Privacy Statement

European Reference Networks for Rare, Low Prevalence and Rare Diseases
Clinical Patient Management System (CPMS)

Contents

1. Introduction

The Clinical Patient Management System (CPMS) is a web-based clinical Software as a Service developed by sub-contractors of the European Commission and used by the European Reference Networks (ERN), which are networks of healthcare providers working together across national borders to diagnose and treat patients with rare, low prevalence and complex diseases in Europe. The objective of the CPMS is to support the work of the ERNs by providing the technical means to run virtual medical consultations.

The Commission also provides secure electronic systems to authenticate the users and to authorise access for healthcare professionals of the ERN member hospitals to access the CPMS.

This privacy statement covers the processing of three categories of personal data, namely:

- **Staff members of the Commission and their subcontractors**, who are responsible for the administrative and technical management of the system.
- **Healthcare professionals data** to permit them to access the CPMS system;
- **Patients personal data**, including data concerning health (health data).

2. On what legal ground do we process personal data?

All processing acts within the responsibility of the European Commission are governed by Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 (EDPR) on the protection of natural persons with regard to the processing of personal data by the Union Institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

The European Reference Networks are set up under the Directive on Patient Rights' in Cross-Border Healthcare 2011/24/EU that gives the Commission the mandate to support the ERNs' establishment, functioning and evaluation through the adoption of implementing measures. The Commission's Delegated Decision 2014/286/EU addresses the need for ERNs to have an efficient and secure exchange of health data and other patient information as well as personal data of the healthcare professionals for the successful functioning of the Networks. The Delegated Decision also defines the informed consent of the patient under the framework of the European Reference Networks to exchange his or her personal and health data between healthcare providers and members of a European Reference Network. The Implementing Decision (EU) 2019/1269, specifies the responsibilities of the Commission and of the healthcare providers that are together joint controllers of processing of personal data of patients in CPMS.

All legal acts regarding the ERNs are available here.

3. Which data are processed by the Commission in the CPMS?

As mentioned above, there are three categories of data processed through the CPMS system:

1. **Data of Staff members of the Commission and their subcontractors**
2. **Healthcare professionals data**
3. **Patients data**

The *staff members of the Commission and their subcontractors* are responsible for the administrative and technical management, such as dealing with problems and security incidents. They are users with restricted permissions in the application software.

The *healthcare professionals* are considered as *users* if they belong to an ERN member hospital or an Affiliated Partner*;* or they are considered as *guest users* if they are local point of care specialists belonging to a non-member hospital or Affiliated Partner. The *users* belonging 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[2].

On *patient's data*, it is the point-of-care healthcare professional who is responsible to enrol the patient in the CPMS and must therefore record that the patient completed the consent form in order to proceed with the consultation. When enrolling a patient a healthcare professional belonging to an ERN member will first encode the identifying data of the patient: last name, first name, gender and date of birth of the patient (place of birth will be soon included). Subsequently, when requesting a virtual consultation for a patient the healthcare professional needs first to enter a nickname for that patient which should have no similarities with the real name of the patient. For the time being, the nickname (pseudonym) is the only non-clinical information that is included in the virtual consultation. Healthcare professionals working in other centres will only have access to data relevant for the purposes of diagnosis and treatment (i.e. year and month of birth, medical images, laboratory reports, as well as biological sample data,area of birth, area of residence)..

[2] European Reference Networks Coordinator means the person appointed as the Coordinator of the Network by the Member of a European Reference Network chosen as the coordinating Member as referred to in recital 3 and Article 4 of Delegated Decision 2014/286/EU.

4. How are data processed?

The Commission's authentication and identity management service[3] provides a way for users (i.e. staff members of the Commission and healthcare professionals) of the CPMS to register for access to the CPMS. In a self-registration process, users are requested to create a user account using the EU-Login for the European institutions.

The user account is then authorised by using e-service tool, the SAAS2 authorisation service[4], which is under the responsibility of the Commission's Directorate General for Health and Food Safety. Please note however that the right to authorization is delegated from the Commission to the Network. 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.

The EU-Login requests the user to provide the following personal data: username, first and last name, professional e-mail address and country. Other optional data (such as a phone number) may also be stored in EU-Login.[5]

Please note that whilst personal data of *staff members of the Commission and their subcontractors* are included as users in the Commission database, their contact details are not published for the user community. Instead, a functional mailbox is used for facilitating contacts between users and administrators[6].

Furthermore, none of the patient data is processed in the Commission authentication and identity management service, nor in the SAAS2 authorisation service. *Patients data* are processed within the ERN exclusively through the CPMS.

5. What is the purpose of processing data in the CPMS?

Healthcare providers that are members of the ERNs, Affiliated Partners or guest users can exchange information within the Networks on the concerned patients with the aim of facilitating their access to safe and high quality healthcare and promoting effective cooperation on healthcare between Member States by facilitating the exchange of relevant information.

The CPMS processes sensitive data concerning patients suffering from rare or low prevalence complex diseases. These data are processed solely for the purposes of a) facilitating patient's diagnosis and treatment, b) for entering them into relevant registries or other databases for rare and low prevalence complex diseases, which serve a scientific research, clinical or health policy purposes and c) for contacting

[3] Record DPR-EC-03187 (Identity and Access Management Service – IAMS)
[4] Record DPR-EC-00176 SAAS (SANTE Authorization Service)
[5] https://webgate.ec.europa.eu/cas/privacyStatement.html
[6] This is SANTE-ERN-CPMS-ITSUPPORT@ec.europa.eu.

potential participants for scientific research initiatives. For all these three cases, the patient signs a specific consent.

6. Who has access to the data?

For Commission staff

Authorised Commission staff or internal or external contractors only have access to the personal data of the authorised users that are strictly necessary to carry out its tasks for administration and technical support purposes related to the user authentication and identity management service used by the CPMS.

