European Reference Networks

SHARE.CARE.CURE.

PROTECTION OF PERSONAL DATA

This privacy statement provides information about the processing and the protection of personal data by the CPMS 2.0 IT platform, desktop and mobile interfaces.

Version 1.1, 25th October 2024

Processing operation: CPMS 2.0
Data Controller: The European Commission

Contents

1. INTRODUCTION

Data privacy in the context of the European Reference Networks is under the responsibility of a joint controllership between the European Commission (hereafter the "Commission") and the healthcare providers (hereafter the "hospitals"). The allocation of responsibilities within this joint controllership is defined in annex 2 of the Commission Implementing Decision (EU) 2019/1269, of 26 July 2019, amending Implementing Decision 2014/287/EU. In this context, the Commission is fully responsible for the IT platform used by the ERNs for cross-border discussions of rare clinical cases, known as CPMS 2.0.

In all its activities, the Commission is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council, of 23 October 2018, on the protection of natural persons regarding the processing of personal data by the Union institutions, bodies, offices and agencies, and on the free movement of such data, repealing Regulation (EC) No 45/2001.

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle, and ensure protection of all personal data provided, how that information is used and which rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer, and the European Data Protection Supervisor.

The CPMS 2.0 (Clinical Patient Management System 2.0) is a web-based application with desktop and mobile interfaces used by the European Reference Networks (ERNs) to support cross-border clinical discussions related to the diagnosis and treatment of rare or complex health conditions. It is a secure platform that allows healthcare professionals to exchange patient information and medical expertise, sharing clinical data across national borders to ensure that patients receive the best possible care.

The information in relation to the processing operations via the CPMS 2.0 platform undertaken by the Commission are presented below i.e. this privacy statement explains how personal data is handled when:

a) as a user, you register in CPMS 2.0 and use the platform;
b) as a patient, your clinical case is uploaded and discussed in the CPMS 2.0.

This privacy statement does not cover the data protection aspects linked to the processing of your personal data by your hospital when you are a healthcare professional or a patient of that hospital. For that, please consult the data privacy office of your hospital.

2. WHY AND HOW DO WE PROCESS YOUR PERSONAL DATA?

2.1. Personal data collected for user management

The Commission, through CPMS 2.0, collects and uses your personal information for the purpose of enabling you, as a user, to connect to the CPMS 2.0 application and use it for sharing patient information and discussing patient cases. Your contact details (email address,

first name and last name) may also be used for contacting you. Your personal data will never be used for automated decision-making, including profiling.

2.2. Personal data collected for discussion of patient cases

The Commission, through CPMS 2.0, collects and uses personal information of patients, including health information, for the purpose of facilitating clinical discussions among healthcare professionals using the system to establish a diagnostic or recommend a treatment. No automated decision-making, including profiling, is done on the patient data.

2.3. Data collected by Healthcare Providers

Each healthcare provider using the CPMS 2.0 acts as data controller of the operations carried out under its responsibility and has the legal obligation to create and publish its own privacy statement. The Commission is not responsible for the privacy policies or practices carried out by the hospitals outside the CPMS 2.0 application.

3. ON WHAT LEGAL GROUNDS DO WE PROCESS YOUR PERSONAL DATA?

We process your personal data, because:

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body;
- the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Data subjects give their informed consent by a positive action. For the users of the CPMS 2.0 this is done the first time the user enters the platform. For the patients this is done by signing a consent form at consultation time.

Data subjects may withdraw their consent at any time:

a) for the users of the CPMS 2.0 platform, they can do it on the platform itself or by contacting the Commission, using the contacts mentioned in section 9.1.;
b) for the patients, the Hospital, using the contacts mentioned in the consent form.

4. WHICH PERSONAL DATA DO WE COLLECT AND FURTHER PROCESS?

To provide the CPMS 2.0 services, through the processing operations, the Commission collects the following categories of personal data:

4.1. User Credentials

To be identified by the system, the user needs a valid login / password, which is managed by the EU Login[1] service. For further information on how EU Login processes your personal data, please refer to the EULogin privacy statement.

4.2. User data

In the CPMS 2.0 application, for each user of the platform we collect:

- Identity information (mandatory): username, first name, last name, email address
- Other information (optional):, affiliation (ERN, hospital), open text description of user expertise.

The identity information is retrieved by an automatic process from EULogin and the European Commission's Central User Database, which is stored at the Data Centre of the European Commission. The Data Centre of the European Commission is bound to comply with Regulation (EU) N° 2018/1725 and with any Commission's security decision and provision established by the Directorate General of Security and Human Resources for this kind of servers and services (Decision 2017/46).

4.3. Transaction data

The CPMS 2.0 may collect data about your interactions within the platform, including log-in and log out details, actions taken within the platform, and other usage metrics to improve the platform.

4.4. Patient data

The CPMS 2.0 collects patient data to enable the discussion of medical cases by healthcare professionals, experts in the fields. Patient data consist of patient identifying data and patient medical data.

- **Patient identifying data**. Patient identifying data consist of first and last name, sex, date of birth, nationality. A nickname is assigned to the patient by the system and can be changed by the enrolling doctor. Only the enrolling healthcare professional has access to the patient identifying data.
- **Patient medical data**. Patient medical data consist of all kinds of medical information needed to establish a diagnosis or advise a treatment. It can contain medical images, text documents, lab results, medical history, etc. Patient medical data is always stored pseudonymized. Only the enrolling healthcare professional and the healthcare professionals that participate in the discussion of a patient case have access to the patient medical data.

[1] EU Login is the Authentication Service of the European Institutions. It is centrally managed by DG DIGIT and based on SSO (Single-Sign On) technology.

