Brussels, 11th April 2018

Mr Clemens-Martin Auer
e-Health Network Member State co-chair
Director General Federal Ministry of Health,
Austria

Subject: 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

Dear Mr Auer,

In June 2017, the eHealth Network submitted a request to the Article 29 Working Party (hereinafter the Working Party) for a legal assessment of the Agreement in question under Regulation 2016/679/EU. The said Agreement, adopted on 9 May 2017 by the eHealth Network, aims at establishing an European Interoperability Framework for Cross-border eHealth Information Services (CBeHIS) with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare in the Union as provided for by Directive 2011/24/EU on the application of patients' rights in cross-border healthcare (hereinafter the Cross-border Healthcare Directive). In particular, the Agreement stems from the fact that whereas organisational, semantic and technical interoperability have been worked upon by the eHealth Network, an overall interoperability legal framework was needed for the achievement of the objectives under the Cross-border Healthcare Directive (notably Articles 11 and 14 thereof). Therefore, the Agreement seems to be intended to materialise "the commitment" of Member States "to fulfil" the organisational, semantic and technical "criteria required for the participation in CBeHIS" which are described in the binding documents that are referred to in the Annex.

First of all, let me express the Working Party's general appreciation for the attention paid by the Member States and the Commission to the data protection and privacy aspects related to establishing an overall interoperability framework for purposes of cross-border healthcare, especially in the e-Health sector. Ensuring continuity of cross-border e-Health applications and services within the EU depends on the exchange of personal data concerning patients' health, in conjunction with the existing electronic healthcare information systems residing on the Member States. For this reason, the fundamental rights of the individuals in relation to their personal data should be safeguarded when their health data are processed and transmitted from one Member State to another for the provision of cross-border e-Health applications and services (see recital 25 of the Cross-border Healthcare Directive). The Working Party acknowledges that both the Member State of affiliation (where the patient is an insured person) and the Member State of treatment (where cross-

border healthcare is actually provided) are involved in this process and therefore share the responsibility of ensuring that the fundamental right to privacy of the individual is protected in accordance with the relevant data protection law (Articles 4 and 5 of the Cross-border Healthcare Directive).

Secondly, regarding your request to consider the said Agreement under the General Data Protection Regulation (hereinafter the GDPR), the Working Party welcomes your efforts to take already into account the provisions of the GDPR so as to ensure the continuing relevance of the established framework through the change of the applicable rules in May 2018. While recalling that it is not the Working Party's role to make any legal assessment of the aforementioned efforts in the light of the GDPR, we would like to draw your attention to some of the main issues that are relevant for the fully compliant implementation of data protection safeguards, bearing in mind that there may be other issues that are not covered by this letter.

In this regard, we thank the Legal Task Force of the Member States Expert Group (eHMSEG) under the eHealth Network for the letter dated 15 December 2017 and the additional documents and explanations provided to the e-Government subgroup. This further information and the detailed elements helped us to clarify some of the criticalities highlighted in a preliminary examination of the Agreement as carried out by the subgroup.

As you pointed out in your 15 December 2017 letter, Article 10 of the Cross-border Healthcare Directive foresees the exchange of information between Member States for its implementation and calls for the Commission to "encourage Member States, particularly neighbouring countries, to conclude agreements among themselves". Furthermore, regarding specifically the e-Health sector, Article 14 of the said Directive calls for the European Union to support cooperation and the exchange of information among Member States, through the e-Health Network (see the EC Implementing Decision 2011/890/EU). In this framework, the Working Party understands your engagement for developing common orientations for eHealth and facilitating interoperability between electronic health systems of different Member States, also by adopting the aforementioned Agreement which is open to the 'voluntary' signature of Member States.

<u>Legal basis for the exchange of health data between Member States</u>

Concerning the legal basis for the exchange of health data between Member States for the provision of CBeHIS, the Working Party would like to recall that each Member State (the Member State of treatment as well as the Member State of affiliation) shall ensure that the processing of personal data is conducted in a lawful manner, in compliance with the GDPR and the respective applicable national law. Therefore, on the one hand, the Member State of affiliation shall ensure that an adequate legal ground is in place allowing the health care providers to prepare the relevant health data of the patient with the intention to make them available in future to other health care providers in the framework of the Agreement and to transfer them to another Member State, according to the GDPR and the applicable national law. In addition, the Member State of affiliation shall guarantee that the patient is provided with adequate, correct and up to date information about the processing (collection, transmission, etc.) of his or her personal data and that (solely) the necessary and accurate personal data concerning health is securely transmitted to the Member State of treatment. On the other hand, the latter Member State shall ensure that the patient's health data is received/accessed on the basis of an adequate legal ground, again in conformity with the GDPR and its national law, and that it is processed in accordance with the aforementioned rules. Furthermore, in the Member State

of treatment it shall also be ensured that the patient is properly informed about the processing of his or her personal data and that he or she can exercise his/her data protection rights [1].

