# eHealth Network

## RECOMMENDATION

for a REQUEST of the eHealth Network to the
Article 29 Data Protection Working Party
for their Opinion on the
Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the
Criteria required for the participation in Cross-Border eHealth Information Services under the General Data Protection Regulation

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, Saint Julian's, Malta, 9 May 2017

-Keep this page free-

# Introduction

Since November 2015 JAseHN WP6 (Monitoring and Assessment of Implementation) T6.2 (Development of legal interoperability in a cross-border context) continued the work done by the legal sub-group established by the eHealth Network (eHN) in November 2014. Main objective of this task is to create a stable and secure legal environment for cross-border data exchange. The activities of T6.2 mainly focusing on drafting a multi-lateral agreement that shall serve as a sustainable legal support for cross-border exchange.

The task succeeded in presenting a final draft version of the *AGREEMENT between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross Border eHealth Information Services* (CBeHIS) *(later on referred to as AGREEMENT).* In addition, there will a *RECOMMONDATION PAPER for the Implementation of AGREEMENT between the National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross Border eHealth Information Services (later on referred to as IMPLEMENTATION GUIDE)*.

There are remaining open legal issues identified to the final draft version of the *AGREEMENT*, which will be presented to the eHealth Network with in *Explanatory Note* in addition to the final draft version of the *AGREEMENT*. One of these open legal issues is how to ensure data protection and the data subjects´ rights via the CBeHIS under the General Data Protection Regulation (GDPR), which shall apply from 25 May 2018 and is to be implemented by the Member States. With this regard, a number of Member States have declared as a prerequisite to sign the *AGREEMENT* to have an input from the Article 29 Data Protection Working Party (Art. 29 WP). Therefore there is the *RECOMMENDATION for an Intermediate Adoption of the AGREEMENT by the eHealth Network* and to agree on to revise the *AGREEMENT* after having more clearance on the GDPR implementation and once the Opinion/Guidance of the Art. 29 WP have been received.

The new legal group as described in the *IMPLEMENTATION GUIDE* must have then be assigned with the additional task to facilitate the discussion and revision process after having more clearance on the implementation of the GDPR and after having received the Opinion/Guidance of Art. 29 WP. As the result of the revision process, legal group would pass an amendment proposal to an eHN member or Contracting Party for proposing this amendment to the Governing Body. The legal group would also be responsible in supporting the eHN and the eHN´s secretariat in communicating towards Art. 29 WP if it has any questions towards the eHN and thus supporting the eHN´s secretariat in ensuring a smooth and rapid consultation process.

The eHealth Digital Service Infrastructure (eHDSI or eHealth DSI) is the initial deployment and operation of services for cross-border health data exchange under the Connecting Europe Facility (CEF) building on the experience of previous pilot projects such as epSOS. eHDSI sets up and starts deploying the core and generic services, as defined in the CEF, for Patient Summary and ePrescription. The generic services are the necessary implementation of data exchange at country level, the core services at EU level. These together enable the provision of Cross Border eHealth Information Services (CBeHIS). The eHDSI is financed by the Member States and the European Union through the CEF programme.

## Legal criteria in the current version of the Agreement

The final draft version delivered by JAseHN T6.2 of the *AGREEMENT* refers as legal criteria to Union and national law compliant to Directive 2011/24/EU and the Regulation 2016/679/EU, in particular Article 9 thereof. It reiterates also, that Patients must be provided by the Contracting Parties with the information pursuant to Articles 13 and 14 of the Regulations. In addition, the *AGREEMENT* foresees clauses to ensure the unambiguous identification and authentication of patients, health professionals and healthcare providers as well as liability, applicable law and jurisdiction.

