eHealth Network

GUIDELINE

on

the electronic exchange of health data under
Cross-Border Directive 2011/24/EU

General Guidelines

Release 3

The eHealth Network is a voluntary network, set up under article 14 of Directive 2011/24/EU. It provides a platform of Member States' competent authorities dealing with eHealth.

Adopted by the eHealth Network, Paris, 1 June 2022

-Keep this page free-

Table of Contents

Acronyms

Acronym	Description
Covid-19	Corona virus disease
eIDAS	Electronic Identities And Trust Services
EEHRxF	European Electronic Health Record exchange format
EES	Entry/Exit System
eHN	eHealth Network
EHR	Electronic Health Record
EIF	European Interoperability Framework
EU	European Union
FAIR	Findable, Accessible, Interoperable, and Reusable
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
ID	Identity
MS/C	Member State/Committee
NCP	National Contact Point
NCPeH	National Contact Point for eHealth
NIS	Network and Information Systems
ReEIF	Refined eHealth European Interoperability Framework
SDO	Standards Development Organisation
TFEU	Treaty on the Functioning of the European Union

1 Guidelines for electronic exchange of health data

THE MEMBER STATES in the eHealth Network,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 114 and 168 thereof,

Having regard to Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, and in particular Article 14 thereof,

WHEREAS:

- According to Article 168 (1) of the Treaty on the Functioning of the European Union (TFEU), a high level of human health protection is to be ensured in the definition and implementation of all Union policies and activities.

- Based on Articles 114 and 168 of the TFEU, the Union adopted Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.

- Article 14 (2) (b) (i) of Directive 2011/24/EU identifies an objective of the eHealth Network to draw up guidelines on a non-exhaustive list of data that are to be included in Patient Summaries that can be shared between health professionals to enable continuity of care and patient safety across-borders and effective methods for enabling the use of medical information for public health and research.
- The 2008 Commission Recommendation on cross-border interoperability of electronic health record systems provides a set of guidelines for developing and deploying interoperable electronic health record systems.

- The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.

- The 2015 Refined eHealth European Interoperability Framework (ReEIF), a common refined framework for managing interoperability and standardisation challenges in the eHealth domain in Europe.

- The Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) forms the legal basis for using personal health data.

- The EU Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society put forward actions aiming in particular to support the Member States' strategies on reforming health systems. Innovative digital solutions can boost people's health and quality of life and enable more efficient ways of organising and delivering health and care services. For this to happen, they must be designed to meet the needs of people and health systems and be thoughtfully implemented to suit the local context. Digital technologies should be seen as an integral part of health and care and geared towards the wider objectives of health systems.

- The Commission Recommendation on a European Electronic Health Record exchange format (EEHRxF) sets out a framework for the development of a European electronic health record exchange format in order to achieve secure, interoperable, cross-border access to, and exchange of, electronic health data in the Union.

- The Common Semantic Strategy for Health in the European Union, establishes a Common Semantic Strategy for the adoption of standards facilitating large-scale exchange of health information in the European Union, by facilitating convergence on interoperability standards for all MS/C.

- The European data strategy aims to make the EU a leader in a data-driven society. Creating a single market for data will allow it to flow freely within the EU and across sectors for the benefit of businesses, researchers and public administrations.

- The EU's Cybersecurity Strategy for the Digital Decade, cybersecurity is an integral part of Europeans' security. Whether it is connected devices, electricity grids, or banks, aircraft, public administrations or hospitals they use or frequent, people deserve to do so within the assurance that they will be shielded from cyber threats.

- Previous work from eHealth Network in the preparation and adoption of digital health interoperability guidelines such as:
  - Guidelines on Patient Summary
  - Guidelines on ePrescription
  - Guidelines on Organizational Framework for the National Contact Point for eHealth
  - Guidelines on approved contact tracing mobile applications in the EU
  - Guidelines on EU Digital COVID Certificate,

These guidelines have been instrumental for the establishment of cross-border infrastructures that are currently in routine operations.

