

# Presentation of ERN CPMS 2.0 DPIA Results

Minutes

05 November 2024, 15:00 - 17:00

Chair: João de Sousa, DG SANTE

## Agenda

1. Introduction and context
2. DPIA presentation
3. Discussion
4. How recommendations are being addressed
5. Next steps for hospitals
6. Discussion
7. Closing remarks

## 1. Introduction and Context (by Commission)

The results of the recent Data Protection Impact Assessment (DPIA) for the CPMS 2.0 were presented and the necessity of a DPIA for a new patient consent form in the context of CPMS 2.0 reviewed. The CPMS 2.0 is an IT platform, designed to support secure, cross-border medical discussions. It has been used for 7 years, initially going live in 2017. It facilitates the sharing of patient cases, including imaging and multimedia, to improve care for rare and complex conditions. Following feedback from healthcare professionals and advancements in technology, CPMS 2.0 was developed in 2022, with a DPIA completed in July 2024. This new platform will replace the original CPMS, which is scheduled to be decommissioned in January 2025. CPMS 2.0 has been evaluated as GDPR-compliant, adhering to EU data protection regulations.

The legal framework for CPMS 2.0 is supported by Article 12 of the Cross-border Healthcare Directive, with joint data controllership held by the EU and HCPs.

## 2. DPIA Presentation (by NRB)

The CPMS 2.0 processes user identification, contact details, and medical data to allow authorised users to access the CPMS 2.0 and to enable collaboration among healthcare providers.

The DPIA followed guidelines from the EU Data Protection Supervisor (EDPS) and ENISA Handbook on Security of Personal Data Processing. A questionnaire was elaborated for security measures required

in high-risks systems, such as CPMS 2.0 because it is accessible from the Internet, is hosted in a cloud environment and processes highly sensitive data.

An assessment confirmed the DPIA requirement as CPMS 2.0 processing met 2 of the EDPS's 9 risk criteria. The following key principles were evaluated:

- Lawfulness: legal basis for the processing of personal data
  - Performance of a task carried out in the public interest or in the exercise of an official authority vested in the Union institution or body
  - Data subject consent
- Necessity and proportionality
  - The processing operation through the CPMS 2.0 is an effective means for the EC to fulfil its task to facilitate the establishment and operation of the ERNs as provided for in Article 12 of Directive 2011/24/EU.
  - Using the CPMS 2.0 platform is the most effective and least intrusive option
  - The processing is proportionate for the fulfilment of the task
  - The nature of the interference caused by the processing is proportionate to its purpose
- Transparency and fairness
  - Information on data processing, as well as on Data Subject's rights and how to exercise them, is effectively communicated to Data Subjects.
  - Information provided is complete and easy to understand
  - Information is targeted to the audience
  - Information is communicated before the data is processed by the CPMS 2.0
  - Data subjects are informed and aware of the processing of their data by the CPMS 2.0
  - As processing is based on the consent of the Data Subject, the freedom of consent is ensured, as is the possibility of revoking it at any time. Regulas of consent is no way implies discrimination.
- Purpose limitation and storage limitation
  - All purposes of the process are identified: data is not reused for other purposes other than access by authorised users to the CPMS 2.0 and facilitation of patient's diagnosis and treatment.
  - The retention period is defined by distinguishing the storage period of the different parts of the data.
  - Personal data is regularly reviewed and kept for no longer than is necessary
- Data minimisation and accuracy
  - The personal data collected and processed is adequate, relevant, and limited to what is necessary for the purpose identified
  - Patient data is pseudonymised. A unique ID is automatically created by CPMS 2.0, when a new patient is enrolled in the system
  - Regarding CPMS 2.0 user data collecting, a distinction is made between mandatory and optional elements.

- The accuracy of the personal data as well as the one obtained from third parties is ensured
- The CPMS 2.0 allows updating/correcting data when necessary

A specific agreement allows data transfer to Ukraine, enabling Ukrainian patients' case data to be shared with designated users. Outcome report of a UA patient case discussion is accessible to download by UA guests or UA enrolling guests that participated in the discussion via the platform, including names and affiliations of all participants in the discussion. One of the recommendations is to carry out a Transfer Impact Assessment to assess the level of data protection of UA legislation and identify potential risks of rights and freedom of Data Subjects.

The risk assessment analysed 16 potential risks, 10 related to data security and 6 concerning compliance with GDPR and EUDPR principles, with the highest residual risk rated at level 4. Mitigations include a layered and security approach across governance, development, infrastructure, and operations.

Recommendations from the DPIA propose several enhancements within 6 months of CPMS 2.0 deployment. The overall recommendations include:

- Coordination with the joint controllers so to develop an acceptable use policy and or user's agreements which must be followed by CMPS 2.0 users when using the system.
- It is mandatory that DPIA is also addressed by the joint controllers. DPIA risk threshold assessment and in case of 2 or more applicable criteria that joint controllers should execute a DPIA regarding their areas of responsibilities
- Establishment of a user access management process
- Holistic and full-scale penetration test execution by an independent party which would complement already executed test at application level
- For the EC, Disaster Recovery Plan development based on the results of Business Impact Analysis and Risk assessment
- Planning of annual Business Continuity and Disaster Recovery test execution
- Transfer Impact Assessment execution regarding the cases of user's identification information transfer to UA.