A non-binding further *Guidance Paper on data protection* with regard to the GDPR was drafted by the European Commission (DG SANTE liaising with DG JUST) in cooperation with JAseHN T6.2 drafting team, which was first referred to in an earlier draft of *AGREEMENT*. However in order to prioritise the *AGREEMENT* and because it was held, that the approach taken in the *Guidance Paper* was not yet found consensus acceptance, the reference was deleted. Furthermore, it is planned to provide Contracting Parties with a Model Patient Information Note. Again, in order to prioritise the *AGREEMENT* JAseHN T6.2 agreed to present only a *basic concept for Model Patient Information Notice (Model PIN)* to the eHN, so that the legal group, as proposed in the *IMPLEMENTATION GUIDE,* needs to finalise the task.

**Legal criteria in the final draft version of the Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross Border eHealth Information Services (CBeHIS)**

Clause II.1.1

Data protection and security

Clause II.1.1.1

Legal basis for the cross-border processing and patient information

(1) The processing of personal data concerning health for the purpose of cross border healthcare pursuant to Directive 2011/24/EU via CBeHIS is lawful in compliance with the conditions stated in Regulation 2016/679/EU, in particular Article 9 thereof, and national law compliant with the stated Regulation. Further processing of these data according to Article 6 paragraph 4 of Regulation 2016/679/EU shall be excluded.

(2) Each Contracting Party shall ensure that patients are provided with the information pursuant to Articles 13 and 14 of Regulation 2016/679/EU.

Clause II.1.1.2

Identification and authentication of patients, health professionals and healthcare providers

(1) In order to enhance patient safety and privacy in cross-border healthcare, Contracting Parties shall ensure the unambiguous identification of patients, health professionals and healthcare providers, without prejudice to Regulation 2014/910/EU:

a.) Contracting Parties using electronic means of identification that are notified under Regulation 2014/910/EU and applicable to the health domain, shall adhere to this Regulation, its Implementing Acts and the documents that are referred to in the Annex.

b.) Contracting Parties using non-electronic means of identification, or using electronic means of identification not notified under Regulation 2014/910/EU, or using electronic means of identification that are notified under Regulation 2014/910/EU but not applicable to the health domain, shall adhere to the relevant documents listed in the Annex.

(2) Each Contracting Party shall ensure that it uses means of authentication that are adequate to the sensitivity of personal data concerning health according to Regulation 2014/910/EU and Regulation 2016/679/EU.

Clause II.1.1.3

Authorization of health professionals

Each Contracting Party of a Country B shall ensure that for the purpose of cross border healthcare only health professionals authorized according to its national law may have access to patients' data concerning health, without prejudice to other lawful grounds for processing under Regulation 2016/679/EU.

Clause II.1.2

Liability, applicable law and jurisdiction

(1) The civil liability of each designated NCPeH as Generic Services under the responsibility of the Contracting Parties is determined by the liability regime in accordance with the applicable law and competent jurisdiction.

(2) The Contracting Parties do not assume any liability for Core Services as described in the documents that are referred to in the Annex.

## Recommendation for Request to Article 29 Data Protection Working Party

While it is intended by the eHN that the *AGREEMENT* shall not interfere with Union and Member States law, Member States have declared at the same time the need for further guidance on how the Contracting Parties can and should make use of the GDPR with regard to the CBeHIS and the services of Patient Summary and ePrescription.

Some Member States have asked whether the *AGREEMENT* is considered a framework agreement and whether concrete terms need to be defined in addition under such a framework agreement. Though it is intended to have only one multi-lateral *AGREEMENT*, it is a valid to question, whether and to what extend the *AGREEMENT* satisfies the obligations of data controllers under the GDPR for instance to send data from one data controller to another data controller across borders (whether that is the NCPeH as a data controller or a data processor). It needs to be discussed after having more clearance of the implementation of the GDPR to what extend a more concrete approach in the *AGREEMENT* can be taken in conjunction with a *Guidance Paper*, that may be referred to through the Annexes.

Due to the different legal grounds possible in the Member States involved (especially the option to introduce national law for further processing), and the possibility of Member States to restrict the rights of the data subject, it is not fully clear, how the data subject can

exercise control of the use of his or her own health data and exercise its rights across borders via the CBeHIS under the GDPR.