HAVE ADOPTED THESE GUIDELINES:

2 General Guidelines

Chapter I - General Considerations

Article 1: Objectives, scope and maintenance

1. These guidelines, as adopted by the eHealth Network, are addressed to the Member States of the European Union and apply to the implementation of cross-border electronic health data exchange. These guidelines could, as well, serve as a guiding principle for national developments and implementations and enabling the use of medical information for public health and research (Art 14(2)(b)(ii).

2. According Article 14 of Directive 2011/24/EU, the eHealth Network guidelines are voluntary, "not-binding". In a cross-border context, interoperability is essential to the provision of high quality care. Member States shall therefore engage in taking appropriate measures to make their respective information systems interoperable, both technically and semantically, for use cases agreed by the eHN. This serves the purposes of establishing and functioning of the internal market according to Article 114 of the Treaty on the Functioning of the European Union.

3. These guidelines aim to support the Member States to achieve a minimum level of interoperability, taking considerations of patient safety and data protection into account, by defining requirements for communication between their respective National Contact Points for eHealth and interfaces between national and European levels.

4. Cross-border sharing of electronic health records (EHR) facilitates free movement of patients, prevents repeated treatments, improves patient safety and facilitates the exercise of lawful rights such as portability of data. Moreover, it enables financial savings for patients and healthcare systems.

5. This Guideline is a general guide to transmitting patient data to another country and is further detailed in the use case specific Guidelines, as described in Article 3 of these guidelines.

6. The eHealth Network is responsible for updating the guidelines (ideally every 2 to 3 years) in accordance with developments and priorities in the field of digital health.

Article 2: Definitions and Terms

For the purpose of this guideline, the definitions of the directive cited within the recitals of this guideline and the following definitions shall apply:

Term	Definition
individual/patient	the subject of EHR exchange and, ultimately, will benefit from interoperability achievements. OR Individual="a person considered separately rather than as part of a group" and patient="a person who is receiving medical treatment", as defined in Oxford Learner's Dictionaries
health professional	a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC, or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment, as defined in Directive 2011/24/EU
interoperability	within the context of European public service delivery, is the ability of disparate and diverse Organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the Organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems, as defined in European Interoperability Framework
European Electronic Health Record Exchange Format	the framework defined in Commission Recommendation on a European Electronic Health Record exchange format, as defined in Commission Recommendation on a European Electronic Health Record exchange format
preferred code systems	international, available and scientifically approved standards, that are widely used in clinical practice that leverage on a certain degree of agreement as being the best way to describe a clinical concept in a specific field/context.
National Contact Point for eHealth, NCPeH	the unique entity on a national level authorised by a Member State to provide an interface between the national and European aspects of cross-border exchange
electronic health record	the systematised collection of patient and population electronically stored health information in a digital format. EHRs may include a range of data, including demographics, medical history, medication and allergies, immunisation status, laboratory test results, radiology images, vital signs, personal statistics like age and weight, and billing information, adapted from https://en.wikipedia.org/wiki/Electronic_health_record

The key words "MUST", “MUST NOT”, "SHALL", “SHALL NOT”, "REQUIRED", "SHOULD", “SHOULD NOT”, "RECOMMENDED", "MAY", and “OPTIONAL” in this document are to be interpreted as described in RFC 2119[1].

MUST	This word, or the terms “REQUIRED” or “SHALL”, means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase “SHALL NOT”, means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective “RECOMMENDED”, means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase “NOT RECOMMENDED” means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
MAY	This word, or the adjective “OPTIONAL”, means that an item is truly optional. One user may choose to include the item because a particular application requires it or because the user feels that it enhances the application while another user may omit the same item.
CONDITIONAL	The usage of an item is dependent on the usage of other items. It is therefore further qualified under which conditions the item is REQUIRED or RECOMMENDED. This is an additional key word used in Doc 9303 (not part of RFC 2119).

[1] Bradner, Scott. (1997). Key words for use in RFCs to Indicate Requirement Levels. https://www.researchgate.net/publication/319393768_Key_words_for_use_in_RFCs_to_Indicate_Requirement_Levels

Article 3: Concept and intended use

1. The '*General Guidelines'* provide overarching and horizontal guidance applicable to domain specific eHealth Network guidelines.