In such regard, it can be assumed that the provisions of Chapter IV of the Directive 2011/24/EU on the basis of which the Agreement has been adopted (notably Articles 11 and 14 thereof) would be implemented on a voluntary basis. Indeed, the deployment of e-Health systems is entirely a national competence and the measures on interoperability developed by the Member States together with the Commission within the e-Health Network "are not legally binding" but provide additional tools that are available for Member States to support patient access to eHealth application "whenever" they "decide to introduce them"[2].

In particular, a specific legal requirement, in accordance with Article 9.2 GDPR, is necessary for the supranational processing operations that are developed on top of the existing national eHealth systems for the purpose of cross-border healthcare by means of CBeHIS [that is provided, according to the Cross-border Healthcare Directive and the Agreement, via the eHealth Digital Service Infrastructure (eHDSI) and the National Contact Points for eHealth (NCPeHs)][3]. To this end the sole provisions of the Cross-border Healthcare Directive along with the Agreement do not appear to fulfil the necessary requirements set forth by Article 9 GDPR for the lawful processing of this special category of personal data. Nevertheless, in the light of Article 9.2.h GDPR, national transposition laws adopted by Member States on the basis of the Directive 2011/24/EU and the Agreement, combined with the general national provisions on eHealth, could be taken into consideration as an adequate ground for the lawful cross-border exchange of health data within the EU, if they provide for specific and suitable measures so as to ensure legal certainty and protect the fundamental rights of the individuals in relation to their personal data[4].

In this framework, the Working Party acknowledges that the legal requirements for the collection, access to and cross-border transmission of health data might not be the same in all Member States, taking into account the possibly different conditions, including limitations, among EU countries as allowed by Article 9.4 GDPR concerning the processing of health data as well as the differences with regard to the respective national e-Health systems. For example, in some Member States, the patient's consent, according to Article 9.2.a GDPR, or additional safeguards[5], like for instance the

[1] See Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare, OJ 2009 C 128/03, para 22.

[2] See Recital 56 Directive 2011/24/EU.

[3] We do not refer to the data processing for the purpose of cross-border healthcare carried out within each eHealth national system, which is not directly affected by the cross-border character of the health care provided. Therefore, we do not address all the possible implications related to the identification of an adequate legal ground arising from the fact that various actors, acting as data controllers, might be involved in such a processing within each Member State. In this framework, several legal bases under Article 9 GDPR could be taken into consideration for the lawful processing of personal data concerning health, such as the data subject's explicit consent or vital interest, or the necessity of the processing for purposes of medical diagnosis, or the provision of health care or treatment or the management of health care systems and services on the basis of Union or Member State law, or for reasons of public interest in the area of public health, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89.1 based on Union or Member State law.

[4] According to Article 9.2.h processing of special categories of personal data concerning health is allowed for healthcare related purposes if it is necessary for the purposes of "medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law", including processing of such data by the management and central national health authorities for the purpose of ensuring continuity of health care and cross-border healthcare (see also recital 53 of GDPR).

[5] For instance the 2-step-consent envisaged by the Working Document 01/2012 on epSOS adopted by the Working Party on 25 January 2012 (WP 189), pp. 7-8.

possibility to opt-out, might be envisaged by national law provisions as legal requirements for lawfully sharing data in the e-Health context among healthcare providers.

In this regard, the provisions of the Directive 2011/24/EU could be of help, since they seem to acknowledge that the protection of the fundamental right to privacy with respect to the processing of personal data should be ensured in each Member State, in compliance with the data protection EU rules as implemented in each national legal system[6]. Having this in mind, the Working Party recalls that, in the light of Article 1.3. GDPR[7], the differences in the respective Member States' legal frameworks described above (including additional conditions or limitations) should not hamper the cross-border exchange of health data within the EU for the provision of CBeHIS according to the Directive 2011/24/EU and the Agreement even when those conditions or limitations apply to the cross-border processing of such data[8].

Notwithstanding this assumption, we understand that, for example, if consent is required as a condition for the e-sharing of medical information under the legislation of the Member State of affiliation and such consent has not been provided prior to the patient's travelling to the Member State of treatment, the latter should**,** in cooperation with the Member State of affiliation, take all reasonable steps to enable the individual concerned to consent to the electronic transmission of his/her health data in order to allow the patient to benefit from cross-border healthcare. In this context the Agreement could further investigate possible and practical solutions for allowing patients to provide their consent - for instance in a secure way over the Internet- in the Member State of treatment (see the solutions already envisaged in the Annexes to the Agreement and in the documents referred to therein).

