Prior Checking Opinion on the Clinical Patient Management System of the European Commission (CPMS)

Case 2017-0804

***

The European Commission is responsible for the use and storage, in a software, of patient data relating to rare diseases across the European Union. Even if the whole processing operation is based on explicit consent, the privacy statement should be improved to reflect the legal basis and/or lawfulness of the processing operation as well as the exercise of rights of erasure and blocking. Further a retention period should be defined and/or a period in which the healthcare providers revise the need to keep the data and some security measures could be reinforced.

***

Brussels, 06 November 2017.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: +32 2-283 19 00 - Fax: +32 2-283 19 50

1) The Facts

The Clinical Patient Management System (hereinafter 'CPMS') is a web-based clinical software application developed for supporting the European Reference Networks (hereinafter 'the ERN') on rare, low prevalence and complex diseases (hereinafter "rare diseases'). These ERNs, of which there are twenty-four (24), are virtual networks of healthcare providers working in Europe, across national borders, in order to diagnose and treat patients with rare diseases.[1] Rare diseases have been defined those that meet a prevalence threshold of not more than five affected persons per 10 000.[2]

This software allows thus the exchange of information between healthcare providers[3] in Europe. The Commission manages this application, which has been developed by a subcontractor.

CPMS will thus contain medical data of patients that have rare diseases.

1.1 The users

There are two kinds of users of the CPMS system.

On the one hand, there are the staff members of the Commission who are responsible for the administrative and technical management, such as dealing with problems and security incidents, who are included as 'users' in the application software.

On the other hand there are the *real* users, this is the healthcare providers. These users belong to an ERN member hospital ('the centre'). In addition to them there may be local point of care specialists who belong to a non-member hospital (the 'guest users'). While the users that belong to a member hospital have direct access to the data of the application, the guest users only have access on a *need-to-do* basis and this access is given by the responsible ERN coordinator. For organisational purposes, the users will create 'panel requests' and 'panel leaders'.[4] Healthcare providers, as users, may create and participate in panels to cooperate on specific dossiers.

[1] Article 12 (1) of Directive 2011/24/EU of the European Parliament and the Council of 9 March 2011 'on the application of patients' rights in cross border healthcare' provides as follows: 'the Commission shall support Member States in the development of European reference networks between healthcare providers and centres of expertise in the member states in particular in the area of rare diseases. The networks shall be based on voluntary participation by its members which shall participate and contribute to the network's activities in accordance with the legislation of the Member State where the members are established and shall at all times be open to new healthcare providers which might with to join them provided that such healthcare providers fulfil all the requirements and criteria [...]' (OJ L 88/45 of 4.4.2011).

[2] See recital number 55 of the above-mentioned Directive (footnote 1).

[3] Article 3(g) of the above-mentioned Directive (footnote 1) defines healthcare providers as 'any natural or legal person or any other entity legally providing healthcare on the territory of a member state.'

[4] The guest users cannot be panel leaders.

Healthcare providers must first authenticate through an EU login in order to access the application. [5] The Commission (through the subcontractor) provides this access and it is thus directly responsible for the processing of the administrative data of the healthcare providers[6].

The Commission's authentication and identity management service is used to register users for access to the CPMS. After the creation of an EU-Login, the user's account is then authorized by using an e-service tool, the SAAS2 authorization service which is under the responsibility of the Commission[7]. This tool is used to authorise a limited and identified population at ERN level acting with precise roles; only authorised users are activated in the CPMS using this tool.

1.2 The categories of data

There are two categories of data processed in the CPMS.

The healthcare providers will first encode the real administrative data of the patient in CPMS under the heading 'identifying data'. These data are the following: name, surname, gender, date and place of birth and education level.

Subsequently, under the heading 'consultation request', the healthcare provider will pseudonymise the name of the patient and will substitute it by a nickname which should have no similarities with the real name of the patient. Other healthcare providers, working in other centres, will only have access to the nickname and the medical data, but not to the real data stored under 'identifying data'.[8] The medical data processed are the following: consultation request, episode description, rare disease diagnosis, comorbidities, phenotype and genetic features and bio banks, family history, health behaviours, allergy and other adverse reactions, history of past illness and disorders, special treatment intervention, surgical and transplantation history and medication. Images, pictures and videos may also be processed. De-identification methodologies are used to remove from the inserted images any tags that reveal the identity of the patient and substitute with their unique ID.

1.3 Pseudonymisation

From a technical point of view, the health data of patients are firstly inserted in the CPMS and subsequently pseudonymised[9]. When a new patient is created in the CMS an automatic ID1 is created by the system. This ID1 will then be stored either into the hospitals record of the patient or the user will substitute the ID1 with the hospitals ID record of the patient. On a second phase,

[5] Users will manage their own password and EU login.

