eHealth Network

GUIDELINE

on

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

Release ~~2~~3

General Guidelines

~~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. The Joint Action supporting the eHealth Network (JAseHN) provides scientific and technical support to the Network.~~

~~Adopted by consensus by the eHealth Network, Brussels, 21 November 2016~~

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.

For eHealth Network adoption, Paris, 1 June 2022

-Keep this page free-

~~TABLE OF CONTENTS~~

~~1.~~

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~~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 guidelines on ePrescriptions~~ borders and effective methods for enabling the use of medical information for public health and research.

~~(1)~~ The 2008 Commission Recommendation on cross-border interoperability of electronic health record systems~~Member States adopted Release 1 of the Patient Summary Guidelines in November 2013 and Release 1~~ provides a set of ~~the ePrescription Guidelines in November 2014.~~

~~(2) The Member States have been playing an active role in the revision of the~~ guidelines~~, in particular by providing their knowledge and experience, and adopted the Organisation Framework (OFW) in November 2015.~~

~~(3) Preliminary work in the field of eHealth, in particular by the European large scale pilot "European Patients' Smart Open Services" (epSOS), the CALLIOPE Network and the eHealth Governance Initiative (eHGI), shall provide a solid and reliable foundation~~ for ~~this guideline.~~

~~(4) As cross border services take place in the field of public health and in accordance with Article 14, the goal must be to use open standards wherever possible.~~

- ~~REGULATION (EU) 2016/679 of 27 April 2016 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~~developing and

deploying interoperable electronic health ~~data. This supersedes Directive 95/46/EC~~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 ~~Chapter I –~~ General ~~Considerations~~Guidelines

Chapter I - General Considerations

Article 1: Objectives ~~and~~, 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 ~~data exchange.~~ 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).

~~1. 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 eHealth National Contact Points (as defined in Article 2) and interfaces between national and European levels.~~

2. ~~According to the primary responsibility of the Member States in the field of healthcare provision, as laid down in Article 168 (7) of the Treaty on the Functioning of the European Union, these guidelines are non-binding.~~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 ~~those~~ 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 ~~directives~~directive cited within the recitals of this guideline and the following definitions shall apply:

~~a) 'Health care professional' means 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[1], 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 aaccording to the legislation of the Member State of treatment.~~

~~b) '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. (European Interoperability Framework)~~

~~c) 'eHealth National Contact Point' refers to 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[2].~~

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

~~[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:255:0022:0142:en:PDF~~

~~[2] Each Member State may establish one or more of these entities (at regional/local level) depending on the respective National Health Service model.~~

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[3].

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.

[3] 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

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).

Article 3: Concept and intended use

1. ~~Each Annex~~The *'General Guidelines'* provide overarching and horizontal guidance applicable to ~~these~~domain specific eHealth Network guidelines ~~describes~~ .

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.

~~1.~~3. Each domain specific guideline, supplementing the General Guidelines, should address concrete Use Cases ~~relating to the intended~~with a well-defined scope, and ~~purpose for~~address primarily cross-border ~~exchange.~~scenarios but open the possibility for other implementations (e.g. at national level).

~~1.~~ These guidelines are non-binding in relation to Member States' national implementation~~, notwithstanding Member States are considered to:~~

~~(b) use open standards for public health activities;~~

~~(c) decide freely whether they want to~~ . However, Member States should consider to align national implementation projects with the provisions in these guidelines and, whenever applicable, adopt such requirements into ~~local legislation;~~

~~2.~~4. ~~bear in mind these guidelines when adapting their~~national legislation.

Chapter II – Legal and Regulatory Considerations

Article 4: Data protection

1. ~~The implementation of these guidelines is in line with Directive 95/46/EC on~~Data within the ~~protection~~ scope of eHealth Network Guidelines typically include special category of personal data within the meaning of Art. 9 of the GDPR~~and free movement of such data, and~~ and therefore Member States will ~~be updated~~need to ~~reflect the~~ ensure that processing and storage are in line with applicable data protection requirements ~~of the General Data Protection Regulation~~.

2. ~~In the meantime,~~ 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.