In its Opinion 189 dated with 25 January 2012 the Art. 29 WP gave guidance on the implementation of the previous ePSOS pilot project, where it was recommended to be based on two-steps-consent.[1] The Art. 29 WP also gave an early input on the processing of personal data relating to health in electronic health records (EHR) in its Opinion 131 dated with 15 February 2007.[2] However, since these Opinions were given before the GDPR, an updated Opinion/Guidance of the Art. 29 WP is needed.

**Therefore, it is recommended that the eHN agrees to send the following request to the Art.29WP:**

Subject: Request by the eHealth Network to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, established under Article 29 of Directive 95/46/EC

Dear Chairman [*Name*] of the Working Party,

The eHealth Network, established under Article 14 of Directive 2011/24/EU,

Having regard to

- The Guidance of the Working Party in its Working Document 01/2012 on epSOS as adopted on 25 January 2012,
- The transposition of Directive 2011/24/EU into Member States' national laws by 25 October 2013,
- The entry into force of Regulation 2016/679/EU that shall apply from 25 May 2018,
- The current discussion in the Commission expert group on the Regulation 2016/679/EU and Directive 2016/680/EU,
- The Charter of Fundamental Rights of the EU, notably Articles 8 and 35 thereof, given that everyone's right to the protection of personal data must be duly balanced with the right of access to health care and to benefit from medical treatment, in order to reach a lawful and equally practical solution for the cross-border processing of personal data concerning health,
- Article 168(7) of the Treaty on the Functioning of the European Union, pursuant to which Union action shall respect the responsibilities of the Member States for the definition of their health policy and for the organisation and delivery of health services and medical care, including the management of health services and medical care and the allocation of the resources assigned to them,

[1] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp189_en.pdf
[2] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf

- The Grant Agreement under the Connecting Europe Facility (CEF) – Agreement No INEA/CEF/ICT/A2015/1149608, notably the pressing timeline for its implementation by the Member States,

may hereby submit a request to the Working Party for its Opinion on the legal assessment under Regulation 2016/679/EU of the

**Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Services**

as intermediately adopted by the eHealth Network at its 11th meeting on 9 May 2017.

Sincerely yours,

[*Name*] [*Name*]

Commission co-chair Member State co-chair

Attachments to this letter:

- Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Services
- Documents that are referred to in the annex of the stated Agreement
- List of exemplary questions for consideration by the Working Party

**APPENDIX**

List of exemplary questions for consideration by the Working Party:

- Is the AGREEMENT compatible with European data protection law?
- How can the National Authority or National Organisation of country A ensure that the data subject enjoys a high level of rights across the Union via the CBeHIS taking into account the possible legal grounds in principle under GDPR and that Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health?
- Could the current intermediate version AGREEMENT together with the GDPR and Member States law compliant to the GDPR provide a sufficient legal basis for the NCPeHs or healthcare providers as data controllers (or data processors) in country A to send data to another data controller in country B abroad in conjunction with the unambiguous identification of the patient in country B?
- How is the data subject to be informed about any processing via the CBeHIS under the GDPR in country B, incl. further processing, if further use is not restricted?
- If the processing of health data in country A is based on consent (in conjunction with the necessary information about the CBeHIS and its purposes and level of minimum rights under the GDPR in other Member States), would processing on another legal ground other than consent in country B be covered by this consent and would further processing in the public interest, for scientific or historical research purposes or archiving purposes in country B be compatible according to Art. 5 (1) (b) GDPR, even though Art. 6 (4) GDPR does not refer to data processing based on the data subject´s consent.
- Can the National Authorities or National Organisations agree to exclude further processing via the CBeHIS under the GDPR in such an AGREEMENT and if this is held to be of an interference with Union or Member States law what other safeguards can be foreseen?
- How can the data subject exercise their rights after data has been transferred to country B?