A service directory of ERN members is available to the authorised users who have access to the system, including information about name, organisation, country, area of specialisation.

For healthcare professionals

Healthcare professionals have access to the pseudonymised health data of patients only for the purpose of diagnosis and treatment; whilst only the enrolling healthcare professionals will have access to the identifying patient data. Please note that the Commission shall not access personal data of patients unless it is strictly necessary to fulfill its obligations as joint controller. Staff members of the Commission and their subcontractors: they have access to such personal data of the authorised users that are strictly necessary to carry out its tasks for administration and technical support purposes related to the user authentication and identity management service used by the CPMS.

Healthcare professionals have access to the pseudonymised health data of patients whilst only the enrolling healthcare professionals will have access to the identifying patient data. The Commission will not access personal data of patients unless it is strictly necessary to fulfil its obligations as joint controller.

For patients

The patient can access its data via its point-of-care healthcare professionals.

7. How long will the data be stored?

For healthcare professionals & Commission staff data

Personal data of healthcare professionals and responsible persons of the CPMS recorded through the EU-login system are retained for as long as necessary and will be stored for as long as the person is recorded as an active user and for a period of one year thereafter. Personal data recorded through SAAS2 are retained for as long as necessary.

Please note that if healthcare professionals , are not able to delete their CPMS profile (including all associated personal data), but only to deactivate it, their personal data (Full name and specialization), together with any patient's pseudonymised data that have been uploaded in the system, will still be visible for purposes of patient care and diagnosis, even after the deactivation of their account. Please note that if a patient request for his/her data to be deleted, the panel data become anonymized (there is no possible way to retrieve patient ID with data kept in the CPMS) and therefore those data are considered as anonymized data, they are no longer personal data. Also, any health professionals from the same centers authorized in CPMS can delete patient record.

If, upon deactivation, a request is received from a patient exercising his or her data subject rights (e.g. full or partial consent withdrawal), the relevant ERN coordinator should be contacted.

For healthcare professionals who are guest users, their accounts are active for 90 days from the date of registration, unless different requirements are needed, in which case a shorter or longer period can be set. Once the end has been reached, the guest user account is deactivated and data is kept in exactly the same way as for the healthcare professional's accounts.

For patients data

Healthcare professionals authorised to access CPMS shall delete data no longer necessary. Personal data of the patients shall only be retained for as long as necessary in the interest of patient care, diseases' diagnosis or for the purpose of ensuring care with an ERN to the patients' family members. The data of a patient should therefore be periodically reviewed and deleted if no longer necessary. This shall be done, for each patient, every 15 years the latest, starting on the date of his/her enrolment.
The patient has the right to withdraw the consent given previously at any time, request the blocking or erasure of his/her personal details and request data portability.

8. Which security measures are in place against unauthorised access?

The Commission ensures that the CPMS complies with the requirements applicable to all IT systems at EU level on security of Information Systems and its implementing rules as established by the Directorate of Security for this kind of servers and services[7].

CPMS users' personal data are stored in a database hosted by the European Commission or its contractors with specific security protection measures (solely for EU Login and SAAS2 data), and in the CPMS for all data (hosted in the Commission's subcontractor data centre in Germany, with implemented standards on

[7] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017D0046&from=EN

secure processing). Only Commission authorized staff permitted to access to modify user data in the database through the authentication and authorisation systems (EU-Login and SAAS2).

All data in electronic format are stored either on the servers of the European Commission or of its contractors or sub-contractors; the operations of which abide by the European Commission's security decision of 16 August 2006 [C(2006) 3602] concerning the security of information systems used by the European Commission.

At the level of the CPMS, security measures applied include:

- Encryption: all patient data is encrypted
- Secure transfer: HTTPS protocol is used for secure transfer
- Authentication: EU Login – only users authenticated have access
- Authorisation: SAAS – only users authorised have access
- Hosting: user data is securely hosted.

In addition, staff holding the roles described in section 6 above are bound by confidentiality, data protection and non-disclosure agreements under specific contractual arrangements.

9. Access to personal data

The user can exercise the rights as a data subject (access, rectification, blocking, objection to processing and erasure) by contacting the data controller via the contact address below in point 10.

Personal user data collected via EU login can be manually modified and deleted by the user. The systems consequently erase the user data. Alternatively, access revocation can be requested by the user to the respective data controller. User data and the complete user profile are erased manually by the SAAS2 Processor in the SAAS2 system. The contact information regarding the data controllers for both systems is available below under point 10.

10. Additional information

A list of National Data Protection Authorities is available here. Please be aware that in some cases national law may contain exceptions to the exercise of your rights as a data subject. In case of doubt, please contact your national data protection authority.

You can find the records of processing operations mentioned above in the Register of the Data Protection Officer.

11. Contact

The CPMS is managed by the European Commission's Directorate General for Health and Food Safety. The contact address is:

Directorate-General for Health and Food Safety
European Commission
1049 Bruxelles/Brussel
Belgium
E-mail: SANTE-ERN@ec.europa.eu

If you have any questions or comments regarding SAAS2, or if you would like to exercise your rights as a data subject, please contact the controller, explicitly stating your request, at the following email address: SANTE-SAAS2@ec.europa.eu.

If you have remarks regarding the processing of your personal data under the Commission's responsibility you may contact the European Commission's Data Protection Officer at: data-protection-officer@ec.europa.eu.

If you want to file a complaint regarding the processing of your personal data, please contact the European Data Protection Supervisor.

European Data Protection Supervisor (EDPS) 60 Rue Wiertz
B-1047 Brussels
Belgium
phone: +32 2 283 19 00
e-mail: edps@edps.europa.eu