

THE **NRB** GROUP


TRASYS
INTERNATIONAL

AIRBUS
PROTECT



DG SANTE: ERN CPMS2.0 DPIA
Framework Contract AIRBUS – SR3422
November 5th 2024



1. Introduction
2. DPIA Requirement
3. Compliance Checklist – EUDPR/GDPR Principles
4. International Data Transfer
5. Risk Assessment
6. Implemented Security Measures
7. Recommendations
8. Q&A



Clinical Patient Management System 2.0 (hereafter CPMS 2.0)

CPMS 2.0 is an IT system provided by European Commission to support **remote collaboration** between healthcare professionals affiliated to ERNs members in the diagnosis and treatment of patients with **rare or low prevalence complex diseases or conditions**, across national borders.

- CPMS 2.0 processes:
 - **Identification** and **contact details** of CPMS 2.0 user's (Healthcare Professional and Non-healthcare professional)
 - To allow authorised users to access the CPMS 2.0
 - **Identification** and **medical data** of patients suffering from rare or low prevalence complex diseases enrolled into CPMS 2.0
 - To facilitate patient's diagnosis and treatment

Introduction - Methodology used



- European Data Protection Supervisor guidelines
 - Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments
 - Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation
 - Security Measures for Personal Data Processing Article 22 of Regulation 45/2001
 - Flowcharts and Checklists on Data Protection
 - European Commission Data Protection Guide
- ENISA Handbook on Security of Personal Data Processing
 - A questionnaire was elaborated for security measures required in high-risk systems such as CPMS 2.0 because it is accessible from the Internet, is hosted in a cloud environment and proceeds highly sensitive personal data





1. Introduction

2. DPIA Requirement

3. Compliance Checklist – EUDPR/GDPR Principles

4. International Data Transfer

5. Risk Assessment

6. Implemented Security Measures

7. Recommendations

8. Q&A



EDPS risk threshold assessment

- CPMS 2.0 processing operation corresponds to **two of the nine criteria** established by EDPS:
 - ***Sensitive data***: CPMS 2.0 processes patient medical data consisting 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.
 - ***Data concerning vulnerable data subjects***: CPMS 2.0 processes data concerning vulnerable data subjects, such as physically and/or mentally weak, including minors.

➤ *Processing operation corresponds to more than one criterion.*

➤ *Processing is likely to result in a high risk to the rights and freedoms of natural persons.*

DPIA is required



1. Introduction
2. DPIA Requirement
3. Compliance Checklist – EUDPR/GDPR Principles
4. International Data Transfer
5. Risk Assessment
6. Implemented Security Measures
7. Recommendations
8. Q&A

Compliance Checklist – EUDPR/GDPR Principles (1/5)



Lawfulness

- **Legal basis** for the processing of personal data (Article 5 of the EUDPR):
 - Performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body:
 - ✓ Article 12 of the Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.
 - Data subject consent:
 - ✓ CPMS 2.0 users and patients are informed about processing of their data within CPMS 2.0, by a Privacy Statement available within CPMS 2.0 and consent forms used by the healthcare providers.
 - ✓ And their consent is obtained by :
 - consent box in the CPMS 2.0 to collect CPMS 2.0 users' consent.
 - consent form (template available in each EU language) used by the healthcare providers to collect EU patients' consent to be enrolled into the CPMS 2.0.
 - special consent form (available in Ukrainian and English) used by healthcare providers from Ukraine, to collect UA patients' consent to be enrolled into the CPMS 2.0.

Compliance Checklist – EUDPR/GDPR Principles (2/5)



Necessity

- The processing operation through the CPMS 2.0 is an **effective means** for Commission to **fulfil its task to facilitate the establishment and operation of the European Reference Networks (ERNs)** as provided for in Article 12, § 4, point c) of Directive 2011/24/EU.
 - Other alternatives were also considered, as telephone or video call, as well as other solutions.
 - Other commercial products (MS Teams, Zoom, Google meet) or opensource solutions (Jitsi, big blue button) for remote collaboration were also considered.
- ✓ *Using the CPMS 2.0 platform is the most effective and least intrusive option.*

Proportionality

- The processing is proportionate for the fulfilment of the task:
 - CPMS 2.0 implement the least possible workflow and support the minimum features.
- The nature of the interference caused by the processing is proportionate to its purpose:
 - Each related interference is considered mitigated and is proportionate to the CPMS 2.0 purpose to ensure remote collaboration between healthcare professionals across national borders and to help the rare disease patients.
- The various interests involved were weighed up:
 - The superior interests of the patient are the driving force of the CPMS 2.0 platform.

Compliance Checklist – EUDPR/GDPR Principles (3/5)



Transparency

- Information on data processing, as well as on the Data Subject's rights and how to exercise them, is effectively communicated to Data Subjects, by:
 - CPMS 2.0 Privacy Statement available within CPMS 2.0.
 - consent form used by the healthcare providers to collect EU patients' consent.
 - special consent form to be used by healthcare providers from Ukraine, to collect UA patients' consent.
- 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.

Fairness

- 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. Refusal of consent in no way implies discrimination.
- Is it easy for people to exercise their rights to access, rectification, erasure etc.:
 - CPMS 2.0 Users can contact the EC (at ERN-DataPrivacy@ec.europa.eu) or access to and/ or rectify their data, and/ or withdraw their consent directly by logging on to the CPMS 2.0.
 - Patients can contact the correspondent healthcare provider using the contacts mentioned in the correspondent consent form.



Purpose limitation

- All purposes of the process are identified:
 - CPMS 2.0 user's personal data are processed to allow authorised users to access the CPMS 2.0.
 - Patient's data are processed only for the purpose of facilitating patient's diagnosis and treatment.
- *Data is not re-use for other purposes.*

Storage limitation

- The retention period is defined by distinguishing the storage period of the different parts of the data:
 - **User identification, discussion and transaction data** - As long as CPMS 2.0 user account remains active. After 5 years of inactivity, the need for keeping user data is evaluated and the user account is deleted if deemed necessary.
 - **Patient data** - For the time required to the correct follow up of the patient and his/her family needs, as defined at enrolment time. 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.
- *Personal data is regularly reviewed and kept for no longer than is necessary (for the purposes for which it was collected).*

Compliance Checklist – EUDPR/GDPR Principles (5/5)



Data minimisation

- The personal data collected and processed is adequate, relevant and limited to what is necessary for the purposes identified:
 - CPMS 2.0 users' identification and contact details: to allow authorised users to access the CPMS 2.0.
 - Patients' identification and medical data : to facilitate patient's diagnosis and treatment.
- 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.

Accuracy

- The accuracy of the personal data collected is ensured:
 - CPMS 2.0 users who enters their own or patient's data on the platform must ensure that this data is accurate and updated, where necessary.
 - The CPMS 2.0 enables inaccurate personal data concerning users or patients to be deleted or rectified without delay.
 - The accuracy of the personal data obtained from third parties is ensured:
 - EU login user data, the only data obtained from third parties, is retrieved using well defined APIs.
- *The CPMS 2.0 allows updating / correcting data where necessary.*



1. Introduction
2. DPIA Requirement
3. Compliance Checklist – EUDPR/GDPR Principles
4. International Data Transfer
5. Risk Assessment
6. Implemented Security Measures
7. Recommendations
8. Q&A



Transfer to third country – Ukraine (UA)

- Administrative agreement signed with Ukraine:
 - Ukraine patients may be uploaded in the CPMS 2.0 system.
 - Outcome report of a Ukrainian patient case discussion is accessible to download by UA guests or UA enrolling guests that participated in the discussion via the platform.
 - This report includes the names and affiliations of all the participants in the discussion.
 - Legal base for the transfer - Data subject consent (Article 51(a) of the EUDPR):
 - The data subject explicitly consents to the transfer by ticking the consent box provided for this purpose in the CPMS 2.0, which inform of the possible risks of such transfers for the data subject due to the absence of an adequacy decision with regards to Ukraine and the absence of appropriate safeguards on the part of Ukraine.
- *The execution of a Transfer Impact Assessment is recommended.*



1. Introduction
2. DPIA Requirement
3. Compliance Checklist – EUDPR/GDPR Principles
4. International Data Transfer
5. Risk Assessment
6. Implemented Security Measures
7. Recommendations
8. Q&A



- 16 risks have been analysed based on EC relevant guidance and template in a scale of 1-16.
 - 10 risks related to the security protection of personal data.
 - 6 risks related to non-compliance with EUDPR/GDPR principles and requirements.
 - The highest residual risk level is 4.

Security Protection Risks

Insufficient security protection resulting in health information disclosure

Insufficient security protection resulting in health information manipulation

Insufficient security protection resulting in systems unavailability and/or health information loss

Incapability to sufficiently and timely manage security breaches

Insufficient protection provided by the security measures

Insufficient security governance

Personal data are merged or included in systems outside CPMS 2.0

IT administration systems being used by external malicious actors

Insecure systems and / or practices are being used by the users

Users' activities tracking

Non-Compliance Risks

Unfair processing of personal data

Unavailability of transparent information on data processing

Personal data processing by external systems and / or non-CPMS 2.0 purposes

Unnecessary personal data processing

Processing of inaccurate personal data

Extended storage of personal data



1. Introduction
2. DPIA Requirement
3. Compliance Checklist – EUDPR/GDPR Principles
4. International Data Transfer
5. Risk Assessment
6. Implemented Security Measures
7. Recommendations
8. Q&A

Implemented Security Measures



- A layered and security in depth approach has been implemented for the security of CPMS 2.0 personal data and processing activities at organisational, procedural and technical level.

