The legal framework and guidance on data protection under the Cross-border eHealth Information Services (CBeHIS)

T6.2 JAseHN – draft v.2 (20.10.2016)

The purpose of this document is to outline the data protection legal framework underlying the CBeHIS. Notably, the document demonstrates how the relevant patient consent principles and requirements are embedded into the current EU data protection acquis[1]. On the other hand, the EU acquis in this sector is complex and gives a wide margin of manoeuvre to Member States, leading to a broad national diversity in the way the rules are implemented.

Therefore, this document aims to respond – based on reflections in the drafting group - to the most pressing legal questions that need to be clarified to make the planned health data exchange to become reality. As such, this document could serve as an orientation as to which extent these issues need to be addressed in the preamble / legal text of the agreement or by "soft law" instruments clarifying the EU law. The document could also serve as a "first incarnation" of a possible legal guidance document in future.

1. Introduction

1.1. Data protection under the Cross-border Healthcare Directive

Safe transmission of personal health data is one of the essential preconditions for ensuring continuity of healthcare across borders. The EU legislator has clearly assumed that such data should be able to flow from one Member State to another while at the same time the fundamental right of privacy should be safeguarded.[2]

The Cross-border Healthcare Directive recognizes the protection of personal health data as a **shared responsibility** of the Member State of affiliation and the Member State of treatment:

- The Member State of **treatment** shall ensure that the fundamental right to privacy is protected in conformity of the national measures implementing the Union provisions of the protection of personal data (Directive 95/46/EC).[3]

- The Member State of **affiliation** should provide the patient with adequate, correct and up to date information about the transmission of his or her personal data to another Member State, together with ensuring the secure transmission of the data to this Member State. The Member

[1] The emphasis of this document is on the General Data Protection Regulation (679/2016/EU) that will replace the current Data Protection Directive 95/46/EC as from 25.5.2018. The real data exchange under CEF might already start before 25.5.2018 but realistically only afterwards. Therefore, it is suggested for now to refer only to Regulation (679/2016/EU) in the Agreement and eventually modify (via additional references to the Data Protection Directive 95/46/EC e.g. in footnotes) if exchange is foreseeable before 25.5.2018.

[2] Recital 25 of the Cross-border Healthcare Directive (2011/24/EU).

[3] Article 4(b)(e) of the Cross-border Healthcare Directive (2011/24/EU)

State of treatment should also ensure secure receipt of this data and provide the appropriate level of protection when data is indeed processed, following its national data protection law.[4]

Moreover, in context of the mutual assistance and co-operation in cross-border healthcare, the Directive foresees exchange of information between the Member States and calls for the Commission to "encourage Member States, particularly neighbouring countries, to conclude agreements among themselves".[5]

1.2. Personal health data under the Data Protection Directive

According to the Data Protection Directive (95/46/EC) personal data concerning health may either be processed on the basis of the **patient's consent** or on **any other** of the grounds for lawful processing of personal data (i.e. with no consent). [6]

According to Article 8(3) of the Data Protection Directive, processing is allowed for health-care related purposes "where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

While this provision is essentially kept in the new Regulation, there is an additional requirement: processing must happen on the basis of Union or Member State law:[7]

(h) "*processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, 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 or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;*

In its Opinion 189 the WP Art 29 recommended the epSOS pilot project to be based on **two-tier consent**. However, this has to be seen in the light of three important caveats:

1) The Opinion was given before the implementation of the CBHC Directive and it expressly assumes that national provisions will be adopted to comply with it.[8] As shown above, the CBHC Directive took privacy aspects into account.

2) The Opinion was given before the new GDPR that requires certain stronger safeguards to be set by Member State law for health data processing.[9]

---

[4] Opinion of the European Data Protection Supervisor, OJ 2009 C 128/03, para 22.
[5] Article 10 of the Cross-border Healthcare Directive (2011/24/EU).
[6] Article 8(2), (3) and (4) of the Data Protection Directive.
[7] Article 9(2)(h) of the GDPR. Paragraph 3 further specifies that *personal data […] may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.*
[8] Opinion 189, p.10.

3) The Opinion was based on the assumption that the epSOS pilot will "probably take place outside the specific purposes mentioned in Art 8(3) of the Data Protection Directive as interpreted by the WP 131".[10]

4) Earlier Opinion 131 of the same WP recognises that Article 8(3) could serve as a legal base for EHR (electronic health record) systems provided that :

- Processing of medical data is strictly limited to those medical and healthcare purposes mentioned therein and is carried out strictly under the conditions that processing is "required" and done by health professional or by another person subject to an obligation of professional or equivalent secrecy;[11]
- Given the relatively high risk scenario inherent in the EHR systems, additional/new safeguards beyond those required by Article 8(3) would be appropriate; considering the special need for transparency of such systems, the safeguards should preferably be laid down in a special comprehensive legal framework
- If the EHR systems are not based on consent, the patient's self-determination concerning when and how his data are used should have a significant role as a major safeguard; whereas consent as a legal basis would always have to be "explicit", agreement as a safeguard **need not necessarily be given in a form of opt-in** – the possibility to express self-determination could depending on the situation also be offered in form of opt-out/ a right to refuse.

