

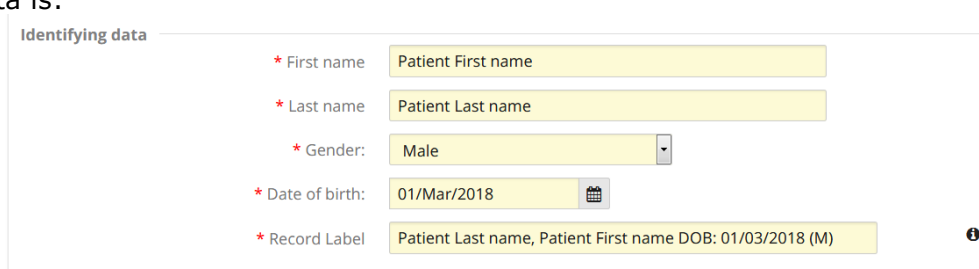
# CPMS SECURITY

## Frequently Asked Questions

### What identifying data collected in CPMS when enrolling a patient?

It was agreed during the specification phase and compilation of the common data elements, that a minimum amount of identifying patient data would be recorded at enrolment stage.

This data is:



The screenshot shows a form titled 'Identifying data' with the following fields:

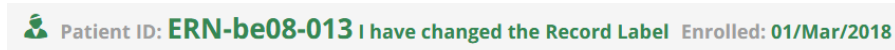
- \* First name: Patient First name
- \* Last name: Patient Last name
- \* Gender: Male (dropdown menu)
- \* Date of birth: 01/Mar/2018 (calendar icon)
- \* Record Label: Patient Last name, Patient First name DOB: 01/03/2018 (M)

The Record Label is displayed in the patient banner during the panel for the enrolling hospital only:



Patient ID: ERN-be08-013 Patient Last name, Patient First name DOB: 01/03/2018 (M) Enrolled: 01/Mar/2018

It can be manually changed:

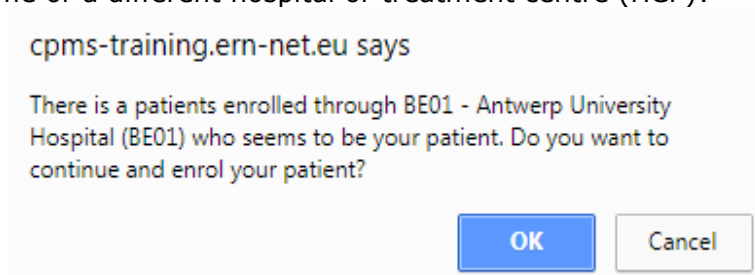


Patient ID: ERN-be08-013 I have changed the Record Label Enrolled: 01/Mar/2018

The identifying data (above) captured at enrolment stage of a patient is available only to the enrolling hospital or treatment centre, in a secure ring-fenced app, called the 'Centre' app. It is not available to other hospitals in any of the other CPMS apps.

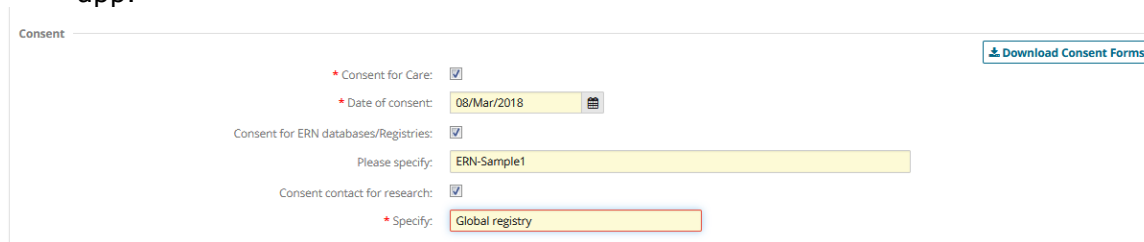
### Why is this identifying data recorded?

1. It enables an algorithm to check the encrypted identifying data\* (first name, last name, date of birth, gender) to ensure the same patient is not enrolled twice at the same or a different hospital or treatment centre (HCP):



2. It is necessary to log the completion of the informed consent to an actual person. This logging of the informed consent is captured in the enrolment window in the

app available only to the enrolling hospital or treatment centre, in the 'Centre' app.



3. To ensure the usefulness of the system over time with changes of personnel in hospitals or treatment centres a standard methodology for patient enrolment is required at system level.

## Where and how is this identifying data stored and who has access?

This data is security ring-fenced to be separated from any further sharing of this data within the other apps of CPMS. To be clear, this personal identifying data is ONLY available to from the Centre app, which is available ONLY to authenticated and authorised CPMS health professionals from the enrolling hospital or treatment centre (HCP).

In the fixed requirements to the specification for tender for the CPMS software as a service, the European Commission specified that the data must be hosted in the European Union. Due to data protection considerations from the outset, the software supplier selected a data host that is ISO27001 compliant and specialises in healthcare. It contracted with the data hosting company that the data would be hosted in Germany in two servers (one located in the south of Germany and one located in the north). This decision was taken because data hosted in Germany is subject to strict data protection regulations and is controlled by a German data trustee responsible for controlling the physical and logical access to customer data under German law.

The identifying data captured at patient enrolment is not stored in the database as is but is encrypted when stored (which makes it unintelligible, e.g. ☒🗑️✂️”). The encryption key for the encrypted data is sealed in a dated envelope and stored unopened in a European Commission safe to which there is restricted, controlled and logged access.