2. eHealth Network use case specific guidelines (e.g. ePrescription and Patient Summary) should highlight, at the beginning, as being "supplementary guidance to the '*General Guidelines*'" and provide use case specific provisions.

3. Each domain specific guideline, supplementing the General Guidelines, should address concrete Use Cases with a well-defined scope, and address primarily cross-border scenarios but open the possibility for other implementations (e.g. at national level).

4. These guidelines are non-binding in relation to Member States' national implementation. However, Member States should consider to align national implementation projects with the provisions in these guidelines and, whenever applicable, adopt such requirements into national legislation.

Chapter II – Legal and Regulatory Considerations

Article 4: Data protection

1. Data within the scope of eHealth Network Guidelines typically include special category of personal data within the meaning of Art. 9 of the GDPR and therefore Member States will need to ensure that processing and storage are in line with applicable data protection requirements.

2. National legal frameworks may further define the conditions under which health data may be shared, making provisions for specific safeguards that need to be in place without, however, being prescriptive of such safeguards. Member States should ensure they have measures in place to assure and evaluate their own compliance with both GDPR and national regulations.

Article 5: Identification, authentication and authorisation

Member States and implementers shall take measures to:

1. Ensure reliable health professionals' identification, authentication and authorisation. Access policies shall be defined to ensure that only authorised health professionals have access to patients' data. Access policies may reflect domain specific guidelines.

2. Establish electronic registers of health professionals and providers, facilitating the verification of health professionals identity and their professional credentials (e.g. licence to practice), while respecting European and national regulations where applicable.

3. Provide the digital capabilities that allow health professionals to verify patient's identity. This is particularly important in cross-border scenarios where patients will use identification means and traits that health professionals may not be acquainted with (e.g. an identity card from another country, specific document ID). In online scenarios, digital capabilities shall support the electronic identification of patients, including using electronic identification means issued by other Member States.

4. Where appropriate, involve the patient while confirming authorisation to access and use health data (e.g. Patient Information Notice, Consent) in accordance with data protection law.

5. Open the possibility for authorised people to act on behalf of the patient (including legal guardians e.g. individual/patient is a minor child and the parents are acting on his/her behalf; individual/patient is an incapacitated or disabled adult and another person is authorised/entitled to act on their behalf, individual/patient has authorised someone to act on their behalf for convenience reasons and the use of so-called digital pilots (e.g. to assist individuals/patients with less developed digital skills).

Article 6: Patient safety

All information sharing in healthcare introduce risks, for example for information integrity, privacy, misinterpretation, or reliance on information that may be missing. Sharing of information cross-border may increase the likelihood of events while making mitigation of problems harder due to issues ranging from language and cultural to use of different coding practices and systems. Due to these reasons, measures should be taken to ensure patient safety and trust.

1. For safety and audit reasons, in the event of semantic transformation of health data, both (the transformed and the original health data) shall be available to the patients and authorised health professionals.

2. Implement verification/confirmation means to ensure health data accuracy and integrity. This is particularly relevant in health data exchange scenarios where data flows between different organisations and to prevent harming the patient due to misleading, inaccurate or incorrectly stored or exchanged health data.

3. Entities performing semantic transformations, such as NCPeHs in MyHealth@EU, shall enable logging sufficient for examination of events potentially leading to patient safety issues.

4. Health professionals and providers must ensure the proper and safe use of information systems and the effective flow of information.

5. Make clear to patients and health professionals the legal responsibilities applicable in any health data exchange scenario.

Chapter III – Organisational and Policy Considerations

Article 7: Enablers for implementation

1. The application of these guidelines should at all times take place in line with the provisions of relevant European and national legislation. Where such provisions do not exist or are not in force, Member States and implementers are expected to adopt, monitor and audit common policies, safeguards and measures representing multilateral interoperability agreements.

2. Interoperability agreements are particularly important for cross-border health data exchange scenarios, overcome the differences between countries and converge on common policies, standards and specifications.

3. The entry into operation of a health data exchange scenario should be subject to the explicit approval of the responsible entities. For EU driven cross-border health data exchange projects, the eHealth Network is the responsible entity for such approval. Non-EU and EEA (European Economic Area) countries may also operate in line with eHealth Network Guidelines.