1.3. Interim conclusion

Therefore, the legal base for the movement of personal health data across borders within the EU may either be **consent** or another legal ground laid down in law.

For the purposes of CBeHIS, these other legal grounds principally include the **medical diagnosis** and **provision of healthcare or treatment** and **vital interests** of the data subject or another person.

Processing of personal data concerning health has also other purposes based on public interest, such as ensuring high standards of quality and safety of healthcare, or public health research. Moreover, a **legal obligation** may also come into play, e.g. in some countries doctors have a legal obligation to collect personal health data for the purposes of electronic health records.[12]

Therefore, the protection of patient's privacy across the border should in principle be guaranteed by the combined effect of correct – although not necessarily identical -

[9] Article 9(2)(h), (i) and (j) as well as Article 89 as regards processing for scientific research/archiving/statistical purposes.
[10] Opinion 189, p.5.
[11] Opinion 131, p.11.
[12] These alternative legal grounds are stated in Articles 6(1) and 9(2) of the GDPR. This is also recognised in the Charter of Fundamental Rights, Article 8(2): "Such data must be processed fairly for specified purposes on the basis of the consent of the person concerned or some other legitimate legal basis laid down by law"…

implementation of both the Cross-border Healthcare Directive and the Data Protection Directive.

Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.[13]

This practically means that the principle of **mutual recognition** should prevail. Each patient will in the first place enjoy the EU level and rights of data protection in Member State A, ie his Member State of affiliation. At a second step, the patient is subject to the data protection rules in the Member State of treatment.[14] This is in line with the CBHC Directive that assumes the law of the Member State of treatment to apply to the healthcare received in another Member State. Of course, the equivalent level of protection under the GDPR must be guaranteed in all cases.

2. Consent as a legal basis

Those Member States that use consent as a legal basis will need to apply the relevant consent principles as implemented in their national law.[15]

In general consent must be "a freely given, specific, informed and unambigious indication of the data subject's wishes by which he or she, by a statement or a clear affirmative action, signifies agreement to the processing of personal relating to him or her".[16] In addition, any consent for processing of data concerning health must be 'explicit'.[17]

An important precondition for a valid consent is that the data subject has received information which satisfies the requirement of Article 13 and 14 Of the GDPR.[18]

3. Healthcare legal basis

Instead of consent, Member States may use national law based on Article 9(2)(h) GDPR – current Article 8(3) of the Directive[19] - as a legal base for cross-border health data exchange:

[13] Article 9(4) and corresponding Recital 53 of the GDPR.

[14] This also applies to the case of vital interests: Member State A is expected to recognise the judgment made on the applicability of this ground in Member State B. Otherwise it is difficult to see how the system could work.

[15] See WP 131 in the first place. It is to be noted, however, that the consent principles included in WP 189 (epSOS Opinion) are not fully applicable in a system based on alternative legal bases (consent / other ground prescribed in law).

[16] The definition of 'consent' in Article 4(11) of the GDPR.

[17] Article 9(2)(a) of the GDPR.

[18] For further details see WP 189, p.7-8, that should be taken as a basis for the upcoming Model Information Notice.

[19] The general public interest ground in Article 8(4) of the Data Protection Directive is in principle also possible. This corresponds to Article 9(2)(g) in the GDPR: "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

"(*h) processing is* ***necessary*** *for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, 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 or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;*

As already stated above, processing of medical data must strictly be limited to those medical and healthcare purposes mentioned in that legal base and must be carried out strictly under the conditions that processing is **necessary** and done by health professional or by another person subject to an obligation of professional or equivalent secrecy.

Normally these conditions should be reflected in the national law that constitutes *sine qua non* for processing under this legal base. The national legal framework may also include additional specific safeguards for this kind of processing given its high risk scenarios.[20] Highly sensitive data (such as genetic data) may require additional safeguards.

It is to be noted that although consent is not used as a legal basis, the most important safeguard here should be respecting self-determination: Member States may use opt-out systems provided there is adequate information to the patient[21] (see below point 6.2 for details on the patient's right to opt-out).

