is coordinated appropriately internationally and proven test capabilities for interoperability between different implemented solutions are available

However, the current landscape is dominated by proprietary platform APIs, leading to the proliferation of specialised applications at each point of contact between citizens and healthcare providers, thereby creating a fragmented system. The adoption of a consistent, end-to-end interoperability strategy is essential to developing a cohesive and integrated digital health ecosystem across Europe.

From observing various interoperability projects in healthcare, several essential design elements can be identified for any successful interoperability solution guided by use cases and incentives within the EHDS framework:

1. Clearly define and scope the proposed interoperable scenario: The interoperability goals must be clearly defined, with a precise scope outlining the specific data, processes and outcomes involved.

2. Ensure a legal basis: There must be a solid legal foundation for the proposed interoperable scenario, particularly in terms of data protection, privacy and the rights of data subjects.

3. Identify stakeholders: All stakeholders must be identified from the perspective of business interests, including patients, healthcare providers, technology vendors and regulatory bodies.

4. Clarify organisational roles: The roles and responsibilities of each stakeholder must be clearly defined, ensuring that all parties understand their obligations and contributions to the interoperable solution.

5. Address stakeholders' needs and interests: Engage with stakeholders to understand their needs and interests, ensuring that the interoperability solution aligns with their objectives and concerns.

6. Ensure substantial benefits: The interoperable, secure solution must offer substantial benefits that justify the routine efforts required to use and maintain the digital solution, as well as the investment in technology. That could include improved patient outcomes, enhanced operational efficiency or cost savings.

7. Design in non-technical terms: Ensure that the design of the interoperable solution is described in non-technical terms, focusing on the stakeholders, care flows and care characteristics, such as time, effort, clinical achievements and business outcomes.

8. For the interoperability specifications, make use of and align with internationally proven standards which address the interoperable scenario in scope.

9. Provide proven test capabilities between different solutions which are in development, as well as those which are already available on the market.

The IHE Methodology which is described in ISO/TR 28380:2014 can serve a blueprint for addressing most of those essential design elements.

The Cybersecurity Challenge in the EHDS

As the digital transformation of healthcare accelerates, cybersecurity risks are becoming more pronounced, particularly in the context of health data sharing across the EHDS. EU healthcare providers, especially hospitals, face increasing security threats, including ransomware attacks and cyber intrusions by geopolitical actors, leading to disruptions in healthcare services and the theft of sensitive patient data.

The EU has recognised those challenges, as evidenced by introduction of the NIS2 Directive and the requirements under the Medical Devices Regulation (MDR). However, legislation alone is insufficient to address the complexities of cybersecurity in the rapidly evolving digital health landscape. Effective implementation requires substantial investments in infrastructure, software and human resources.

Considering those challenges, COCIR welcomes the European action plan to enhance the security of European health systems. Cybersecurity is a critical prerequisite for ensuring safe, high-quality healthcare and must be integrated into every aspect of health data interoperability. That includes the secure transmission of health data across borders, the protection of patient privacy and the prevention of unauthorised access to health information.

Standards: The Intersection of Interoperability and Cybersecurity

Standards play a pivotal role in bridging the gap between interoperability and cybersecurity. The adoption of recognised standards, such as HL7 FHIR and IHE Profiles, not only facilitates seamless communication between health IT systems, but also helps to ensure that those systems are secure and resilient against cyber threats.

1. API standards and cybersecurity: Advancements in cybersecurity standards offer a unique opportunity to embed cybersecurity features directly into interoperability frameworks. By e.g. incorporating security protocols, such as OAuth, into IHE Profiles, it is possible to ensure that data exchanges are both interoperable and secure. That dual focus on interoperability and cybersecurity is essential for protecting sensitive health data as they move through different systems and across borders.

2. End-to-end interoperability strategy: A consistent, end-to-end interoperability strategy that spans both eHealth and mHealth must include robust cybersecurity measures at every stage. That includes secure data transmission, authentication protocols and the use of encryption to protect patient information.

3. Guidelines for secure interoperability: To support the implementation of secure interoperability solutions, dedicated guidelines should be developed. Those guidelines should clarify the requirements for interoperability under the EHDS while ensuring that cybersecurity is embedded into every aspect of the framework. That includes the integration of MDS2[1] (Manufacturer Disclosure Statement for Medical Device Security) as a tool for health technology providers to communicate about security capabilities of their products and services and to support healthcare delivery organisations in their security obligations, such as cybersecurity risk assessments.