4.5. Discussion data

Discussion data consists of the log of the written opinions of the participants in the clinical discussions. Audio and video recordings of the discussion are kept in the system for a limited period after the meeting. Recordings are accessible to participants of the meeting but cannot be downloaded. The outcome report of a discussion is a document containing a summary of the discussion and/or the establishment of a diagnosis or advice for a treatment. The participants in the discussion that have a valid consent at the time of generation of the outcome report will be identified in the outcome report by their names, affiliations and profession. The outcome report can be generated and downloaded by or sent to the treating doctors who requested the discussion of the patient case. It represents the opinion of the ERN experts who participated in the discussions and is not binding - the treating doctor(s) always remain liable for the diagnosis and treatment of the patient.

4.1. Web Analytics data

CPMS 2.0 uses a dedicated web analytics engine to monitor web traffic statistics and analytics Both the infrastructure and software are under the control of the European Commission and comply with the current EU data protection legislation. CPMS 2.0 may use the Europa Analytics for web traffic statistics and analytics. Europa Analytics is the corporate service that monitors and evaluates the effectiveness and efficiency of the European Commission's websites. Europa Analytics also complies with current EU data protection legislation. Cookies policy is completely configurable by the user.

5. FOR HOW LONG DO WE KEEP YOUR PERSONAL DATA?

The CPMS 2.0 retains data for as long as is necessary to fulfil the purposes for which the data was collected. The retention period will vary depending on the specific data.

5.1. User-related data

The Commission keeps user personal data only for the time necessary. As long as a user wants to use the CPMS 2.0 the user account remains active, and the associated personal data is therefore retained. A user can, at any time, delete the user account. In this case, the user account and all associated personal data will be permanently deleted. After 5 years of inactivity, the need for keeping user data will be evaluated and the user account will be deleted if deemed necessary.

5.2. Patient-related data

The Commission keeps patient related data for the time required to the correct follow up of the patient and his/her family needs, as defined at enrolment time. Patients can, at any time and by simple request to the correspondent healthcare provider, request the deletion of their personal data. At least every 15 years, the need for keeping patient data will be evaluated by the ERN concerned and the patient data will be deleted if deemed no longer relevant.

5.3. Discussion Data

Audio and video recordings are kept for 30 days after the discussion.

6. HOW DO WE PROTECT AND SAFEGUARD PERSONAL DATA?

All personal data are stored on secure servers on European soil. There is no personal data stored in the mobile devices used to access the CPMS 2.0 using the mobile interface. All data are encrypted in transit and at rest. There are no personal tracking mechanisms (location, time, motion, usage patterns, physical activity, etc.) embedded in the mobile interface. All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

For the mobile app, the system may store some required session data on the mobile device itself, such as temporary log-in information or cached data. This data is stored securely on the device and is not accessible to the outside. This data is erased once the user logs out.

To protect your personal data, the Commission has put in place several technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed.

Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of the processing operations.

7. WHO HAS ACCESS TO PERSONAL DATA AND TO WHOM IS IT DISCLOSED?

Access to personal data is provided, by design, always according to the “need to know” principle. Commission and ERN staff responsible for carrying out this processing operations abide by statutory requirements concerning professional secrecy and awareness of good practices in data privacy and cyber security. This includes:

- Infrastructure administrators;
- EC administrators (global administration of the system).

Hospital and ERN staff responsible for carrying out this processing operations also abide by professional secrecy and awareness of good practices in data privacy and cyber security. This includes:

- Clinicians;
- ERN administrators (administration of the system at ERN level);

Hospitals are responsible for continuously improving the staff awareness on data privacy and cyber security good practices.

The information collected by the CPMS 2.0 will never be given to any third party, except to the extent and for the purpose required by law.

The Commission will never share personal data with third parties for direct marketing. The Commission will not use personal data to contact users about newsletters, marketing, or promotional information. However, the Commission may use collected email addresses to contact users about important CPMS 2.0 and ERN related announcements, in case of need. Patients will never be contacted by the Commission as no contact information is collected.

8. WHAT ARE YOUR RIGHTS AND HOW CAN YOU EXERCISE THEM?

You have specific rights as a data subject under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725. In particular, you have the right to access your personal data, and to rectify them, in case your personal data are inaccurate or incomplete. Where applicable, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing, and the right to data portability.

As a user you can exercise your rights from the CPMS 2.0 user interface. You may also contact the Commission. Please note that your first name, last name and email address are extracted from EULogin and can only be modified there. At first login, your account is automatically created using data extracted from the EULogin database. Other personal data can be modified from the CPMS 2.0 user interface.

This Privacy Statement enters into force immediately after being posted on the platform and read by the user. In case of changes to this Privacy Statement, the user will be invited again to read the new Privacy Statement before being logged in.

As a patient you can exercise your rights by contacting your hospital's data privacy office.

9. CONTACT INFORMATION

9.1. The Commission as joint Data Controller

If you would like to exercise your rights as a user of CPMS 2.0 under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the data controller at: ERN-Data-Privacy@ec.europa.eu

9.2. The hospitals as joint Data Controllers

If you would like to exercise your rights as a patient under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact your hospital, who acts as joint data controller, using the contact details mentioned in the consent form you've signed.

9.3. The Data Protection Officer (DPO) of the Commission

As a user of CPMS 2.0 or as a patient, you may contact the Commission's Data Protection Officer with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725. DPO contact: DATA-PROTECTIONOFFICER@ec.europa.eu.

The Commission DPO publishes the register of all processing operations on personal data which have been documented and notified to him. You may access the register via the link http://ec.europa.eu/dpo-register and search for "CPMS".

9.4. The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

The European Data Protection Supervisor is acting as an independent supervisory authority. The EDPS makes sure that all EU institutions and bodies respect people's right to privacy when processing their personal data.