4. Adequate monitoring procedures should be established by the respective controllers, for each health data exchange scenario. The monitoring procedures shall provide evidence to assess the impact of such intervention and support the decision-making about the continuation of such "data exchange scenario / use case.

5. Member States shall participate in expert bodies and communities under eHealth Network, such as eHealth Network Subgroup on Semantics and eHealth Network Technical Subgroup. Member States shall be encouraged to explicitly name representatives in the expert bodies and communities under eHealth Network.

Article 8: Quality standards and validation

1. Internationally used standards and specifications provide solid foundations for interoperability and quality standards.

2. Member States and implementers should consider, by design, the adoption of international standards and specifications.

3. The implementation of such standards should be supplemented by quality and safety standards to ensure adequacy to the specific context of each health data exchange scenario.

4. Member States and implementers should establish reliable testing and audit frameworks to scrutinise and validate implementations and minimise risks.

5. Health data structure and encoding should be subject to the high quality standards to preserve meaning and understandability.

6. In order to assure safe implementation, particularly patient safety and data protection, and further development of cross-border health data exchange scenarios, Member States should consider setting up a National Contact Points for eHealth (if not exists) for cross-border services to design, deploy, operate, quality assure, benchmark and assess progress on legal, organisational, technical and semantic interoperability for their successful implementation;

7. Whenever possible, Member States and implementers should measure the quantitative and qualitative benefits and risks (including economic benefits, risks and cost-effectiveness) of health data exchange scenarios.

Article 9: Education, training and awareness

In terms of education, training and awareness raising, Member States and implementers should:

1. Undertake activities towards increasing patients' and health professionals' awareness, knowledge and benefits understanding from health data exchange scenarios, especially which data are needed for the respective data processing purposes.

2. Undertake activities towards increasing health professionals' and health IT professionals' awareness, knowledge and benefits understanding about interoperability standards and specifications for exchange of health data, including cross-border scenarios.

3. Raise awareness, on the need to foster interoperability of digital health platforms, products and services, among producers and vendors of information and communication technologies, health professionals, health care providers, public health institutions and other stakeholders.

4. Pay particular attention to education, training and dissemination of good practices in electronically recording, storing and processing patient information.

5. Initiate appropriate, easy to understand information and awareness raising measures for all individuals, in particular patients.

6. Consider drafting recommendations for digital health literacy and competency, especially education and awareness raising measures targeting health policymakers and health professionals.

Chapter IV - Semantic Considerations

Article 10: Data

Safe and secure healthcare in cross-border situations requires an ability to convey both meaning and context in data exchange.

1. To convey both meaning and context in data exchange in the best possible way, it is necessary to have structured and coded data.

2. When health data is subject to semantic transformations (e.g. transcoding, mapping, enrichment, annotation), the rationale and rules for such transformations should be documented.

3. Health data semantic transformations shall credibly preserve the original content and make it available in an understandable way to the health professionals.

4. Each implementation of health data exchange shall clearly identify entities responsible for the accuracy and integrity of semantic transformations.

5. When structured and coded data is not available, original documents should be transferred, as they may still provide important information relevant for care processes.

6. Member States should work together to build a convergent use of code systems. Mappings should be done as shared activities when more MS are affected. Licensing activities with SDO partners should be done together. This will reduce the burden of the workload, support capacity building and also foster the EU pathway towards a harmonised way forward.

Article 11: Terminology

Common terminology practices shall ultimately contribute to reinforcing patient safety and increase the overall quality of the continuity of the care process.

1. The purpose of identifying "*preferred code systems*" is to promote convergence towards code systems internationally used, officially maintained, using FAIR-principles, available in several languages as well as open for the possibility to transcode to other relevant code systems.

2. "*Preferred code systems*" should be understood as a *guiding principle* and not as an *obligation*. When convergent use of "*preferred code systems*" is not achievable in practice, solutions should be found to enable the exchange of existing information without undermining patient safety.

3. When national/local standards exist, Member States and implementers should consider the creation of transcoding maps to "*preferred code systems*" and envisage the adoption of "*preferred code systems*" to replace national/local ones. This is particularly important for cross-border health data exchange scenarios.