[6] EU login username, first and last names, healthcare provider name, the hospital or centre, ERN name, professional email address and country.

[7] More precisely the Commission's Directorate General for Health and Food Safety.

[8] When enrolling the patient into the CPMS, the system automatically generates a unique ID for each patient. This ID is only visible for health professionals within a particular centre or hospital.

[9] Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

when the health care professional wants to enter the health data to create a panel for discussion he will choose a nickname for the patient. By substituting the ID1 with a nickname, the CPMS reinforces the layers of pseudonymisation. It has already been said that pseudonymised data is then passed to the other CPMS users for panel discussion and assessment of a patient file. Only the centre and the health care professionals have access to the ID1 of the patient. The other centres and users are able to see only the nickname of the patient. CPMS allows only users from the enrolling centre/hospital to delete patient data from CPMS.

1.4 Consent forms and access to data

In order to be included in the software application, the patient has to give explicit and unambiguous consent to his healthcare provider.[10] There is a form entitled '*patient consent form for data sharing in European Reference Network for Rare Diseases for Patient care and creation of rare disease registries.*' This consent form has three boxes: the first concerns consent for sharing data, the second is about consent on the inclusion in the database and the third is about the possibility to be contacted for research purposes. Patients have to sign directly either in the box providing 'I consent' or in the box entitled 'I do not consent'.

The healthcare provider who is responsible for including patient's data in the database cannot proceed to CPMS without indicating explicitly that the consent form was completed.[11] These forms are translated into all official EU languages. The consent forms are not uploaded in CPMS once they are filled in; they are kept by the healthcare provider.

Access is given only to the healthcare providers who have been first authenticated by the Commission and who have first obtained explicit written consent for uploading information. Neither the Commission nor the subcontractor have, at any stage, access to the patient data, as stated in a note signed by the Director, as data controller for the CPMS system.[12] In other words, no patient data is processed in the Commission authentication and identity management service, nor in the SAAS2 authorization service.

1.5 Retention period

There is no defined retention period for medical data inserted by healthcare providers; data will be kept as long as necessary.

[10] Consent has been defined in by the Commission Delegated Decision as: 'informed consent under the framework of European Reference Networks means any freely given, specific, informed and explicit indication of a subject's wishes by which he or she, either by a statement or by a clear affirmative action, signifies agreement to the exchange of her or his personal and health data between healthcare providers and Members of the European Reference Network as provided in this Delegated Decision.' See Article 2 (e) of the Commission Delegated Decision of 10 March 2014 'setting out criteria and conditions that European Reference Networks and healthcare providers wishing to join a European Reference Network must fulfil' (OJ L 147/1 of 17.05.2014).

[11] They have to tick a box for each kind of consent given. The Manuals for Use and other practical documentation state that the enrolment form cannot be saved unless the checkbox 'consent for care' is ticked indicating that valid consent has been given. There are three different boxes for consent which correspond to the three types of consent that can be given in the consent form.

[12] See 'Commission access to ERN-CPMS system'. Note for the file electronically singed on 1/09/2017 [Ares reference (2017) 4283273].

1.6 Security features

[....]

2) Legal analysis

This prior checking Opinion[13] under Article 27 of Regulation (EC) 45/2001[14] (the Regulation) will focus on those aspects which raise issues of compliance with the Regulation or otherwise merit further analysis. For aspects not covered in this Opinion, the EDPS has, based on the documentation provided, no comments.

The processing operation falls within Article 27 because it concerns processing of sensitive data, i.e. health data, and this may have an impact on the rights and freedoms of the data subject.

2.1 Lawfulness of the processing operation

It should be clarified from the outset that there are two distinct processing operations here. On the one hand, there is the collection and treatment of administrative data of the users by the Commission (via its subcontractor). Since processing of these data is merely administrative and relates only to identification data of healthcare providers, it does not fall within the scope of Article 27(2) of the Regulation and does not need to be prior checked.

On the other hand, there is the processing operation made by the healthcare providers that enter, access, modify, consult, and retrieve data of the patients.[15] This processing operation is carried out solely by the healthcare providers, who are responsible for collecting consent forms, but takes places in a support platform managed by the Commission. The Commission, through its subcontractor is responsible for the storage and security of the data and thus bears co-responsibility together with the centre of the healthcare provider treating the patient and processing the data. The Commission and the centres are thus co-controllers. The present prior checking opinion will focus only on this last processing operation, this is, the one carried out by health providers as it directly concerns health data in the sense of article 27 (2) (a) of the Regulation.

The processing operation is lawful on two different grounds.