~~1. Data contained in health records are "sensitive personal data" and therefore Member States will need to ensure processing and storage are in line with legal and data protection requirements. In particular, Member States may need to implement consent management for the processing and storing of data and subsequent authorised access.~~

~~*Authorisation*~~*Article 5: Identification, authentication and authorisation*

Member States and implementers shall take measures to:

~~*Article 4:*~~ Ensure reliable health professionals' identification

~~1. Member States shall adopt the Organisational Framework for their eHNCP that comprises the commonly adopted policies, processes and audit mechanisms for cross-border care.~~

~~2. Member States shall ensure validation of foreign patients' identity.~~

~~3. Member States shall ensure their eHNCP enforces identity~~ , authentication ~~of~~ and authorisation. Access policies shall be defined to ensure that only authorised health professionals ~~who use cross-border services.~~

1. ~~Member States may wish~~have access to ~~consider the content of a register~~patients' data. Access policies may reflect domain specific guidelines.

4. Establish electronic registers of health professionals ~~who are entitled to prescribe~~ and ~~dispense, for instance:~~

~~(a)~~ providers, facilitating the ~~name and profession,~~

~~(b) a personal identification number, including the ISO 3166 country code,~~

~~(c) the current address~~verification of ~~the~~ health ~~care provider organisation with which the health~~professionals identity and their professional ~~is affiliated or the address of his or her private practice,~~

~~(d) the date of issue of the healthcare professional's~~ credentials (e.g. licence to practice~~,~~

~~1.~~2. ~~the speciality may be recorded in line with~~), while respecting European and national ~~practice as the prescribing of some medicinal products may be restricted.~~regulations where applicable.

~~*Article 5: Patient safety*~~

~~1. Health professionals, patients and National Contact Points for eHealth can rely upon the information released by the eHNCP of other Member States.~~

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 ~~documents~~health data) shall ~~for safety and audit reasons~~ be available to ~~all persons who are~~the patients and authorised ~~to use this data~~health professionals.

~~2. Liability for errors in the semantic transformation will be as described in the Legal Agreement.~~

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 ~~according to~~ 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 ~~implement~~adopt, monitor and audit common policies, safeguards and measures representing multilateral interoperability agreements ~~of the eHealth Network~~.

~~1. Such agreements will apply to the exchange of health related data across borders in a generic way and they will include but are not limited to agreements on duties and responsibilities of the eHNCPs and on common identification, authentication and authorisation measures.~~

~~2. Member States participating in cross-border exchange shall set up an eHNCP compliant with the OFW. This should be unique to each Member State in its relationship with other Member States, i.e. a single eHNCP communication gateway should be responsible for interaction with the eHNCP for each other Member State for cross-border services.~~

~~3. Member States must ensure that their eHNCP establishes the connection with the national infrastructure, ensuring that appropriate processes and procedures are in place (security measures, safeguards etc.).~~

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.

~~4.~~ The entry into operation of ~~an eHNCP requires the~~ a health data exchange scenario should be subject to the explicit approval of the ~~coordination mechanism established through the~~ responsible entities. For EU driven cross-border health data exchange projects, the eHealth Network ~~for the cross-border environment.~~

~~2.~~3. ~~Non-EU~~ is the responsible entity for such approval. Non-EU and EEA (European Economic Area) countries may also operate in line with ~~Cross-Border Directive 2011/24/EU with the explicit approval of the~~ eHealth Network~~.~~ Guidelines.

~~5. Participating Member States should establish adequate monitoring procedures for their eHNCP.~~

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. ~~Each Member State should apply such~~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 ~~as eHN might agree in~~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.

~~1.~~5. Health data structure and encoding should be subject to the ~~process of coding the information, such as validation checking~~high quality standards to preserve meaning and understandability.

~~l)~~ In order to assure safe implementation, particularly patient safety and data protection, and further development of cross-border ~~eHealth services~~health data exchange scenarios, Member States should ~~:~~

~~2.~~6. consider setting up a ~~facility~~ 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;

~~3.~~7. ~~undertake assessment activities, such as measuring~~ Whenever possible, Member States and implementers should measure the quantitative and qualitative ~~possible~~ benefits and risks (including economic benefits, risks and cost-effectiveness) of ~~cross-border services~~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 ~~of the~~, knowledge and benefits ~~of and need~~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 ~~and related~~ standards and specifications for ~~electronic~~ exchange of health data, including cross-border ~~patient data exchange, including~~scenarios.