4. Whenever possible, a master catalogue should be made openly available to describe the code systems and value sets applicable for each health data exchange scenario (further described in Art. 12).

Guidelines should adopt the concept of "*preferred code systems*", for data elements where there is a consensus around current practices. Additionally, guidelines should also highlight strategic aims by pointing to upcoming code systems.

Article 12: Controlled Lists (Value set Catalogues)

1. A master catalogue should be made openly available for each health data exchange scenario. The master catalogue:

2. Indicates and describes the preferred code systems (i.e. controlled vocabularies used for encoding health data).

3. Indicates and describes the agreed selection of sets of concepts, from the preferred code systems, necessary to facilitate the understanding of the health data exchanged. That selection of concepts and its designations, organised into sets, form the Value set Catalogues, which will be based on international code systems whenever possible.

4. Should be evaluated on a regular basis with regards to the selection of concepts and the code systems used. For historical health data meaning preservation, Value set Catalogues should maintain previous versions of the code systems.

5. Should, wherever possible, use the latest version of code systems. If this is not possible, at minimum adoption of critical concepts should be considered (e.g. the new concepts released for the Covid-19 pandemic).

6. Might hold one or multiple Value set Catalogues depending on the scope of each specific implementation.

7. Shall support designations in multiple languages (facilitate translations based on meaning - code translation - and not literal/textual translation).

8. Facilitates the transcoding between different code systems (i.e. from national/local code systems to agreed code systems).

Every Member States shall make, if necessary, transcoding of national code systems to ensure the correct transmission of patient data to another Member State. Member States should come to an agreement on how to develop, publish and maintain a master catalogue for cross-border health data exchange scenarios. Relevant Value set Catalogues should be easily available for implementers. Ideally, Value set Catalogues should form a network of EU Value set Catalogues accessible and interoperable across Europe with a harmonised and sustainable maintenance process.

Chapter V - Technical Considerations

Article 13: Technical requirements

Member States and implementers shall adopt sound technical interoperability standards and specifications, so that health data exchange scenarios can take place in a multi-organisation, multi-vendor, multi-network, multi-service environment.

1. Machine-to-machine communication shall adopt widespread and, whenever possible, payload agnostic standards.

2. Machine-readable structured data exchange should be applied to the greatest extent possible. The exchange of unstructured health data should be foreseen whenever it complements or enriches the health data exchange scenario.

3. When applicable, a gateway software should be established to transform data from proprietary/local settings (formats, code systems, languages) to interoperable settings and desirable languages. The gateway should be established by the participants in the personal electronic health data exchange scenarios.

Article 14: Security

Member States and implementers shall apply the highest security standards for data exchange scenarios, such as:

1. Protect and properly secure health data so that its confidentiality, integrity, availability and non-repudiation are ensured and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems and avoid health data breaches.

2. Design secure, safe, trustable information systems including data protection by design and by default.

3. Apply preventive measures and protect against unauthorised or unlawful processing of health data and against accidental loss, destruction or damage.

4. Ensure that health data is transmitted only to trusted organisations or entities.

5. Ensure that communication of health data is subject to secure communication and end-to-end security measures.

6. Ensure that personnel dealing with electronic health record systems is properly aware of cybersecurity risks and adequately trained.

7. Establish an appropriate system of audit trails and allow authorised bodies to duly inspect the established mechanisms.

8. Notify security incidents having a significant or substantial impact on the continuity of the health data exchange scenarios. Whenever possible, apply systems for active monitoring and incident detection (Security Operation Centres).

9. Whenever possible, require cybersecurity assessment to demonstrate the fulfilment of cybersecurity requirements.

Article 15: Testing and audit

The Member States and implementers shall adopt appropriate measures to test and audit health data exchange scenarios.

1. Demonstrate compliance with agreed standards and specifications.

2. Perform end-to-end testing with health professionals to ensure the correctness and understandability of health data.
3. Promote the use of automated validation tools for technical and semantic interoperability criteria.

1. These tools should be extended to address the specificities of each type of data category being exchanged (e.g. data models, datasets, data formats, code systems, value sets).
2. These tools check and stress security requirements at infrastructure and application level.
3. These tools check automatically schema, schematron and model based validation of clinical documents in place.