Recommendations for the Privacy Statement Update:

- The user data will be immediately deleted, except of user's activities such as healthcare professional's participation in discussions, if the user delete his/her data account through the CPMS 2.0 web interface. The Privacy Statement should also determine the legal basis for this storage, in accordance with Article 5 of the EUDPR, based on EDPB Guidelines 05/2020 on consent under Regulation 2016/679, points 117 and 118.
  - The user data will not be immediately deleted if the user withdraw his/her consent through the CPMS 2.0. In this context, the Privacy Statement should also determine the legal basis for this storage.
  - The user identification information could be transferred to UA if a UA HCP will invite the user so to assess a UA patient's rare disease through the CPMS 2.0
  - The users should be informed about the potential risks to their rights and freedoms in case of identification information transfer to a third country (UA) based on the results of TIA execution.
- The usage of web cookies (if confirmed) including details about the information being recorded and processed.

### 3. Discussion

University Medical Centre Ljubljana asked about the preparation of the Transfer Impact Assessment (TIA), specifically inquiring who would be responsible for this document and whether there were any templates or recommendations available. The EC responded that there is a specific guidance regarding the TIA. TIA should be prepared by the party initiating the data transfer.

Endo-ERN sought clarification on document storage within CPMS 2.0, asking whether documents would be stored on the system itself or if there would be a specific location from which they would need to be requested. The EC confirmed that all general documentation will be accessible on the platform and advised contacting support if any particular document was missing.

Mater Dei Hospital raised concerns about using patient consent as a legal basis for processing personal data, noting the power imbalance between hospitals and patients and questioning whether controllers could meet GDPR standards for explicit consent, such as the right to withdraw. The EC reiterated the legal base used: the Cross-border Healthcare Directive, which provides the primary legal basis for platform operation. The processing of user data is required either for tasks in the public interest or by legal mandate. Due to these legal grounds, patients' data rights are limited to a certain extent. Following discussions with the HCPs, it was determined that a specific consent form from patients was necessary. Regarding the power imbalance, the HCP should declare in the consent form text that the healthcare provided will not be affected if the patient refuses to go through CPMS 2.0. Mater Dei noted that patient rights are somewhat limited, and that HCPs should only use CPMS 2.0 if patients have consented.

Mater Dei Hospital further inquired about managing patient requests to withdraw consent if their information had already been entered into CPMS. The EC clarified that any data processing conducted before the withdrawal of the consent is legal. If HCPs are legally required to retain certain data, this obligation still applies, and patients should be informed of this limitation. The EC noted that in most countries, HCPs are required by national laws to document any medical advice given to patients. It was also clarified that relying on consent as a legal basis is consulted with the EU Data Protection Supervisor.

Rigshospitalet questioned the timeline for the TIA concerning Ukraine. The EC reiterated that the TIA should be carried out by the transferring party, particularly for healthcare professionals' authentication data, and stated that the EC could not offer support in assessing Ukraine's legal environment.

ERN-RND asked when supporting documentation, such as DPIA results and certificates, would be available on CPMS 2.0. The EC responded that some documents were already available, and the recently presented DPIA results would also be uploaded.

Endo-ERN inquired about the process for removing a patient or user from the system. The EC explained that users can delete their accounts to be "forgotten," with records of only their participation in meetings retained but anonymised. If users just withdraw consent, without account deletion, their information is frozen and they are unable to log in until consent is restored.

Mater asked whether the CPMS DPIA template could be adapted for other ERN activities, such as registries. The EC explained that, as CPMS is a clinical care platform, patient consent is primarily for care purposes, with optional consents for the purpose of HCP education/training or exporting patient

data for ERN registries if fully anonymised. The EC also noted that due to differences in IT infrastructure, the DPIA for CPMS would likely be unsuitable for other systems. It can nevertheless be a good source of inspiration for other texts.

Uzleuven asked if hospitals could operate without a consent form and instead use an opt-out system. The EC clarified that consent forms are obligatory for the use of CPMS 2.0.

Mater Dei asked if patients could access discussions related to their care. The EC confirmed that patients could access relevant information, by asking their treating doctors, subject to national law, but reminded that CPMS is intended for clinician discussions and does not support patient accounts.

Endo-ERN sought clarification on whether a formal consent form was necessary or if obtained consent would suffice under national legislation. In response, it was clarified that the form is a recommended template, however, HCPs should review it against national legislation and use a different form if required.

Mater Dei asked if written consent was required, or if verbal consent would be adequate. The EC responded that there must be evidence of received consent, such as testimonial or video/audio recording if consent is verbal. The provided consent form template allows for adaptations to support verbal consent, and HCPs can further develop it in line with guidance from national supervisory authorities.