~~1.~~3. Raise awareness ~~of~~, on the need to foster ~~the~~ interoperability of ~~technical systems~~digital health platforms, products and services, among producers and vendors of information and communication technologies, ~~healthcare~~health professionals, health care providers, public health institutions ~~, insurers~~ and other stakeholders.

~~2.~~4. Pay particular attention to education, training and dissemination of good practices in electronically recording, storing and processing patient information.

~~3.~~5. Initiate appropriate, easy to understand information and awareness raising measures for all individuals, in particular patients.

~~4.~~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 ~~care~~ situations requires an ability to convey both meaning and context in data exchange. ~~It is agreed that to achieve this~~

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

2. ~~The responsibility~~ 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 ~~the process is~~ 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.

~~2.~~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 ~~each national designated competent entity for such semantic processing.~~ 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

~~1. The eHNCP must use the latest version of the Master Valueset Catalogue and~~

~~the~~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 ~~versions of these~~/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:

~~1.~~2. Indicates and describes the preferred code systems (i.e. controlled vocabularies used ~~in semantic transformation.~~for encoding health data).

~~2. Member States must ensure the eHNCP performs semantic transformation (e.g. translation and mapping), which is needed for the cross-border information exchange.~~

~~3. Member States wishing to engage in cross-border communication must provide conformant messages operating to standards agreed by the eHN. Internally, Member States may perform mapping, transcoding and translation activities to local codes to support such activity.~~

~~4. Further work is needed to review the code schemes used for cross-border~~

~~scenarios. Member States will work with the agreed governance arrangements of the eHealth Member State Expert Group (eHMSEG) to achieve this.~~

~~*Article 6: Master Catalogue*~~

~~Agreement on a set of coding schemes as set out in Article 11 will require a master catalogue at EU level which can be used by all Member States to share value sets, allowing each Member State to translate and transcode schemes, if required, to their national equivalents. It is expected that the eHN will agree on the mechanism by which the Master Catalogue will be maintained and published.~~

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

~~1.~~ Member States ~~must provide a gateway service, a request port~~ and ~~a semantic transformation service in order~~

~~to enable the core steps for relevant cross-border use cases to be executed.~~

~~2. The eHNCP~~implementers shall ~~guarantee that all cross-border service requirements~~adopt sound technical interoperability standards and specifications ~~(legal, organisational, semantic and technical) agreed by the eHN are fulfilled.~~

~~3. The eHNCP must ensure the appropriate interface with the core services set up at EU level.~~

~~*Article 7: Security*~~

~~1. The eHNCP Security Policy Baseline creates a general security and~~, so that health data ~~protection baseline adapted to cross-border needs. This was approved by the eHealth Network as Annex A to the Organisational Framework.~~

~~2. Member States shall ensure that they are fully compliant with the cross-border security policy.~~

~~The eHNCP shall~~ exchange scenarios can take ~~all reasonable steps~~ place in a multi-organisation, multi-vendor, multi-network, multi-service environment.

1. Machine-to-~~ensure~~-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 ~~(including data~~ standards for data exchange scenarios, such as:

1. Protect and properly secure health data so that its confidentiality, integrity, ~~authenticity,~~ 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. ~~The eHNCP must~~ 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.

~~2.~~4. Ensure that ~~cross-border~~health data is ~~not~~ transmitted ~~via these services to a Member State that either does not belong~~only to ~~or is not allowed into the cross-border environment~~trusted organisations or entities.

~~3.~~5. ~~Member States shall~~ Ensure that communication of ~~identifiable personal~~ health data is subject to secure communication and end-to-end security measures.

6. ~~Member States shall~~ Ensure that ~~their eHNCPs~~ personnel dealing with electronic health record systems is properly aware of cybersecurity risks and adequately trained.

