

De-Identification Mechanisms in CPMS for European Reference Networks

Document type: De-Identification Techniques in CPMS

File name: De-Identification Methodology

Document reference: 22022019DE-CPMS

Produced by: OpenApp

Version: 3.0

Release date: 22.02.2019

Abbreviations

ERN: European Reference Network

CPMS: Clinical Patient Management System for ERNs

DOB: Date of Birth

HP: Health Professional

GUID: Global Unique Identifier

ID: Identifier

DICOM: Digital Imaging and Communications in Medicine

NMRN: National Medical Reference Number

CDA: Clinical Document Architecture

C-CDA: Consolidated Clinical Document Architecture

1 De-Identification approaches

De-identification, anonymization, and pseudonymization are approaches to remove information from data that are not strictly required for the intended purpose of those data.

- Anonymization is a method to disassociate all identifiers from the data, where pseudonymization supports longitudinal linking and authorized re-identification
- Pseudonymization¹ 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

2 Pseudonymization in CPMS

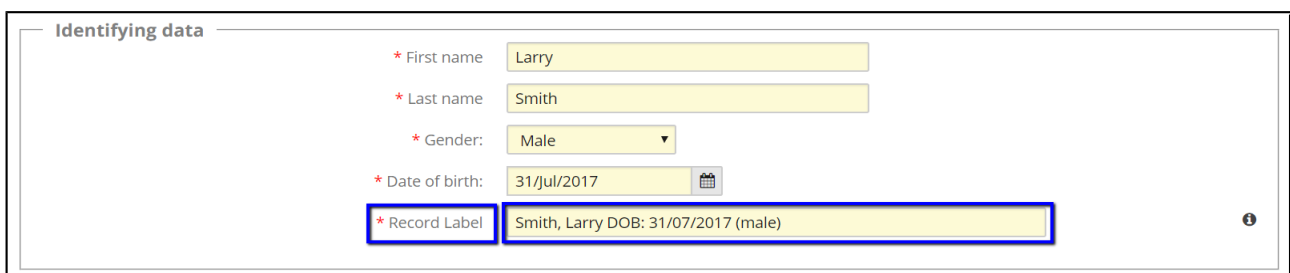
CPMS ID

When enrolling a patient into the CPMS, the system generates automatically a unique ID for each patient known as **CPMS ID**. This ID is only visible for health professionals within a particular centre/hospital.

Patient Id: ERN-cy02-001

Record Label

Within a particular centre, the CPMS proposes by default a structured **Record Label** for each patient to complete the enrolment. This record label is composed of the patient identifying data entered in the enrolment form (e.g. first, last name, etc.). Only authorised medical professionals can see and edit the record label if they wish. Similarly to the CPMS ID, the record label is only visible to authorised users in a particular centre/hospital.



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

- * First name: Larry
- * Last name: Smith
- * Gender: Male (dropdown menu)
- * Date of birth: 31/Jul/2017 (calendar icon)
- * Record Label: Smith, Larry DOB: 31/07/2017 (male)

The "Record Label" field is highlighted with a blue border and a blue box around its label.

From the **Security tools** in the CPMS, the system administrator can configure the relevant identifying data in the enrolment form. Thereafter, the CPMS proposes automatically a label for the

¹ Article 4, point (2) of Regulation EU/2016/679

patient record that contains the patient identifiers and can be edited by authorized users as mentioned above.

Patient Identity Fields

- Collect patient name
- Collect patient name at birth (for GUID)
- Collect date of birth for clinical use
- Collect gender
- Collect patient label
- Collect exact date of birth (for GUID)
- Collect patient CITY of birth (for GUID)
- Collect patient COUNTRY of birth (for GUID)
- Collect patient National Identity Code (for GUID)

Panel ID

When initiating a panel in an ERN, OpenApp emphasise that none of the invited experts from different centres/hospitals from same/different ERN, can see any patient identifiers (i.e. CPMS ID, Record Label, enrolment data). That means all Panel members from outside the centre to which the patient belong, can not see the real patient identity when participating in a Panel or a Meeting.

Panels are identified uniquely by a **unique Panel ID number**, shown always in the Panel Header.

