Co-funded by
the Health Programme
of the European Union

JASEHN
Joint Action to Support the eHealth Network

GUIDELINE

on

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

Release 2

General guidelines

Document Information:

Document status:	Adopted by the eHealth Network at their 10th meeting on 21st November 2016
Approved by JAseHN sPSC	Yes
Document Version:	V4.0
Document Number:	D5.3.1
Document produced by:	Joint Action to support the eHealth Network • WP 5 - Interoperability and Standardisation • Task 5.3 - Update & revision of EU eHealth Guidelines
Author(s):	Jeremy Thorp (HSCIC), Daisy Smet (ASE Luxembourg), Christof Gessner (GEMATIK)
Member State Contributor(s):	Austria, Finland, Germany, Greece, Hungary, Lithuania, Malta, Sweden
Stakeholder Contributor(s):	CEN IPS, COCIR, DG SANTE, EMA, European Society of Cardiology (ESC), Eurorec, Hl7 Foundation, Pharmaceutical Group of the European Union (PGEU), Results4care

TABLE OF CHANGE HISTORY

VERSION	DATE	SUBJECT	MODIFIED BY
1.0	2016-09-20	Draft submitted "for review" by JaseHN WP3	
2.0	2016-10-17	2nd draft submitted to sPSC	
3.0	2016-11-07	3rd draft following sPSC comments at sPSC meeting held on 27/10/2016	
3.1	2016-11-22	Apply final format	
4.0	2016-12-01	Formal language review	

TABLE OF CONTENTS

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:

(1) 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.

(2) 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.

(3) 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 guidelines on ePrescriptions.

(4) The Member States adopted Release 1 of the Patient Summary Guidelines in November 2013 and Release 1 of the ePrescription Guidelines in November 2014.

(5) 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.

(6) 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.

(7) 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.

(8) 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 health data. This supersedes Directive 95/46/EC.

(9) 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.

HAVE ADOPTED THESE GUIDELINES:

Chapter I – General Considerations

Article 1: Objectives and scope

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.

2. 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.

3. 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. 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 the internal market according to Article 114 of the Treaty on the Functioning of the European Union.

Article 2: Definitions

1. For the purpose of this guideline, the definitions of the directives 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 a *health professional* according 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].

[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.

Article 3: Concept and intended use

1. Each Annex to these guidelines describes Use Cases relating to the intended scope and purpose for cross-border exchange.

2. 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 adopt such requirements into local legislation;

(d) bear in mind these guidelines when adapting their 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 the protection of personal data and free movement of such data, and will be updated to reflect the requirements of the General Data Protection Regulation.

2. In the meantime, national legal frameworks 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.

3. 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.

Article 5: Authorisation, authentication and 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 health professionals who use cross-border services.

4. Member States may wish to consider the content of a register of health professionals who are entitled to prescribe and dispense, for instance:

(a) the name and profession,

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

(c) the current address of the health care provider organisation with which the health professional is affiliated or the address of his or her private practice,

(d) the date of issue of the healthcare professional's licence to practice,

(e) the speciality may be recorded in line with national practice as the prescribing of some medicinal products may be restricted.

Article 6: 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.

2. In the event of semantic transformation, both the transformed and the original documents shall for safety and audit reasons be available to all persons who are authorised to use this data.

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

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 the provisions of relevant European and national legislation. Where such provisions do not exist or are not in force, Member States are expected to implement, monitor and audit common policies, safeguards and measures representing agreements of the eHealth Network.

2. 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.

3. 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.

4. 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.).

5. The entry into operation of an eHNCP requires the explicit approval of the coordination mechanism established through the eHealth Network for the cross-border environment.

6. Non-EU countries may operate in line with Cross-Border Directive 2011/24/EU with the explicit approval of the eHealth Network.

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

Article 8: Quality standards and validation

1. Each Member State should apply such quality and safety standards as eHN might agree in the process of coding the information, such as validation checking.

2. In order to assure safe implementation, particularly patient safety and data protection, and further development of cross-border eHealth services, Member States should:

a) consider setting up a facility for cross-border services to quality assure, benchmark and assess progress on legal, organisational, technical and semantic interoperability for their successful implementation;

b) undertake assessment activities, such as measuring the quantitative and qualitative possible benefits and risks (including economic benefits, risks and cost-effectiveness) of cross-border services.