OPBG inquired whether the latest opinion from the EU Data Protection Board from 22 October 2024 on obligations for processors and subprocessors had been evaluated within the DPIA, especially regarding joint controller responsibilities over data processors. Their concern was whether joint controllers would also bear responsibility for processors and subprocessors. Their second question addressed consent for paediatric hospitals, noting that the provided standard consent form is directed at adults and may require adaptation for legal representatives in a paediatric context.

The EC responded that the example consent form is flexible; HCPs may modify it to better suit specific needs, such as those of paediatric hospitals, while still meeting minimum requirements and consulting national authorities. On the first question, the EC directed OPBG to Annex 3 of the Implementing Decision, which describes responsibilities and boundaries between the joint controllers, namely HCPs and the EC.

ULSSM inquired about the availability of translated consent forms for all EU countries, noting that it had been previously mentioned. The EC responded that a patient consent kit had been prepared, including the original English template and unofficial translations in all EU languages. These will be accessible on the CPMS 2.0 landing page. The EC advised that HCPs should follow their national authority's guidelines when drafting consent forms and check if a centralised approach had been decided by their national healthcare authority. They emphasised that, despite any national guidance, the joint controller remains the HCP, not the ministry, placing responsibility on the hospital.

## 4. How recommendations are being addressed (By Commission)

The DPIA for CPMS 2.0 provided several recommendations for improvement, primarily concerning coordination with HCPs.

- These include developing an acceptable use policy and ensuring HCPs conduct their own DPIAs while raising security awareness among users.  
**Status:** The EC has expressed willingness to facilitate best practice discussions with HCPs and will survey interest in these sessions.
- Another recommendation was to establish a user access management process aligned with EC standards.  
**Status:** This has been integrated into the platform, with documentation still in progress.
- Further recommendations included conducting full-scale penetration tests by an independent entity.  
**Status:** These tests are now part of the acceptance workflow for each major release.
- Additionally, developing a Disaster Recovery Plan and executing an annual Business Continuity Plan were advised.  
**Status:** Both are now covered under annual contracts.

## 5. Next steps for hospitals (By Commission)

Transition to CPMS 2.0 involves several key steps:

Each HCP must determine which patient consent form (PCF) to use, with the preferred option being the EC-provided CPMS 2.0 PCF template. HCPs may continue using their current PCF or adopt a different form if needed. The second step in the preparation of the transition to CPMS 2.0 is for the HCPs to conduct a DPIA for processing activities under their responsibility **if necessary**.

Regarding the comparison of current vs. new consent text, the initial consent is essential for enrolling patients, and this part of the text is mostly unchanged. However, the second and third consents (both optional) have been updated. If using the old form, HCPs should exclude the two optional consents and retain only the primary consent.

The preferred approach is to use the new consent form in CPMS 2.0. The EC recommends using the CPMS 2.0 template kit, customised to each hospital's needs and compliant with national legal requirements. This kit is available at the [entry page](#) of the platform, under [supporting documents](#).

Using a different patient consent form is a decision of the HCP, who is accountable to the national supervisory authority.

With respect to the DPIA for HCP activities, if HCPs have already completed a DPIA for the current CPMS, they may only need to update it if their activities have changed. If no prior DPIA has been done, HCPs should assess the need for one, consulting national supervisory guidelines if necessary.

## 6. Discussion

EuroBloodNet asked if the CPMS pseudonymisation tool is related to SPIDER, ERDRI's pseudonymisation tool. The EC clarified that CPMS generates an internal pseudonym for patient discussions, which can be modified by doctors. This pseudonym is independent of SPIDER, as it only ensures that no personal information is used within discussions. However, CPMS is designed to potentially export data to registries in the future, a feature that would use the SPIDER mechanism to ensure compatibility with the work done by the JRC. The EC noted that the SPIDER mechanism would be applied solely for future data export and is not involved in other pseudonymisation activities within CPMS.

SJD raised concerns about how long patient data will be stored within CPMS and the process for its deletion. The EC responded that, under the legal framework, CPMS can store patient data for as long as necessary for accurate diagnosis. Data retention will vary per case, but the system includes a mandatory review every 15 years to determine if data retention is still necessary. This review is automatically triggered by the system.

Helse Bergen questioned the handling of identifiable images (e.g., facial images) when necessary for collaboration and whether the Informed Consent Form (ICF) should be updated to reflect this. The EC clarified that identifiable images may be shared if essential for the discussion, but only on a "need-to-know" basis, restricted to doctors directly involved in providing an opinion. HCPs are free to adapt the consent form text if deemed necessary.

SVHG asked whether national obligations might require retention of records if a patient withdraws consent or requests profile deletion, referencing guidelines like those from the Irish Medical Council. The EC explained that the obligation lies with the joint controller (the HCP) according to their internal procedures and national legislation. While certain records may be beneficial to retain, if there is no legal basis, they should not be kept after a deletion request.

## 7. Closing remarks (By Commission)

The EC emphasised the tangible actions being taken to enhance patient care, extending thanks to Member States, healthcare providers, and external contractors. The next phase marks the implementation of the preparations discussed in the meetings.