<u>The nature of the Agreement and its Annexes</u>

With regard to the nature of the Agreement and its Annexes, we acknowledge the clarifications provided as to the bindingness of the Agreement –with its legal, organisational, semantic and technical requirements laid down in the Annexes– on its signatories, i.e. the national authority or national organisations responsible for NCPeHs in each Member State. However, considering that different parties are involved in the processing operations related to the provision of CBeHIS (including health professionals, healthcare providers, dispenser of e-Prescriptions and other institutions), we would recall that each Contracting Member State should clearly identify all the actors involved in the electronic exchange of medical data along with their data protection responsibilities. This should include both the NCPeHs acting as organisational and technical gateways for the provision of CBeHIS, as long as they process personal data[9], and the Commission as the supplier of the network infrastructure provided for the transmission of health data - though only to the extent the latter role entails a certain degree of involvement in the processing of personal data also in terms of defining security and communication standards. Therefore, each Contracting Member State should ensure, according to the respective national legal system, that the requirements set forth by the Agreement and its Annexes are binding on all of the said actors.

[6] See Articles 4.2.e and 5.d Directive 2011/24/EU.

[7] "The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data".

[8] See Recital 53 GDPR.

[9] See Clause II.2 of the Agreement in question.

Data protection impact assessment

As for the safeguards to be put in place in order to ensure that the sharing of data for the provision of CBeHIS will be in compliance with the GDPR, it should be taken into account that the cross-border exchange of health data increases the risk of inaccurate or illegitimate data processing. Hence, the Working Party would like to draw the Member States' attention to the need to fully and comprehensively assess the impact of the envisaged processing on the protection of privacy and personal data under Articles 35-36 GDPR, to the extent such processing is "likely to result in a high risk to the rights and freedoms of natural persons" since it regards data concerning health processed on a large scale. Because of the cross-border character of the processing, it would be preferable that a Data Protection Impact Assessment (DPIA) is performed, in a collaborative manner, by the Member States before going live in order to facilitate the achievement of a coordinated approach; indeed, Article 35 GDPR provides that such assessment should be carried out prior to the processing and that a single evaluation may address a set of similar processing operations of personal data presenting similar risks. Furthermore, considering the potential impact on individuals' lives of the intended processing, it would also be appropriate to involve representatives of the data subjects, in order to take into account their views[10]. This being said, an alternative would be for the data protection impact assessment to be carried out by each Member State as part of the broader impact assessment required in the context of the adoption of the national measures transposing the Directive 2011/24/EU and implementing the Agreement (which would serve as legal basis for the cross-border exchange of health data). Regarding the framework that could be used for designing and carrying out a DPIA, the Working Party recommends referring to the Guidelines on Data Protection Impact Assessment (DPIA) as last revised and adopted on 4 October 2017 (WP 248 rev.01).

Security measures

Moreover, the Working Party took great interest in reading your additional documents and explanations on the envisaged security measures. In this regard, attention should be paid to the data retention periods set out in the Annexes to the Agreement, in particular relating to the personal data concerning ePrescription and eDispensation stored in the national infrastructures, as well as to log files (which seem also to contain personal data concerning health) - considering that this information should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed. While we acknowledge that personal data is to be processed in accordance with the law of the relevant Member State, it would be crucial to determine the entities that may be authorised to access the log files and specify the purposes for which they may be used so as to ensure a comprehensively high level of protection of patients with regard to the personal data concerning their health.

Appropriate measures to guarantee transparency and safeguard patients' rights

The circumstance that the personal data relating to the patients' health has been transferred to another Member State might make it more difficult for data subjects to understand whether, by whom and for what concrete purpose their data is being processed and thereby to exercise their rights in relation to these data; this is all the more the case if one considers the proliferation of the actors involved in the provision of CBeHIS and the technological background of the processing operations carried out in a cross-border setting of the eHDSI and of NCPeHs. In this context, an effective protection of the fundamental rights and freedoms of patients requires that these drawbacks should be mitigated by appropriate measures to guarantee transparency and safeguard patients' rights.

In this regard, the Working Party welcomes that the Legal Task Force is working on a Model Patient Information Notice (PIN) aiming at guiding Contracting Member States - according to Articles 13 and

[10] See Article 35.9 GDPR.

14 GDPR - on how to inform patients in a concise, transparent, intelligible and self-explanatory manner about the cross-border exchange of their personal data. More specifically, it seems from the documents submitted to the Working Party that a Model PIN should complement the Agreement as a recommendation for Contracting Parties[11] and could be provided online via an appropriate website at the discretion of the Contracting Parties, e.g. via the NCP according to Article 6 of Directive 2011/24/EU.

As for the patients' rights in relation to the their personal data concerning health, the Working Party acknowledges that these rights have to be exercised in accordance with the law of the relevant Member State. However, the Agreement should envisage possible solutions and identify best practices in order to facilitate the exercise of patients' rights, taking into account that the data subject might not be a national or resident of the Member State of treatment and that his/her data may derive from data controllers in other Member States. To this end, clear, concise and intelligible information should be made easily available to patients specifying the rights, conditions and practicalities according to the different legislations of the Contracting Parties in the language of each participating Member State[12].