Article 9: Education, training and awareness

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

a) undertake activities towards increasing awareness of the benefits of and need for interoperability and related standards and specifications for electronic cross-border patient data exchange, including awareness of the need to foster the interoperability of technical systems among producers and vendors of information and communication technologies, healthcare professionals, health care providers, public health institutions, insurers and other stakeholders

b) pay particular attention to education, training and dissemination of good practices in electronically recording, storing and processing patient information

c) initiate appropriate, easy to understand information and awareness raising measures for all individuals, in particular patients

d) consider recommendations for education and awareness raising measures targeting health policymakers and health professionals.

Chapter IV - Semantic Considerations

Article 10: Data

1. Safe and secure cross-border care requires an ability to convey both meaning and context in data exchange. It is agreed that to achieve this, it is necessary to have structured and coded data for identified fields.

2. The responsibility for the *accuracy* and integrity of the process is with each national designated competent entity for such semantic processing.

Article 11: Terminology

1. The eHNCP must use the latest version of the Master Valueset Catalogue and the maintained national versions of these controlled vocabularies used in semantic transformation.

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 12: 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.

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 shall guarantee that all cross-border service requirements 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 14: Security

1. The eHNCP Security Policy Baseline creates a general security and 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.

3. The eHNCP shall take all reasonable steps to ensure data security (including data confidentiality, integrity, authenticity, availability and non-repudiation).

4. The eHNCP must ensure that cross-border data is not transmitted via these services to a Member State that either does not belong to or is not allowed into the cross-border environment.

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 establish an appropriate system of audit trail and shall

a) allow authorised official bodies to duly inspect the established mechanisms for data collection, processing, translation and transmitting

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

7. 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.

Article 15: Testing and audit

1. Member States will need to establish testing mechanisms that demonstrate compliance with 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).

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

3. The eHNCP shall establish and maintain an incident management solution to support health professionals, healthcare providers and citizens in its territory.

4. The eHNCP must ensure an auditing mechanism for legal, organisational, semantic and technical requirements.

Chapter VI – Amendments

Article 16: Amendments to the guidelines

The eHealth Network is responsible for updating the guidelines.

These guidelines are addressed to Member States.

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.

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.

Article 2: Definitions

The definitions section focuses on concepts which are common to cross-border health.

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.

Chapter II – Legal and Regulatory Considerations

Article 4: Data protection

The General Data Protection Regulation and its subsequent Delegated and Implementation Act aim to improve consistency and reduce diversity in data protection and rights including access to personal data and deletion or suppressions of sensitive information. As such, it could in the future abolish 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.

Article 5: Authorisation, authentication and identification

Issues of identification, authentication and authorisation of patients and health professionals involved in cross-border care relationships are crucial elements. To be able to link patients with their patient records, the existence of a patient identifier is necessary.

Besides having means to identify a patient, facilities to identify a health professional or health care provider organisation are a prerequisite for maintaining a high level of confidentiality for medical information when it is exchanged in a secure manner between other health professionals/health care provider organisations. The health professional/health care provider organisation identifier is linked to a digital identity which is issued by a certified authority. This identifier provides a base to create 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.

Member States will have to consider their approach to implementing digital signature services at the eGovernment or eHealth service level in the light of the electronic identification and trust services (eIDAS[3]) regulation adopted in July 2014.

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 of the health professional and/or health care provider organisation is also used for authentication purposes by a majority of Member States. Similarly, the majority make use of digital signing 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.

For most Member States, the digital identity of the health professional is linked to the health professional role, 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 of the health professional. In the majority of Member States, the health professional prescribing role or health professional medication dispensing role can be inferred from the digital 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 cross-border countries, in which:

- the responsibility for the *accuracy* and integrity of the process is with each national designated competent legal entity for such semantic processing
- liability 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.

[3] http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

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*** 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. 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 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 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. Each Member State must have a documented process for implementing changes of 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.

Article 9: Education, training and awareness

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

- national training materials and activities to be provided to support CBeHIS operation
- participating MS engage health professionals/health care providers in specification updates and other clinical concerns related to the operation of services
- participating MS inform citizens about CBeHIS provisions, including a description of the national infrastructure.

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.

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 existing national implementations.

To ensure the highest quality of data and to avoid loss of information, documentation 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 in discussions with relevant SDOs regarding licensing arrangements.

Article 12: Master Catalogue

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 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 made to the central reference terminology server, the local terminology repositories are notified and updated.

Chapter V – Technical Considerations

Article 13: Technical requirements

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

Article 14: Security

Security includes general security of the connected networks and infrastructures. Please consider referencing appropriate parts of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS directive).

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 and evaluation of 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 16: Amendments to the guidelines

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