4. Cybersecurity in procurement: Cybersecurity considerations should also be integrated into the procurement processes for healthcare IT solutions. Guidelines for embedding cybersecurity in healthcare procurement tenders will ensure that all acquired systems meet the necessary security standards, thus protecting integrity of the EHDS.

[1] MDS2 promotes consistent security practices, encouraging vendors to align with standardised solutions, which ensures product interoperability and prevents the disabling of cybersecurity features due to conflicting system requirements.

Recommended Actions

To address the intersection of interoperability and cybersecurity in the EHDS effectively, COCIR recommends the following actions:

1. Ensure that the EHDS is supported by adequate resources, clear success metrics and practical use cases that directly benefit care providers, incentivising their participation without adding to their routine workload. That will prevent the EHDS from becoming an academic exercise and ensure it delivers measurable real-world outcomes before further funding is allocated.

2. Increase capacity, expertise, awareness and education: Invest in dedicated skills development and up-skilling programmes for health authorities, hospitals and healthcare providers to enhance their capacity to implement secure interoperability solutions. Cybersecurity should be standardised alongside interoperability standards to ensure consistent protection of sensitive health data across different systems, facilitating seamless information exchange. To support such efforts, it would be beneficial to promote becoming a benefactor of IHE-Europe and HL7 Europe and to assist IHE's work in developing cybersecurity profiles (e.g. ITI work item proposals related to US TEFCA that incorporate cybersecurity). Additionally, launch an awareness campaign for NIS2 in healthcare, organising stakeholder webinars at national and regional levels to facilitate coordination, collaboration and the exchange of best practices.

3. Ensure a harmonised and interoperable framework: It is recommended that the EHDS specifications be derived from existing Integrating the Healthcare Enterprise (IHE) Profiles. That approach would utilise established, recognised standards that facilitate interoperability and data exchange across healthcare systems. Additionally, the development of new IHE Profiles should be supported and sponsored where necessary to address emerging needs and gaps specific to the EHDS. That strategy will promote consistency, enhance data interoperability and accelerate implementation of the EHDS across Member States.

4. Upgrade legacy systems: Allocate dedicated funding to upgrade or replace obsolete software and hardware in healthcare environments to reduce the risk of security incidents related to known exploitable vulnerabilities in legacy systems.

5. To improve the quality of data within the EHDS, primary healthcare data interfaces should be designed to capture and consider the full care context, including the healthcare professional's environment, the patient's situation and specifics of the clinical encounter – while preserving the privacy of patients and caregivers. That approach will enable better interpretation of raw medical data collected during care interactions, ensuring that data are more meaningful and applicable to broader health insights.

6. Develop comprehensive guidelines: Create dedicated guidelines for implementation of the NIS2 Directive in healthcare, with a focus on clarifying the interaction between different applicable legislations (especially MDR) and ensuring shared responsibility and communication between healthcare delivery organisations and health technology providers to drive cybersecurity across the supply chain.

7. Enhance procurement standards: Develop guidelines, based on MDS2, for embedding cybersecurity into healthcare procurement tenders to ensure that all acquired health IT solutions meet the necessary interoperability and security standards.

Conclusion

Establishment of the European Health Data Space represents a significant opportunity to enhance the quality and efficiency of healthcare across Europe through the seamless exchange of health data. However, that vision can only be realised if interoperability and cybersecurity are addressed in tandem to build trustworthy solutions. COCIR is committed to working closely with the European Commission, Member States and all relevant stakeholders to ensure that the EHDS is both interoperable and secure.

The European Commission's focus on health underscores the urgency of those efforts. As we move forward, it is imperative that implementation of the EHDS is guided by clear standards, robust cybersecurity measures and a commitment to collaboration across the healthcare ecosystem. By taking such steps, we can ensure that the EHDS becomes a cornerstone of a strong European Health Union, protecting patients, their data, fostering innovation and delivering high-quality healthcare to all citizens.

COCIR looks forward to contributing to those important activities and supporting successful implementation of the EHDS. Together, we can build a secure, interoperable and future-proof healthcare system for Europe.

About us:

COCIR is the European Trade Association representing the medical imaging, radiotherapy, health ICT and electromedical industries. Founded in 1959, COCIR is a non-profit association headquartered in Brussels (Belgium) with a China Desk based in Beijing since 2007. COCIR is also a founding member of DITTA, the Global Diagnostic Imaging, Healthcare IT and Radiation Therapy Trade Association.