## Is there pseudonymisation, anonymisation or third party pseudonymisation?

The data is pseudonymised before any panel is opened, when the enrolling health professional clicks Enrol Patient.



In the ERN Databases/Registries, the query builder environment in the CPMS, pseudonymised data is made available for authorised users (using the role 'data manager/researcher') subject to the condition that the second consent has been opted-in by the patient (i.e. ERN Databases/Registries)

When the panel data is pushed to the ERNregistries/databases query builder, a unique identifier (Research ID) is assigned, other than the identifier that was used during the consultation phase of the panel. The data stored in the ERNregistries/databases query builder can be queried by an authorised user by combining particular fields, e.g. without the identifier or aggregated, in which way the data would be classed as anonymized. If

the authorised user does include the unique identifier in the query (i.e. Research ID), the data output from the query would be classed as pseudonymised rather than anonymised.

The ERN IT Advisory Group approved a recommendation in 2018 to implement Third Party Pseudonymisation (in addition to the existing pseudonymisation) with a view to potential future use cases for research. Third party pseudonymisation would align CPMS with the work being carried out at a technical level by the Joint Research Centre on the platform on rare disease registries (to provide a directory of registries). Third Party Pseudonymisation had been envisaged from the outset although not required for the first release and it is one of the reasons identifying data, albeit a minimum amount, is collected as it is required to pseudonymise the patient.

## **What security testing was carried out and were any issues identified solved and retested?**

On 10/11/2017, a status report was sent to all ERN Coordinators with details of the tests carried out on the system. Included in the set of tests carried out were full security and vulnerability tests. These were carried out independently once by an external company and twice by the IT Security Team in the European Commission, DG Health and Food Safety. The security and vulnerability tests were carried out to gauge the security posture of CPMS. The targets and scope were defined in advance and the tests were carried out and concluded following best practice methodologies and were performed with Burp suite, semi-manual and manual. The testing phase included reconnaissance of the application, preparation and execution of automated vulnerability tests, additional manual tests and documenting observed anomalies all of which were followed up and subsequently retested. Unfortunately, it is not secure for us to allow the 900+ hospitals/treatment centres associated with the ERN project to run their own security and vulnerability tests.

The CPMS and the model informed consent form were the subject of a prior check by the European Data Protection Supervisor (EDPS). The EDPS technical recommendations were implemented and retested prior to launch of the clinical patient management system.

## **Are uploaded images de-identified?**

The upload of PACs images (CT scans, MRIs, PET scans, Tomography, Ecographs, RXs, Dicomized Static Images and Endoscopies) is using a tool that automatically anonymises the images (see documentation in CPMS on the image viewer and on de-identification). If health professionals upload jpegs, pdfs, PowerPoint slides, etc., it is not possible to automatically de-identify these if they contain personal data. There is a checkbox for health professionals to tick reminding them of their obligations.

If it is not allowed to upload files or images because of local, regional or national data protection rules, these can instead be shared on the health professional's screen during a video consultation using the integrated video tool.

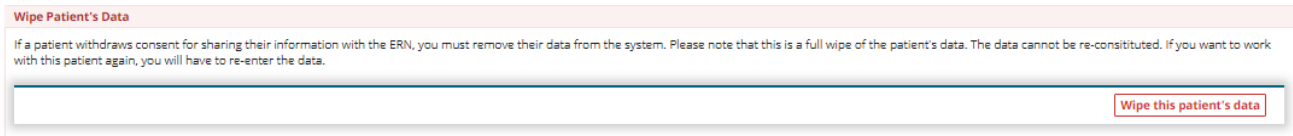
Transfer of data is also possible using FTP or IHE (supporting four profiles).

## How to wipe patient data?

Only the enrolling healthcare professional enrolling the patient or a healthcare professional from the same treatment centre can wipe patient data.

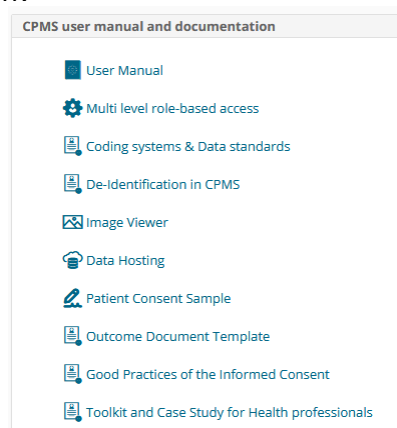
From your Centre Dashboard, go to Patient List, select the Patient whose data you want to Wipe then Click on Enrolment on the left. Scroll to the bottom and find the button

'Wipe this patients data'.

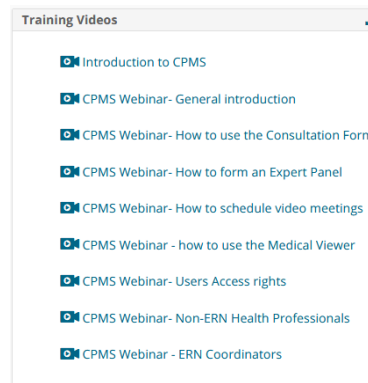


## Where can I find more information?

Please refer to the documentation available from the CPMS landing page, which includes comprehensive documentation:



and a series of Training Videos:



and, from the Help menu, there is a link to a FAQ as well as a page containing Security Documentation:

