CPMS 2.0 DPIA recommendations section

3.3 Conclusion and recommendations

CPMS 2.0 provides a layered and in-depth security ecosystem for the protection of personal data and a variety of organisational and procedural measures for the fulfilment of data subject's rights and freedoms. Each identified risk is being sufficiently mitigated to low levels.

This study 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 framework:

1. Coordination with the joint controllers (i.e. healthcare providers) so to develop an acceptable use policy and/or users' agreement which must be followed by CPMS 2.0 users when using the system;
2. DPIA risk threshold assessment and in case of 2 or more applicable criteria the joint controllers (i.e. healthcare providers) should execute a DPIA regarding their areas of responsibilities [R10], covering the users' systems which are being used for accessing CPMS 2.0, any internal IT system which is interconnected with CPMS 2.0 IT ecosystem and the security awareness of users. EC should contribute and provide support, if needed;
3. Establishment of a user access management process based on EC standard taking into account the variety of actors responsible for the IT administration activities and ERN networks which are responsible for users' access approval. The process should cover, at minimum, the activities and the recording for access rights request, approval, regular review and revocation;
4. Holistic and full scale penetration test execution by an independent party which would complement the already executed test at application level, would cover the AWS infrastructure elements and would also cover the simulation of specialised scenarios such as the internal malicious actors;
5. Disaster Recovery Plan (DRP) development based on the results of Business Impact Analysis and Risk assessment (i.e. Maximum Tolerable Time of Disruption is 48 hours, the unavailability impact is 6/10 and the unavailability of patient data could threaten the life of individual(s)). Although an IT contingency Plan and CPMS 2.0 integration in DG SANTE's Business Continuity Plan have been planned and the probability of an IT Disaster in cloud environments is very low, a DRP would cover the unavailability of the cloud provider for a limited period of time (i.e. higher than the defined RTO, RPO and MTPD) which can't be excluded;
6. The planning of annual Business Continuity and Disaster Recovery tests execution.

Furthermore, the study proposes a) the execution of a Transfer Impact Assessment (TIA) regarding the cases of users' identification information transfer to Ukraine. b) the update of the current draft version of CPMS 2.0 Privacy Statement in alignment with GDPR/EUDPR requirements. In particular, the Privacy Statement should describe:

1. That 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;
2. That 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, in accordance with Article 5 of the EUDPR, based on EDPB Guidelines 05/2020 on consent under Regulation 2016/679, points 117 and 118;
3. That 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. Also, 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 [R4];
4. The usage of web cookies (if confirmed) including details about the information being recorded and processed.