~~3.~~ Establish an appropriate system of audit ~~trail~~trails and ~~shall~~

~~4.~~7. allow authorised ~~official~~ bodies to duly inspect the established mechanisms ~~for data collection, processing, translation and transmitting~~.

~~a) make logs available for legal purposes, e.g. if requested by a patient.~~

~~4. The Member States must ensure that the eHNCP has clearly identified the responsible data controller and data processor in accordance with the provisions of General Data Protection Regulation.~~

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 ~~will need~~and implementers shall adopt appropriate measures to ~~establish testing mechanisms that~~ test and audit health data exchange scenarios.

~~1.~~ Demonstrate compliance with agreed standards ~~agreed by the eHN. For cross border purposes, a Europe-wide testing process will also be required, including validation of data fields against defined criteria (e.g. dates in valid date format).~~

1. ~~Testing will be supported by processes and tools agreed by the eHN. Member States shall ensure that their eHNCP meets the interoperability~~ and specifications ~~and security requirements~~.

2. ~~The eHNCP shall establish and maintain an incident management solution to support~~ Perform end-to-end testing with health professionals~~, healthcare providers~~ to ensure the correctness and ~~citizens in its territory~~understandability of health data.
3. ~~The eHNCP must ensure an auditing~~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.

~~2.~~ Establish the appropriate audit trails system and audit mechanism for legal, organisational, semantic ~~and~~ , technical, security and operational requirements.

~~3. apter VI Amendments~~

~~*Article 8: Amendments to the guidelines*~~

~~The eHealth Network is responsible for updating the guidelines.~~

~~3.~~5. ~~These guidelines~~ Ensure that audit trails are ~~addressed to Member States~~recorded to support the monitoring and verification of events related to the specific health data exchange scenario.

3 ~~2.~~ 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 ~~guidelines themselves~~guideline itself.

~~Chapter I - General Considerations~~

Chapter I - General Considerations

Article 1: Objectives and scope

~~The primary objective of these guidelines is to support implementation of eHealth Digital Service Infrastructure Use Cases under CEF.~~

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 ~~which~~that work as building blocks for the eHealth Network interoperability guidelines for health data exchange scenarios. The concepts described are ~~common~~horizontal to ~~cross-border health~~ several implementation scenarios and not specific from one project or implementation.

Article 3: Concept and intended use

~~The contents of these guidelines are seen as required for cross-border exchange, but also as advice that will help each Member State to make progress in terms of its own agenda.~~

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 ~~and its subsequent Delegated and Implementation Act aim to improve consistency and reduce diversity in data~~) lays down rules relating to the protection ~~and rights including access to~~ of natural persons with regard to the processing of personal data and ~~deletion or suppressions of sensitive information.~~rules relating to the free movement of personal data. As such, it could in the future ~~abolish~~ reduce the need for specific data protection agreements and~~, together with the transposition of Directive 2011/24/EU,~~ 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.

~~*Authorisation,*~~ *Article 5: Identification, authentication and* ~~*identification*~~ *Authorisation*

~~Issues~~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 ~~of patients and health professionals involved in cross-border care relationships are crucial elements. To be able to link~~ schemes in place in each Member State. Each data exchange scenario should ensure a univocal link between patients with their ~~patient~~electronic health records~~, ~~. The existence of ~~a patient~~ patient's identifier ~~is necessary~~can facilitate the univocal link between patients and their health data.

~~Besides having means to identify a patient, facilities to~~ There is also the need to identify a health professional ~~or~~and health care provider organisation ~~are a prerequisite for maintaining a~~ to the high level of confidentiality ~~for medical information when it~~ required when personal electronic health data is exchanged ~~in a secure manner~~ between ~~other~~ health professionals/health care provider organisations. The health professional~~/health care provider organisation identifier is~~ should be linked to a digital identity which is issued by a certified authority. ~~This identifier provides a~~The healthcare provider organisation should as well have a unique identifier. These identifiers provide a reliable base to ~~create~~ establish and maintain a ~~trust~~ circle ~~between health professionals/health care provider organisations and is also a precondition for electronic signing by the health professional/health care provider organisation~~of trust between all the participants in a scenario involving the exchange of personal electronic health data.