4. Record any incident resulting from health data exchange scenario in an incident management system. When applicable, establish adequate cross-border communication arrangements.

5. Establish the appropriate audit trails system and audit mechanism for legal, organisational, semantic, technical, security and operational requirements. Ensure that audit trails are recorded to support the monitoring and verification of events related to the specific health data exchange scenario.

3 Supporting information

This chapter provides supporting information and explanatory text to aid understanding of the guidelines, and the rationale behind the proposals. It therefore follows the same structure as the guideline itself.

Chapter I - General Considerations

Article 1: Objectives and scope

The primary objective of this guideline is to provide common grounds for the implementation of cross-border health data exchange scenarios, like the ones implemented through the MyHealth@EU. However, many guidelines are project and implementation specific to facilitate their adoption by a wider range of initiatives. These guidelines including the ones at national level, are to promote at a larger scale the adoption of the principles promoted in the eHealth Network Common Semantic Strategy.

Article 2: Definitions

The definitions section focuses on clarifying the meaning and depth of concepts that work as building blocks for the eHealth Network interoperability guidelines for health data exchange scenarios. The concepts described are horizontal to several implementation scenarios and not specific from one project or implementation.

Article 3: Concept and intended use

This general guideline provides common principles for the domain specific guidelines. eHealth Network use case specific guidelines are the ones addressing the specific requirements and conditions of well-defined implementation scenarios like:

- Exchange of Patient Summaries
- Exchange of ePrescription and eDispensation
- European Digital COVID Certificate
- Exchange of Laboratory Results
- Organizational Framework for the National Contact Point for eHealth

Chapter II - Legal and Regulatory Considerations

Article 4: Data protection

The Regulation (EU) 2016/679 (General Data Protection Regulation) lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. As such, it could in the future reduce the need for specific data protection agreements and significantly reduce the scope of such (interoperability) agreements.

A common cross-border website should provide information about the specific rights of data subjects according to the different legislations of all the participating Member States. The information on the website should clearly specify the rights, conditions and practicalities according to the national legislation of each Member State.

Article 5: Identification, authentication and Authorisation

Patients and health professionals’ identification, authentication and authorisation are essential aspects in any data exchange scenario.

The cross-border scenarios face increased challenges due to the existing diversity of identification, authentication and authorisation schemes in place in each Member State. Each data exchange scenario should ensure a univocal link between patients with their electronic health records. The existence of patient's identifier can facilitate the univocal link between patients and their health data.

There is also the need to identify a health professional and health care provider organisation to the high level of confidentiality required when personal electronic health data is exchanged between health professionals/health care provider organisations. The health professional should be linked to a digital identity which is issued by a certified authority. The healthcare provider organisation should as well have a unique identifier. These identifiers provide a reliable base to establish and maintain a circle of trust between all the participants in a scenario involving the exchange of personal electronic health data.

Member States shall follow Regulation (EU) No 910/2014 (eIDAS2) when implementing digital signature services at the eGovernment or eHealth service level to ensures that patients and health professionals can use their own national electronic identification schemes (eIDs) to access online public services in other EU countries that use eIDs.

The electronic identity of the health professional and/or healthcare provider organisations is also used for authentication purposes by a majority of Member States. For example, MyHealth@EU has a requirement of 2-factor identification for health professionals. Similarly, the majority of Member States makes use of digital signature for health professional/health care provider organisations at national level.

For most Member States, the electronic identification is also linked with the health professional entitlement, and authorisation for accessing patient information is based on the entitlement of the health professional. In the majority of Member States, the prescribing entitlement or medication dispensing entitlement can be inferred from the electronic identity of the health professional.

Article 6: Patient safety

The semantic transformation is performed according to the translation, mapping and transcoding performed by designated competent legal entities in Member States that have activity in cross-border services, in which:

- the responsibility for the *accuracy* and integrity of the process is with each national designated competent legal entity for such semantic processing
- the responsibility for errors in the semantic mapping is a shared cross-border responsibility between the respective Member States.

