Privacy Statement (14 December 2017)

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

1. What is the ERN Clinical Patient Management System?

The Clinical Patient Management System (CPMS) is a web-based clinical software application developed by sub-contractors of the Commission with the objective to support the European Reference Networks (ERNs) on rare, low prevalence and complex diseases. The ERNs are networks of healthcare providers working together virtually across national borders to diagnose and treat patients with rare, low prevalence and complex diseases in Europe.

The CPMS provides a secure electronic system managed by the Commission to authenticate the identity of the users and to authorise access for healthcare professionals of the ERN member hospitals to collaborate in the cross-border assessment of a patient file.

This privacy statement covers solely the part of CPMS that concerns the authentication, authorisation, registration, storage, deletion and usage of the personal data of the CPMS users and guest users (i.e. the health professionals) to permit their access to the pseudonymised (no name, no address) patient file made available in the CPMS system.

The local point of care specialist may be an existing CPMS user (from an ERN member hospital or treatment centre) or a non-member hospital or treatment centre (a guest user). Guest users may have more limited access rights, which are attributed by the ERN coordinators on a "need-to-do" basis.

Neither the Commission, nor its contractors and subcontractors, have access, at any stage of the processing and/or storage operations, to any patient data. The encrypted data is securely stored, on behalf of the Commission, by its subcontractor in Germany, solely to ensure the proper functioning of the CPMS platform.

The patient's data is collected solely by the local specialist, i.e. the treating doctor, who must have obtained the explicit written consent of the patient to allow (i) for his or her pseudonymised data to be processed in the CPMS for the diagnosis and treatment of his or her condition in an ERN, (ii) to be included in the rare disease database or registry, or (iii) for the patient to be contacted for use of his/her data for a specific research project. [2]

All processing acts within the responsibility of the European Commission are governed by Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free

2 What is the applicable law?

movement of such data. The data controller of this specific processing operation (user management in the CPMS) is the European Commission.

The European Reference Networks are set up under the Directive on Patient Rights' in Cross-Border Healthcare 2011/24/EU which gives the Commission the mandate to support the ERNs' establishment, functioning and evaluation through the adoption of delegated and implementing acts. 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. All legal acts regarding the ERNs are available at https://ec.europa.eu/health/ern en .

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

The CPMS comprises two types of users, whose data is processed in the CPMS:

- CPMS users / guest users: healthcare professionals of ERN member hospitals / non-ERN member hospitals;
- Commission staff, for administrative and technical purposes (users managing access rights).

The same personal data categories are collected for both users and guest users.

The Commission's authentication and identity management service[3] [4] provides a way for users of the CPMS to register for access to the CPMS. In a self-registration process, you are requested to create a user account using the EU-Login for the European institutions.

The user's account is then authorised via a e-service tool, the SAAS2 authorisation service[2], which is under the responsibility of the Commission's Directorate General for Health and Food Safety. 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.

Guest users, on the other hand, can be invited and authorised by the coordinator of a specific ERN to have a guest account in order to complete patient enrolment in the CPMS ring-fenced app or to participate in virtual panels due to their specific expertise.

The EU-Login requests the user / guest user to provide the following personal data: username, first and last name, organisation details (healthcare provider name), professional e-mail address and country. Other data (such as phone number) may also

[3] **Notification to the DPO 839.4 (Identity and Access Management Service - IAMS)**
[4] **Notification to the DPO 2065.4 SAAS (SANTE Authorization Service)**

be stored in EU-Login[5], namely for the purpose of the two-step authentication process.[6] The CPMS does not store phone numbers.

The personal data of Commission staff responsible for the administrative and technical management (i.e. dealing with problems and security incidents) are included as users in the Commission database. The only personal data processed is the one collected by EU-Login. Their contact details are not published for the user community. Instead, a functional mailbox is used for facilitating contacts between users and administrators.

No patient data is processed in the Commission authentication and identity management service, nor in the SAAS2 authorisation service.

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

The objective of the CPMS is to support ERN users to collaborate on the medical assessment of a patient file for treatment and diagnosis across national borders.

5. Who has access to the data?

Authorised Commission staff or internal or external contractors only 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.

The data subjects (the users / guest users) have access only to view and to directly modify (change, delete in EU Login or deactivate in the CPMS) their personal details. In very specific situations (e.g. in order to ensure the exercise of patients' rights in the absence of a user/guest user), ERN coordinators may have access to users / guest users personal data.

A service directory of ERN members is available to the authorised users / guest users who have access to the system, including information about name, organisation, country, area of specialisation. In this way, recipients of this data can build the most effective panels of relevant specialists to diagnose and care for patients.

A notification of this processing operation was made to the Commission's Data Protection Officer and is available for consultation in the DPO register[7] [8].

6. How long will your data be stored?

[5] **http://ec.europa.eu/dpo-register/details.htm?id=42750.**

[6] **A) ECAS Mobile App PIN code, B) ECAS Mobile App* QR code, C) on mobile authentication, D) Mobile phone + SMS. For all these options a mobile device has to be registered with EU Login not with CPMS**

[7] **http://ec.europa.eu/dpo-register/search.htm**

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

A user's personal data in the CPMS is retained for as long as the user's account is active in the system. Certain user data categories (full name and specialisation), as well as any pseudonymised patient data imputed into the system, are also retained and visible in the CPMS after a user decides to deactivate its profile, for the purpose of ensuring the ongoing care of the patient and/or to contribute to the care and diagnosis of another patient. Any patient data will be kept in the system for a period of 15 years, subject to review. The healthcare provider organisation will be reminded by the system shortly before the expiry of the 15 years period to review any uploaded patients' data and determine whether it is necessary to keep it in the CPMS system.

Guest users' 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 date has been reached, the guest user account is deactivated and data is kept in exactly the same way as for users' accounts.

Personal data 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.

7. 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 .

CPMS users' personal data are stored in both a database hosted at the European Commission Data Centre, with specific security protection measures (solely for EU Login and SAAS2 data), and in the CPMS (hosted in the Commission's subcontractor data centre in Germany, with implemented standards on secure processing), for all data. Only Commission authorized staff permitted to access to modify user data in the database through EU-Login and SAAS2.
All data, including personal 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 will be encrypted
- Secure transfer: HTTPS protocol will be 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 5 above are bound by confidentiality, data protection and non-disclosure agreements under specific contractual arrangements.

8. Access to your personal data

You can exercise your rights as a CPMS user (access, rectification, blocking, objection to processing and erasure) by contacting the data controller, explicitly stating your request, via the contact address below under point 10.

Please note that, as a user or guest user, you are not able to delete your CPMS profile (including all associated personal data), but only to deactivate it. Your personal data, together with any patient's pseudonymised data that you have uploaded into the system, will still be visible for purposes of patient care and diagnosis, even after you deactivate your account. If, upon deactivation, you receive a request from a patient exercising his or her data subject rights (e.g. full or partial consent withdrawal), please contact your ERN coordinator.

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.

9. Additional information

A copy of the patient consent form for sharing data in the European Reference Networks for rare diseases and information on the patient's rights can be found here: This consent form is held by the patient's treating doctor at local level and is not uploaded into the CPMS system.
A list of data protection authorities is available at the following address: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm 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.

10. Contact

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

European Commission
Directorate Health Systems, Medical Products and Innovation
B-1049 Brussels
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 any questions or comments regarding EU Login / ECAS, or if you would like to exercise your rights as a data subject, please contact the controller directly, explicitly stating your request, at the following address:

Director General Informatics DG (DG DIGIT)
European Commission B1049 Brussels

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