Member States ~~will have to consider their approach to~~shall follow Regulation (EU) No 910/2014 (eIDAS4) when implementing digital signature services at the eGovernment or eHealth service level~~ in the light of the~~ to ensures that patients and health professionals can use their own national electronic identification ~~and trust~~schemes (eIDs) to access online public services ~~(eIDAS[5]) regulation adopted in July 2014.~~in other EU countries that use eIDs.

~~For functions such as ePrescribing, the identification of the health professional will need to be linked to access the data (i.e. confirmation of patient consent) and the authorisations to prescribe. Datasets to enable this are available from some Member State competent authorities, but further work is required for professional bodies to support cross-border ePrescribing.~~

The ~~digital ID~~electronic identity of the health professional and/or ~~health care~~healthcare provider ~~organisation~~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 ~~make~~of Member States makes use of digital ~~signing~~ signature for health professional/health care provider organisations ~~in their country. In some countries a prescription is not valid without the (electronic) signature of the health professional~~at national level.

For most Member States, the ~~digital identity of~~electronic identification is also linked with the health professional ~~is linked to the health professional role~~entitlement, and authorisation for accessing patient information is based on the ~~role, e.g. GP or pharmacist, of the health professional. In most of these Member States, this is based on the *digital* identity~~ entitlement of the health professional. In the majority of Member States, the ~~health professional~~ prescribing ~~role~~ entitlement or ~~health professional~~ medication dispensing ~~role~~ entitlement can be inferred from the ~~digital~~ electronic identity of the health professional.

Article 6: Patient safety ~~issues~~

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

---

[4] 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

~~http://ec.europa.eu/digital-agenda/en/trust-services-and-eid~~

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

Chapter III ~~–~~ Organisational and Policy Considerations

Article 7: Enablers for implementation

~~Each Member State would be expected to have one "eHealth National Contact Point" (eHNCP), which is the technical and organisational entity that ensures interoperability across national borders with other Member States and decouples the national infrastructure from other Member States.~~

~~The first consequence is that the external interface (with the other eHNCP) is standardised, with specifications of protocols, procedures and exchanged documents. The interface with the national infrastructure is specified at a conceptual level, but each Member State remains free to adopt the most suitable solution to interface the eHNCP with their national infrastructure.~~

~~The organisational setup and procedures for operating the eHNCP are based on ITIL (Information Technology Infrastructure Library). The selected service and support processes have been deemed a minimum requirement for operating the eHNCPs in a coherent way.~~

~~"Regional replicas" of both the technological and organisational arrangements of a typical eHNCP, which constitute a Regional Contact Point (RCPeH), are possible and follow the same principles and requirements. If an MS has two or more Regional Contact Points, it needs to nominate one to act as an eHNCP, to act as the national gateway vis à vis the eHNCP of another MS. Participating MS should make adequate arrangements to ensure eHNCP readiness for operation of cross border services and level of service sustainability (by following the compliance establishment process described in Article 15).~~

~~Each Member State must have its own national support organisation in place and publish information about the responsible persons. There should be a central service desk for managing incidents, problems and changes and the interface between the national and central service desks should be arranged.~~

~~All Member States must have *incident management*~~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 ~~but is likely to act as the co-ordinating centre for any users having difficulty accessing patient summaries or ePrescriptions.~~, 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 ~~aims to~~ should address and resolve the root causes of incidents and thus ~~to~~ minimise the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure, and ~~to~~ prevent recurrence of incidents related to these errors~~. Member States must have organised ways to solve problems~~.

Change management ~~aims to ensure~~ 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 ~~a Member State.~~scenarios involving the exchange of personal electronic health data. Each ~~Member State~~ 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 ~~continuum~~ continuity of care, and receive treatment and care wherever they are in Europe. Suggested activities might include:

- ~~national~~ provide health professionals with training materials and activities to ~~be provided to~~ support ~~CBeHIS operation~~

- ~~participating MS engage health professionals/~~ cross-border health ~~care providers in specification updates and other clinical concerns related to the operation of~~ information exchange services, in addition to national health data exchange services.