232 Julian

Open Panel Selection Data Completion Assessment Outcome Sign-off Closed Archived

Next »

Centre	AT01 - EB-Haus Austria	ERN	ERN Skin - Skin Disorders
Lead	Hany Mina	Thematic Area	Cutaneous diseases related to DNA Repair Disorders
Panel	Mr. Emma Jackson (Radiologist), Doctor One		

Schedule Meeting

Nickname

The CPMS allows users to give **Nicknames** to their patients per each individual consultation request. Clinicians will be always requested not to reveal any real patient identifiers. When a user initiate a panel, he/she will be requested to fill in the consultation request as the minimum amount of data required to invite other health professionals to consult the submitted request.

In the consultation request section, users will need to provide a “Nickname” for every individual consultation request for the same patient.

In line with the data protection regulation, CPMS prevents users to save the Consultation request when recording any *Nickname* that contains any part of the patient’s First or Last name.

ERN Databases/Registries ID

In the ERN Database/Registry application known as low accessibility database wherein all data are made available provided that the patient has given a specific consent (i.e. second consent in the enrolment form) to share their data with ERN Databases/Registries. A *new patient ID* is given to the Panel and the nickname is removed; this database contains only anonymised clinical data collected as part of the panel, small amount of panel admin data, decision column as the outcome of the consultation interaction. Data in the ERN database can be exported by authorized researchers/data managers in several formats with no identifiable data.

3 Pseudonymisation of Hospital Relationship

The CPMS always allocates a unique identifier to a patient in the context of a dataset (study). The standard approach is that the hospital copies the patient id to a standard location (patient record), and the patient id is then used to link the data. When a patient presents in the hospital, the hospital patient record is retrieved, and from the data in the patient record, the CPMS record can be retrieved.

The CPMS data model allows multiple identifiers to be linked to the same patient. Each identifier has a “domain” i.e. the owner and identifier type. This mechanism has been used in bespoke deployments to link a hashed version of the hospital’s National Medical Reference Number (NMRN) to a patient. The hashed version of the NMRN allows a user with an NMRN to retrieve the patient data, but cannot be used to find the hospital record using the hash.

4 Linking Exported Data

Where a dataset is exported from CPMS and a separate independent consultation, there is difficulty linking the data. It is necessary for both datasets to go to their identifying data and to link the data based on common identifying data. CPMS collects and stores the patient identifying data in encrypted database.

The normal process is that an independent party is given the identifying data from both datasets. The independent party hashes both sets of identifying data in a common way and returns the data plus hashes to the parties with the data. Both datasets are regenerated including the hash for that row and can be joined by the authorised person.

5 DICOM De-identifications

The CPMS is supported by DICOM viewer to enable health professional browse imaging in files as single instance or full study. The next few pages summarise what de-identification methodologies are used to remove the study tags from an image or a study.

Anonymizing the images comes effectively with erasing most of the tags as specified in Table E.1-1 from PS 3.15 of the DICOM standard 2008 in addition to the following tags:

- Patient’s Address
- Requesting Physician
- Patient Telephone Number
- Medical Alerts

For more information on the DICOM Table E.1-1, please visit this link:

http://dicom.nema.org/dicom/2013/output/chtml/part15/chapter_E.html#sect_E.1.1

However, it is notable to say the CPMS keeps certain non-identifying data on the study/image to help health professionals recognize the examined fields/areas such as study description and its UID. The Viewer will replace the patient name on the image with UID given to patients previously as well as rename the study.

Other than DICOM images, any uploaded non-imaging files might be found within the study containing identifying data (e.g. PDF files) fall within the responsibility of the user.

6 CDA Document

CDA (Clinical Document Architecture), and C-CDA (Consolidated Clinical Document Architecture) include a header that contains identifying patient data, so a **Redaction mechanism** is used when the CPMS retrieves those documents from hospitals. Users must review the documents to reduce the risk that any identifying data are included and not useful in medical context.

7 Files Uploads

The CPMS allows authorized users to upload images and other files in specific formats into into the consultation form. Notification and warning messages can be seen to remind users to verify the uploaded materials do not contain any identifying data. Another mechanism, **Tick Box** is shown in the attachment section to be ticked confirming the user has acknowledged to upload only documents with no identifying patient data.