Unambiguous identification and authentication of patients, health professionals and healthcare providers

With regard to the unambiguous identification and authentication of patients, health professionals and healthcare providers for purposes of cross-border healthcare, the Agreement states that Contracting Parties using electronic means of identification notified under Regulation 2014/910/EU and applicable to the health domain, shall adhere to the said Regulation. On the contrary, participating Member States that use electronic means of identification not notified under Regulation 2014/910/EU, or electronic means of identification notified under Regulation 2014/910/EU but not applicable to the health domain, shall adhere to the relevant documents listed in the Annex to the Agreement[13]. In this regard, the Working Party wonders if compliance with Regulation 2014/910/EU as required by the Agreement would be appropriate, since the cross-border eHealth services agreed on at this stage by the eHealth Network (and envisaged by the documents listed in the Annex) do not include online services and are provided accordingly only via access by the health professionals and healthcare providers to the respective national e-Health system in the relevant Member State[14]. In addition, the Working Party wonders if, once on line cross-border eHealth services are developed[15], adherence to the said documents will be adequate to provide a common, stable framework equivalent to Regulation 2014/910/EU for ensuring secure and trustworthy electronic identification and authentication.

Structure of the Agreement

In relation to the structure of the Agreement, the Working Party notes that the relevant requirements from a privacy and data protection point of view for the Member States' participation in CBeHIS are mentioned in the documents listed in the Annex. Moreover, the procedure set forth by the Agreement for amending the documents referred to in the Annex and their list is not equivalent

[11] The Model PIN is indeed set out in a separate template from the Agreement. It will not have the same status as other documents that are referred to in the Annex to the Agreement, since its use by Member States is not mandatory.

[12] See the Working Document 01/2012 on epSOS adopted by the Working Party on 25 January 2012 (WP 189), pp. 14-15 as well as the Guidelines on transparency under Regulation 2016/679 (WP260).

[13] See Clause II.1.1.2 of the Agreement

[14] At a this stage, the cross-border eHealth services agreed by the eHealth Network are Patient Summary for unscheduled care, ePrescriptions and eDispensations.

[15] Indeed, the Agreement and the documents listed in the Annex have been designed to be also operational in relation to further cross-border eHealth services agreed in the future by eHealth Network. Moreover, see Clause III.2 of the Agreement setting out the amendment procedure of documents referred to in the Annex and their list.

to the procedure provided for regarding amendments of the Agreement. Indeed, according to the Agreement, the amendments of the list and of the documents in question are not considered as amendments of the Agreement[16]. Therefore, it can be assumed that the documents addressing the relevant privacy and data protection issues do not have the same legal status as the Agreement. In this regard, the Working Party would like to draw your attention to the need for fine-tuning the procedure in question by providing for the mandatory notification to the Contracting Parties of the amendments made to the documents referred to in the Annex and their list as well as for the establishment of a transition period to allow the participating Member States to comply with the new requirements.

Further processing

Finally, the Agreement seems to exclude further processing of medical data processed in the Member State of treatment on the same legal basis according to Article 6.4 of the GDPR but not secondary use on a separate legal basis[17]. We understand the Agreement would restrict further processing to statistical, historical or research purposes based on a EU or national law under Article 9.2.j GDPR provided that the processing is subject to appropriate safeguards, in accordance with Article 89.

Given that Article 5.1.c of the GDPR provides that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes, the Agreement's provision aiming at excluding further processing under Article 6.4 GDPR seems to be misleading and unnecessary. In that regard, it has to be noted, that if a controller processes data based on consent and wishes to process the data for another purpose, that controller may need to seek a consent from the data subject for this other processing purpose (or else find a different lawful basis which better reflects the situation) as the original consent will never legitimise further or new purposes for processing18. Regarding the information to be provided by the Member State of treatment on further processing for the aforementioned purposes, we emphasise the need to inform the data subject of his or her rights and in particular the right to object to the processing (Article 21 par. 4 and 6), by clarifying that the exercise of those rights may not impair the requested treatment. The Working Party would also like to highlight that data controllers should pay attention to possible different applicable legal requirements for research envisaged by the legislation of Member States of affiliation19.

Sincerely,

On behalf of the Article 29 Working Party

Andrea Jelinek
Chairperson

[16] See Clause III.2 of the Agreement.
[17] See Clause II.1.1.1 of the Agreement
[18] See the Guidelines on Consent under Regulation 2016/679, adopted by the Working Party on 28 November 2017, par. 3.2.
[19] These requirements might include, for example, stricter safeguards for professional secrecy.