[13] According to Article 27(4) of the Regulation, the EDPS has to provide his Opinion within two months of receiving the notification, not counting suspensions. The notification was received on 8 September 2017.The EDPS shall thus render his Opinion by 8 November 2017. By email of 8 September 2017, the Data Protection Officer (hereinafter 'DPO') of the Commission sent a notification for prior checking on the processing operation called Clinical Patient Management System (hereinafter, the CPMS).[13] By email of 14 September 2017 the EDPS acknowledged receipt of the notification and asked five additional questions. By email of 18 September 2017 the DPO of the Commission responded to the questions and proposed two different dates in order to make a demonstration of the system. The demonstration took place on 28th September at DG SANTE's premises.

[14] OJ L 8, 12.1.2001, p. 1.

[15] As already mentioned these data are pseudonymised for all healthcare providers except those of the hospital of origin.

First, based on Article 5(a) of the Regulation, the processing is necessary for the performance of a task carried out in the public interest based on the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof. The Directive 'on the application of patient's rights in cross border healthcare' sets up, in its Article 12, the European reference networks.[16] In addition, the Regulation establishing the third health programme[17] states that one of the priorities is to provide support for patients that are affected by rare diseases, which includes 'the creation of reference networks [...] Union wide information databases and registries for rare diseases based on common criteria.' This provides a legal basis for setting up CPMS.

Secondly, the processing operation is lawful because it is based on explicit consent and thus falls within article 5 (d) of the Regulation: the patients have to sign directly either a box that provides consent or either in a box that does not provide consent. Provided that there is a signature there is no room for ambiguity. The explicit consent of the patient constitutes the grounds for the lawfulness of the processing operation.

The EDPS takes note that, under the consent form, the patient has to give consent explicitly.[18] Further, the consent is divided into three items, and thus patients, for instance, may consent to share identified data but may not consent to being contacted about research. The EDPS considers this detailed and explicit manner of providing consent as a best practice. The consent has to be freely given, specific and informed[19] which seems to be the case given that it is the form provides as follows: 'If you chose not to give your consent this will not affect your care' and 'if you consent today you may withdraw consent later'. Further it is said '[...] even if you choose not to give your consent your doctors will continue to take care of you to the best of their ability.'

2.2 Data quality

It has already been said that there are two different sets of data here. First of all, there is the real data of the patient which contains the name, surname, and place of residence, place and

[16] See footnote 1.

[17] Regulation (EU) No 282/2014 of the European Parliament and the Council of 11 March 2014 'on the establishment of a third programme for the Union's action in the field of health (2014-2020) and repealing decision n.1350/2007/EC (OJ L 86 of 21.03.2014)'. Annex I point 4.2 provides the thematic priorities for funding among which "Support Member States, patient organisations and stakeholders by coordinated action at Union level in order to effectively help patients affected by rare diseases. This includes the creation of reference networks (in compliance with point 4.1), Union wide information databases and registries for rare diseases based on common criteria."

[18] Recital 12 of the Commission Delegated Decision mentioned in footnote 6 states that 'in order to ensure the exchange of personal data in the context of networks, procedures concerning informed consent for processing this data could be simplified by using one single common consent model that needs to be subject to the requirements set out in directive 95/46/EC with regard to the consent of the data subject.'

[19] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, adopted on 13th July 2011.

date of birth and level of education. Secondly, there is the nickname with the medical data, which may contain additional information related to the disease like images, videos, etc.

Pursuant to Article 4(1)(c) personal data must be 'adequate, relevant and not excessive in relation to the purposes for which collected and/or further processed'. This rule implies a necessary link between the data and the purposes for which the data are processed.

The EDPS considers that information on the educational level of the data subject collected under 'identifying data' is not necessary and relevant in all call cases for the medical purpose sought. It should thus be stated in the application that these data should be collected only if necessary for medical purposes.[20] In addition, there is the possibility that by collecting images and videos patient may become identifiable (e.g. facial images or names appearing in the imagery). The centres should thus ensure that the pictures and real names are blanked out as much as possible.

The EDPS recommends collecting the level of studies of a patient only if it is relevant and necessary for medical purposes. In addition pictures and other identifying information in videos and images should, as much as possible, be blanked out.

2.3 Information to data subjects

First, there is a privacy notice given to the users of the application, namely, healthcare providers, which is quite complete. Second, for the patients there is a consent form which contains a short privacy notice focusing on the data subject's rights. However, it fails to include all the elements listed in Articles 11 and 12 of Regulation 45/2001. In particular, it does not refer to the legal basis and/or lawfulness of the processing operation as well as the deadlines for exercising the rights of access and modification in case of errors. Further, it does not contain information about the rights of blocking and erasure[21], which should also be included. There is no information either on the retention period.