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

https://eur-lex.europa.eu/eli/reg/2014/910/oj

Chapter III - Organisational and Policy Considerations

Article 7: Enablers for implementation

Scenarios involving the exchange of personal electronic health data must have an ***incident management system*** in place, including a service desk function. This service desk function may differ from country to country, however a key common responsibility should be to act as proximity contact point for any users facing difficulties regarding the health data exchange scenarios. As part of this function, service desk should also address end user complaints. Incident management is important for the individual Member State as well as for the cross-border electronic exchange aspect; Member States should be able to contact each other in the event of technical or organisational problems.

Problem management should address and resolve the root causes of incidents and thus minimise the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure, and prevent recurrence of incidents related to these errors.

Change management ensures that standardised methods and procedures are used for efficient handling of all changes in the technical setup, in the organisational setup or in practical matters in scenarios involving the exchange of personal electronic health data. Each implementation must have a documented process for implementing changes of semantical, technical, organisational and practical kinds. The change process must include proper planning and ensure that sufficient information has been disseminated to other Member States.

Article 8: Quality standards and validation

The semantic transformation is performed according to the translation, mapping and transcoding carried out by designated competent legal entities in each Member State. The responsibility for the accuracy and integrity of the process is with each national designated competent legal entity for such semantic processing. EU Commission may support collaboration in translations, mapping-work and transcoding between Member State.

Member States should work together to build a convergent use of code systems. Mappings should be done as shared activities when more Member State are affected. Licensing activities with Standards Developing Organisation (SDO) partners should be done together. This will reduce the burden of the workload, support capacity building and also foster the EU pathway towards a harmonised way forward.

Article 9: Education, training and awareness

Member State~~s~~ and implementers should take steps to engage in education, training and awareness raising. Such an approach would promote the more effective use of health information as individuals/patients move between a variety of health care providers, along the continuity of care, and receive treatment and care wherever they are in Europe. Suggested activities might include:

- provide health professionals with training materials and activities to support cross-border health information exchange services, in addition to national health data exchange services.
- inform individuals/patients about cross-border health information exchange services, in addition to national health data exchange services.
- engage health care professionals/healthcare providers in the design of health information exchange services at national and cross-border level.

Chapter IV - Semantic Considerations

Article 10: Data

Maintaining consistency and backwards compatibility with existing data is of paramount importance to avoid losing relevant data.

Article 11: Terminology

These guidelines promote the principles of the eHealth Network Common Semantic Strategy. Whilst considering the diversity of existing national implementations, the guidelines will promote international standardised terminology solutions and code systems instead of local and specific ones.

1. The convergent use of preferred code systems should contribute to ensure clear understanding and preserve the meaning of the information present in health records, by tackling the variability of coding practices.

2. The convergent use of preferred code systems should also contribute to the increase of quality of health data collection as well as facilitate benchmarking and evaluation initiatives.

To ensure the highest quality of data and to avoid loss of information, health data collected at the point of care should take advantage of the preferred code systems proposed in the domain specific eHealth Network Guidelines.

Article 12: Controlled Lists (Value set Catalogues)

Across Europe, there are different languages, different standards and code systems impacting health data. Even if each implementation should have the possibility to choose and define how to approach this challenge, effort should be made to build on top of existing common health terminology services. The eHealth Network and the Commission should make efforts to sustain and promote the usage of such common health terminology services.

If Member States cannot implement a preferred code system, alternatives can be used given that English is available.

Chapter V - Technical Considerations

Article 13: Technical requirements

Member States and implementers should consider the European Electronic Health Record exchange Format (EEHRxF) in order to achieve secure, interoperable, cross-border access to, and exchange of, electronic health data in the Union.

Article 14: Security

Security includes general security of the connected networks and infrastructures. To this end, Member States should take into consideration the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS directive). Additionally, Member States should consider the "framework for the establishment of European cybersecurity certification schemes", foreseen in the EU regulation 881/2019, for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union. For security purposes, the system's implementation must ensure principles like logging of transactions.

Article 15: Testing and audit

In order to ensure testing and auditing cross-border services and related interoperability provisions and systems, these guidelines will be provided in the domain specific guidelines.