4. Vital interests as a legal basis

Article 9(2)(c) GDPR - the current Article 8 (2) (c) of the Directive 95/46/EC – stipulates that the processing of sensitive personal data can be justified if it is "*necessary in order to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent"*. The processing must relate to essential individual interests of the data subject or of another person. The scope of this exception should be narrowly defined as to when and how it can be applied. Also, technical measures should be employed in order to prevent misuse of the emergency case.[22]

In its Opinion preceding the GDPR and the CBHC Directive, the Working Party recommended that this exception be applied only to a small number of cases of treatment and only where the first consent of the two-steps-model has been given.[23]

From a legal perspective, the question on whether patients may, as long as they are capable of doing so in Country A, exclude data access for emergency cases in Country B or not, will depend on the national law of Country A: if Country A requires the patient's consent (to the transmission of his or her data to Country B), and the patient does not give the consent, this

[20] As stated by WP 131. See also Article 9(4) of the GDPR that expressly allows Member States to « maintain or introduce further conditions, including limitations, with regard to processing of genetic data, biometric data or data concerning health". Recital 53 specifies that, "however, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data".

[21] WP 131, p.14. However, potentially extra harmful data (e.g. psychiatric, abortion) might require opt-in approach.

[22] WP 189, p.8.

[23] Opinion 189, p.8.

patient's data must not be transmitted to any Country B, independently from the legal basis required in Country B for the processing of the patient's data there (vital interests or any other legal basis).

This legal assessment is well in line with the technical perspective: the patient's consent, if required by the law of Country A, is recorded in the national infrastructure of Country A which is verified by NCPeH/A, and if consent is not given and recorded, the patient's data is not disclosed to the requesting NCPeH/B.

The data subject should be informed about this possibility in advance.[24]

In this situation it is especially important that the patient is given access to information about the transmissions that have taken place.[25]

5. Storage period

The Working Party's[26] recommendation on epSOS (decision to be taken on termination procedures and the maximum retention period) has to be seen against the background that possible storage of data in national infrastructure of Country B was outside the epSOS use case and therefore not considered.

Maximum retention period and procedure as to what should happen to the data at the end of the retention period differs between Member States (even within single Member States), depending on categories of data, HCPs (hospitals, established physicians etc.).

In line with the principle of mutual recognition (see Chapter 1.3.) and non-interference with national law, the personal data is to be processed in accordance with the law of the relevant Member State. This should also apply to storage periods. The other Contracting Parties must recognise the differences while the minimum of the GDPR must always be guaranteed.[27]

To regulate the duration and procedure for the retention time in the agreement would theoretically be possible as consensus indeed but the solution must not interfere with national law. Moreover, it seems to be [technically] impossible to distinguish in the physician´s infrastructure between "usual" patient data and those processed for CBeHIS.

6. Rights of the patient

The protection of personal data is a fundamental right.[28] Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.[29] Both

[24] To be taken into account in the Model Information Notice.
[25] See Article 12 of the GDPR.
[26] WP 189, p.9.
[27] Article 5(1)(e) of the GDPR requires personal data to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; longer periods are allowed for archiving purposes for public interest, or scientific or historical research or statistical purposes, subject to specific safeguards in Article 89.
[28] Article 8(1) of the Charter of Fundamental Rights ; Article 16(1) of the Treaty on the Functioning of the european Union (TFEU).
[29] Article 8(3) of the Charter of Fundamental Rights.

of these rights are essential in the sector of healthcare and they are further specified in the GDPR.[30]

Data subjects also have a right to erasure ('right to be forgotten') and the right to data portability.[31] Moreover, there is a right to impose a 'restriction of processing' e.g. where the accuracy of the personal data is contested by the data subject.[32]

For the purposes of the CBeHIS, the starting point must therefore be the definition of these rights in the GDPR and the fact that there will be slightly variable level of protection in the Member State of affiliation (country A) and the Member State of treatment (country B), while the minimum data protection under the GDPR must always be guaranteed in both countries.

The Contracting Parties have to make clear towards patients who is the controller responsible for making these rights operational (as it will be included in the Model Patient Information Notice; see next point).

6.1. Right to be informed

6.1.1. Personal healthcare

The most relevant information requirements for the primary healthcare purposes are the following.[33] The right to be informed applies no matter whether consent is required or not.

- the identity and the contact details of the controller;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the recipients or categories of recipients of the personal data;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

These rights are to be specified in the Model Patient Information Notice to be set-up on a website.

[30] Articles 15 and 16 of the GDPR.
[31] Articles 17 and 20 of the GDPR.
[32] Article 18(1)(a) of the GDPR. Presumably, national laws or programmes may exist in order to maintain the integrity and trust into the data in electronic health records.
[33] See Articles 13 and 14 of GDPR.