The EDPS thus recommends completing the 'consent form' by including information (in the form of a bullet point for each item, for instance) about the lawfulness of the processing operation, deadlines to exercise the rights, modalities for exercising blocking and erasure and a reasonable retention period.

2.4 Security of the processing operation

[20] This issue was raised during the meeting of 28 September 2017. The controllers of the application affirmed that this data may be important when there are mental health issues at stake, as well as when the patient is a doctor for instance that may better understand terminologies etc.

[21] However, it is true that the notification provides that the time to block /erase on justified legitimate requests from data subjects is four weeks.

The controllers of the processing operation are the healthcare providers (together with the Commission as co-controller). Nevertheless, the concept of healthcare providers does not only cover doctors but also 'any natural or legal person or any other entity legally providing healthcare on the territory of a Member State.'[22] Doctors are bound by confidentiality statements or similar. However it is not always clear that other healthcare practitioners are bound by the same rules. Therefore the EDPS recommends that the Commission, as co-controller, ensures that all users of the CPMS sign a confidentiality statement similar to the one of doctors.[23]

The EDPS recommends ensuring that all users of the CPMS sign a confidentiality statement or similar to the one of doctors.

The EDPS takes note that the patient's health data are included in pseudonymised form under a 'nickname'. This nickname has to be given by the healthcare provider, who receives instructions 'not to put any real data' in the form for enrolling patients. This instruction could be reinforced by stating more explicitly that the nickname should have no similarities with the real name of the patient. The EDPS welcomes that the controller, in the meeting of 28th September 2017, offered to provide technical means to ensure an automatic filter and rejection of nicknames that partially contain the name or surname of the patient.

The EDPS recommends the Commission to reinforce the instruction on the nickname by explicitly asking healthcare providers to ensure that it contains no similarities with the patient's real data.

[…]

2.5 Retention period

According to Article 4(1)(e) of the Regulation, personal data 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 were collected or for which they are further processed'. Personal data kept for longer for 'historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted'.

There is no defined retention period. According to the Commission, healthcare practitioners will store the data in CPMS as long as necessary.

The Commission should set up a reasonable period based on the purposes of the processing. The retention period could be different for data treated for diagnosis and treatment (which

[22] See footnote 3.

[23] In this regard see the 'EDPS Guidelines concerning processing of health data in the work place by Community institutions or bodies.' September 2009. These guidelines provide as recommendation the 'use of codes of conduct or confidentiality declarations for all persons involved in the processing who are not bound by a secrecy obligation.'

appear to be no longer relevant in CPMS after a final cure) and data treated for research (where patients have consented to that).[24] For the latter, the retention period could be longer provided that data are kept in a secured anonymised and/or encrypted way. Alternatively the Commission could ask the healthcare providers to review the need for keeping the data at regular intervals (e.g. every 10 or 15 years after the inclusion in the database).

The EDPS recommends setting up a concrete retention period in order to ensure that data are not retained longer than necessary. Alternatively, the healthcare providers who inserted the data could be periodically reminded to review the need for keeping the data.

Recommendations

In this Opinion, the EDPS has made several recommendations to ensure compliance with the Regulation. Provided that these recommendations are implemented, the EDPS sees no reason to believe that there is a breach of the Regulation.

For the following **recommendations**, the EDPS expects **implementation and documentary evidence** thereof within **three months** of the date of this Opinion:

- Collect the level of studies of a patient only if necessary and relevant for medical purposes. In addition pictures and aside information in videos and images should, as much as possible, be blanked out;

- Complete the 'consent form' by including information (in the form of a bullet point for each item, for instance) about the lawfulness of the processing operation, deadlines to exercise the rights, modalities for exercising blocking and erasure and a reasonable retention;

- Ensure that all users of the CPMS sign a confidentiality statement or similar to the one of doctors;

- Reinforce the instruction on the nickname by explicitly asking healthcare providers to ensure that it contains no similarities with the patient's real data;

- […]

- Set up a concrete retention period in order to ensure that data are not retained longer than necessary; alternatively, healthcare providers who inserted the data could be periodically reminded to review the need for keeping the data.

The EDPS welcomes the fact that the Commission has already started to implement some of the recommendations as a follow up of the meeting of 28th September.

[24] The above-mentioned guidelines state that 'as a general rules, as concerns conservation of medical data the EDPS considers that a period of 30 years can in most cases be considered as the absolute maximum during which data should be kept in this context.' (see point 4).

Done at Brussels, 06 November 2017

Wojciech RAFAŁ WIEWIÓROWSKI