- ~~participating MS~~ inform ~~citizens~~individuals/patients about ~~CBeHIS provisions, including a description of the~~ cross-border health information exchange services, in addition to national ~~infrastructure~~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*

~~The epSOS pilot operated on the twin principles of building on what is available and not interfering with the internal systems in a Member State. The need to maintain consistency with existing developments added more constraints to the initial clinical definitions.~~

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

Article 11: *Terminology*

These guidelines ~~focus on the content issues and the description of possible ways to produce this content for cross-border exchange, taking into consideration~~ 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, ~~documentation~~ health data collected at the point of care should ~~use these international standardised terminologies on which the Master Valueset Catalogue is based. In order to achieve a high quality of data and to avoid loss of information, it is recommended to integrate documentation into the MVC internationally agreed standardised terminologies at the HCP. This would enable a 1:1 transfer without loss of information.~~

~~The European Commission initiated three projects under Horizon 2020 to look at aspects of this: eStandards, OpenMedicine and AssessCT. The respective outcomes will inform future~~

~~developments. The Commission is also engaged~~ take advantage of the preferred code systems proposed in ~~discussions with relevant SDOs regarding licensing arrangements~~the domain specific eHealth Network Guidelines.

~~*Article 10: Master Catalogue*~~

Article 12: Controlled Lists (Value set Catalogues)

Across Europe, there are different languages, different standards and ~~different coding schemes. In epSOS, this was addressed by the use of two master files: the Master Value Sets Catalogue (MVC), which applies across all Member States, and~~ code systems impacting health data. Even if each implementation should have the ~~Master Translation/Transcoding Catalogue (MTC).~~

~~The MVC are supported by an EU-wide Central Reference Terminology Server which will be maintained by DG SANTE. Each Member State needs its own local terminology repository as the MTC. If an update is~~ possibility to choose and define how to approach this challenge, effort should be made to ~~the central reference~~build on top of existing common health terminology ~~server, the local~~services. The eHealth Network and the Commission should make efforts to sustain and promote the usage of such common health terminology ~~repositories are notified and updated~~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

~~Internally~~ Member States ~~might base their national implementations on international standards such as EN13606. For~~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 ~~across borders, a shared document structure is needed~~in the Union.

Article 14: Security

Security includes general security of the connected networks and infrastructures. ~~Please consider referencing appropriate parts of~~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.

~~The diversity of national and regional healthcare systems, their structures, cultures and roles of health professionals are taken into account by a "common trust model", which provides the basis for interoperability via eHNCPs. These~~

~~entities are designated by the Member States and serve on the one hand as interfaces between the national and European requirements for exchanging personal health data, and on the other as guarantors regarding the origin and content of personal health data.~~

~~For security purposes logging of transactions, e.g. a health professional request for a Patient Summary, is an important feature. Unauthorised access to private medical data can be detected or prevented when a transactions log is available. Logged information in most cases consists of who has accessed information, when information was accessed, and what information was requested.~~

~~In most Member States, a tool is used to identify suspicious behaviour or other anomalies based on available logging data. Misuse of private medical data could be detected or even prevented using this functionality.~~

Article 15: Testing and audit

~~Member States will need to implement software to support cross-border exchange. One option would be to re-use the Open Source components developed in epSOS ("Open NCP") and released for all in the "JoinUp" EC-supported Open Source Community. These components can be adopted by participating nations and system integrators to build their own eHNCP solution.~~

~~The eHealth Network takes the decision about whether to admit an eHNCP to join the cross-border services on the basis of the audit report issued following the audit process as described in the OFW.~~

In order to ensure ~~monitoring~~testing and ~~evaluation of~~ auditing cross-border services and related interoperability provisions and systems, ~~Member States should:~~

- ~~consider setting up a monitoring facility for cross-border services to monitor, benchmark and assess progress on technical and semantic interoperability for their successful implementation;~~
- ~~undertake assessment activities, such as measuring the quantitative and qualitative possible benefits and risks (including economic benefits and cost-effectiveness) of services.~~

~~*Article 11: Amendments to the guidelines*~~

~~The eHealth Network will be responsible for agreeing amendments to~~ these guidelines will be provided in the domain specific guidelines. ~~It is expected that updates will be conducted following consultations with a wide range of stakeholders.~~