Beyond Regulation 2016/679/EU, also Directive 2011/24/EU (cf. Art. 4, 5 and 6) requires information to patients from HCP and NCP according to Art. 6 Directive 2011/24/EU that must be distinguished from NCPeH relevant for CBeHIS under the Agreement. Since the information requirements under Regulation 2016/679/EU serve different aims than those under Directive 2011/24/EU, i.e. transparent data processing vs. assessing quality and safety standards of foreign HCP and reimbursement of costs of cross-border healthcare, and given that the latter are outside the scope of the Agreement, the information requirements under Directive 2011/24/EU are not covered by the Agreement. Contracting Parties are however free and even encouraged to exploit potential (organizational and functional) synergies arising from the organisation of NCPeH and NCP as well as information requirements under Regulation 2016/679/EU and Directive 2011/24/EU, as long as the criteria required for the participation in CBeHIS under the Agreement are fulfilled. However, the Agreement does not prescribe this in order to not interfere with MS' internal organisation of NCPeH and NCP and thus national law.

6.1.2. Public health and scientific research

Member States may allow processing of personal health data for public health purposes (such as ensuring the quality of health care and protecting against health threats) and more specifically for research purposes as well as statistical and archiving purposes. These purposes cannot always be foreseen or specified at the moment of first processing (the so-called 'further processing').

These legal grounds for processing are described as follows in Article 9(2) of the GDPR:

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary 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 which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Both of these legal grounds require the national law to provide for suitable and specific privacy safeguards. Special safeguards apply in case of processing for scientific research purposes.[34] This effectively means that the safeguards may vary from Member State to

[34] The GDPR lays down reinforced privacy safeguards for such further processing, e.g. various technical and organisations measures such as pseudonymisation (Article 89).

another while the basic safeguards of the GDPR provide for a minimum level of data protection.[35]

As a main rule, GDPR stipulates that processing for scientific research purpose shall be considered compatible with the initial purpose, such as processing for personal healthcare.[36] However, where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose (and with any relevant further information).[37]

Again, in line with the principle of mutual recognition (see Chapter 1.3. and 5) and non-interference with national law, each processing of personal data should happen in accordance with the law of the relevant Member State.

Transparent information should be available on the regimes of secondary processing in each Member State. The patient should be informed about these regimes in each country. In such a way the patient has a possibility to refuse the processing of his/her personal data in a given country. Ideally, such information requirements would be outlined in the Model Information Notice.

6.2. The right to object

In Member States where consent is required for cross-border data exchange the patient has the right to withdraw consent at any time.

Also in Member States were consent is not a requirement, patients must be informed about all initial and secondary purposes for processing (for the personal treatment/for the quality of public health/for public health research or so) and may then, on grounds relating to his or her particular situation, at any time object to processing. However, this right may be limited when the controller demonstrates compelling legitimate reasons for the processing which override the interest, rights and freedoms of the data subject.[38] Therefore, the legal agreement cannot lawfully *require* the patient's right to opt-out as this would interfere with EU and also national law. Neither does the Agreement forbid Member States to foresee opt-out in their national law.

This basic right to object in principle applies both in country A and in country B. It is

[35] Article 89(2) expressly recognises the right of Member States to derogate from the right of rectification (Article 15), right of restriction of processing (Article 18) and the right to object (Article 21) in case of processing for scientific and historical research purposes or statistical purposes.
[36] Article 5(1)(b) GDPR.
[37] Article 13(3) and 14(4) GDPR.
[38] According to Article 21(1) of the GDPR, the right to object applies in case of Article 6(1)(e) – performance of a task carried out in the public interest – and in case of Article 6(1)(f) – legitimate interests pursued by the controller or by a third party. Therefore, the right to object applies in case the Member State uses the need for healthcare or treatment as a legal base for processing personal health data within this system, since this is normally a task carried out in the public interest **[this assumption needs to be checked with JUST carefully**]. In case of Article 6(1)(d) - vital interest of the patient or another person – the right to object does not normally materialize.

expressly required that the right to object must explicitly be brought to the attention of the data subject, shall be presented clearly and separately from any other information.[39] It is to be noted that the Member State may set further conditions to the processing of personal health data through national laws.[40]

A special rule applies in case of data processing for scientific, historical research purposes or statistical purposes. In this case the patient has the right to object unless the processing is necessary for the performance of a task carried out for reasons for public interest.[41] Also here, Member State have relative wide margin of discretion. Therefore, it is essential that the patient in country A is informed about the differences of regimes in Member States for this kind of further processing.[42]

In addition, Member States have the possibility to restrict the right to object by legislative measures, but these restrictions must always respect "the essence of the fundamental rights and freedoms" and be necessary and proportionate measure in a democratic society to safeguard".

As demonstrated above, the principle of mutual recognition means that the level of protection may slightly vary depending to the Member State of treatment, while the minimum protection of the GDPR must always be guaranteed.

A Model Patient Information Notice will be prepared to ensure equal level of information throughout the Union.

Further topics such as data security may be covered by this document as desired by Member States.

[39] Article 21(4) of the GDPR.
[40] Article 9(4) of the GDPR. However, these further conditions should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data (the last sentence in recital 53 of the GDPR)
[41] Article 21(6) of the GDPR.
[42] Details will be included in the upcoming Model Information Notice.