Governance

IT Security Risk Assessment & Security Plan

Roles: System Security Officer, Business Continuity Officer, Data Protection Officer, Data Protection Coordinator

Security requirements have been defined in contractual obligations

DPIA execution and implementation plan for recommendations

Development

Security integration in SDLC based on EC standards and international best practices

By design only the enrolment HCP has access to the patient's real name

By design only the invited HCPs have access to the patient's healthcare information

Patients' personal data are pseudorandomised and encrypted during their storage and transmission

Fake patient data are being used in the development, testing, training and acceptance environments

Infrastructure

The hosting environment is certified by ISO 27001, HIPAA and ITECH and the Cloud Broker by ISO 27001

The production environment is isolated and segregated from the other environments of CPMS 2.0 components, CPMS 2.0 backend/frontend and cloud ecosystem

The IT administrators neither have access to CPMS 2.0 production environment nor to personal data

The cloud broker is monitoring the security related events

Operations

Variety of distinct user and administration roles and access approval by ERNs

Strong password and two factor authentication for both users and IT Administrators

The development and maintenance contractor is monitoring the application security logs

3 specialised cloud security tools to continuously assess and monitor the security

A high availability architecture has been implemented by the usage of redundant systems and different availability zones



1. Introduction
2. DPIA Requirement
3. Compliance Checklist – EUDPR/GDPR Principles
4. International Data Transfer
5. Risk Assessment
6. Implemented Security Measures
7. Recommendations
8. Q&A

Recommendations (1/2)



- The DPIA report proposes the following improvements which should be implemented within 6 months after CPMS 2.0 induction in production, so to enhance the governance and management of CPMS 2.0 security and personal data protection.

Overall Recommendations

Coordination with the joint controllers so to develop an acceptable use policy and/or users' agreement which must be followed by CPMS 2.0 users when using the system.

DPIA risk threshold assessment and in case of 2 or more applicable criteria the 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 the already executed test at application level.

Disaster Recovery Plan (DRP) development based on the results of Business Impact Analysis and Risk assessment.

Planning of annual Business Continuity and Disaster Recovery tests execution.

Transfer Impact Assessment (TIA) execution regarding the cases of users' identification information transfer to Ukraine.

Recommendations (2/2)



- The current draft version of CPMS 2.0 Privacy Statement should be updated in alignment with GDPR/EUDPR requirements so to describe the following recommended aspects.

Recommendations for the Privacy Statement Update

The user data will be immediately deleted, except of users' activities such as healthcare professions participation in discussions, if the user delete his/her account through the CPMS 2.0 web interface. In this context, 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 web interface; In this context, the Privacy Statement should also determine the legal basis for this storage, as above.

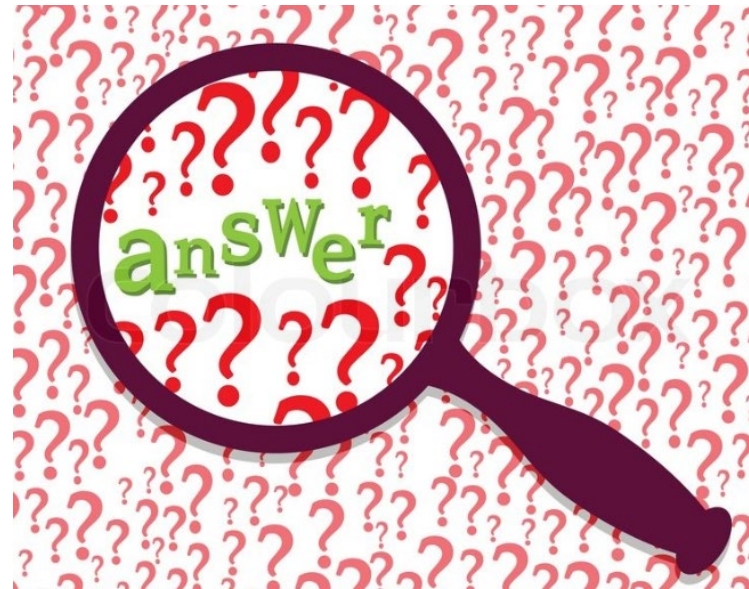
The user identification information could be transferred to Ukraine if a Ukrainian healthcare professional will invite the user so to assess a Ukrainian patient's rare disease through the CPMS 2.0 web interface.

The users should be informed about the potential risks to their rights and freedoms in case of identification information transfer to a third country (Ukraine) based on the results of TIA execution.

The usage of web cookies (if confirmed) including details about the information being recorded and processed.



1. Introduction
2. DPIA Requirement
3. Compliance Checklist – EUDPR/GDPR Principles
4. International Data Transfer
5. Risk Assessment
6. Implemented Security Measures
7. Recommendations
8. Q&A



Thank you for your participation!