eHealth Network

Draft Recommendation Report to Go Live for Portugal

Drafted and adopted by eHMSEG on 16.05.2019

Purpose of this document:

On 4th December 2018, the National Contact Point for eHealth (NCPeH) of Portugal, submitted to the secretariat of the eHDSI Member State Expert Group (eHMSEG) an application to 'go-live' for the services Patient Summary-country A and B and ePrescription-country A and B. The application was accompanied by the following supporting documentation: a signed declaration; test reports; a follow-up audit report; and a list of the corrective actions planned or taken by the NCPeH to address the recommendations contained in the follow-up audit report.

In accordance with the 'go-live procedure', the eHMSEG evaluated the application on 12 December 2018 and decided to keep the Readiness Statement “on hold” until Portugal has undergone a follow up audit. The follow-up audit was carried out from 9 to 10 April 2019.

On 16 May 2019 eHMSEG has reevaluated the application. This document contains a summary of the evaluation and recommendations to the eHealth Network.

Section 1 Executive summary

The eHMSEG recommends that:

Goes live with observations, provided that:
1. All recommendations of the Follow-up audit report Reference No: 2019-6846 have been satisfactorily addressed and that this has been verified by the auditors, before entering routine operations.

- The NCPeH needs to submit a statement of the Auditors to the eHMSEG (via the secretariat) that all recommendations have been satisfactorily addressed.

2. The necessary conformance and functional tests were passed and that this has been confirmed by the Solution Provider before entering routine operations.

- The NCPeH needs to submit a statement of the Solution Provider to the eHMSEG (via the secretariat) that the necessary conformance and functional tests were passed.

The NCPeH can then enter routine operations without the need for further approval.

Section 2 Findings and evaluation

Section 2.1 Main findings of the conformance and functional test reports

The end-to-end functional testing aims to validate, from the user point of view, the process and the information provided by the eHealth Digital Service Infrastructure (eHDSI) services to health professionals. It is expected to detect flaws or malfunctions in any step of the process, from the processing of the original document to its transfer and subsequent processing and display in the receiver country. Furthermore, health professionals participating in the testing assessed the eventual clinical usefulness of the information provided. The evaluation is carried out for all eHDSI services (Patient Summary and ePrescription/eDispensation) in an environment that intends to simulate normal operations as much as possible: e.g. a pharmacist dispensing a medicinal product or a physician in an emergency department providing care to a citizen from a different deploying country. The only difference with a real scenario is that only test data are used and no real patients are involved.

In the Wave 2 Formal Pre-Preparatory Tests (February 2019) Portugal has undergone the tests with the Wave 2 specification for: ePrescription service Country A and Country B; and Patient Summary service Country A and Country B.

The report submitted demonstrates that the NCPeH has passed the necessary conformance tests. The functional tests report submitted demonstrates that the NCPeH should complete the tests with all the partners (in case they are available in the June 2019 test session).

Section 2.2 Main findings of the Follow-up audit report

The initial audit of the NCPeH (SPMS), against the readiness criteria checklist (version 1.19), took place in July 2018. The scope of the audit covered the organisation of the NCPeH and its activities in relation to the services Patient Summary-country A and B and ePrescription-country A and B, including sub-contracted parties. A follow-up audit was carried out from 9 to 10 April 2019.

The audit report concluded that:

"The National Contact Point for eHealth is in compliance with the readiness criteria pertaining to organisation and technical interoperability. Work remains to be done in relation to contractual compliance, service operations, information security, and semantics.

In particular, the NCPeH does not control the processing of cross-border health data by the relevant end users. These end users have not been identified as data processors and their activities are not covered in the business risk assessment, business continuity plan and the information security policies of the NCPeH. This means that the organisation cannot fully demonstrate its accountability for the cross-border services towards its stakeholders at national and European Union level, and that it creates risks to the confidentiality, integrity and availability of patient data.

In addition, the NCPeH does not have the means to properly manage access rights. This jeopardizes the ability to prevent, detect and act upon illegitimate activities, and creates significant risks to the confidentiality, integrity and availability of patient data. The lack of an approval procedure for the transcoding and translation of clinical vocabularies also creates risks to the integrity and availability of data."

No further actions are required in relation to conformance testing. As a result of the functional testing, it is recommended that Portugal should complete the tests with all the partners (in case they are available in the June 2019 test session).

Section 2.3 Evaluation

The draft follow-up audit report identifies nine non-compliances and contains recommendations to the NCPeH to address each of them. The following table provides an overview of these non-compliances and recommendations, and the corrective actions planned or taken by the NCPeH to address the recommendations.

	Non compliance	Audit conclusions for each domain	Recommendation	Corrective action proposed by the NCPeH
1	C.9 [critical]: Although third parties (i.e. health professionals and/or their representative organisations) process cross-border patient within the meaning of processing as defined in Article 4(2) of Regulation (EU) 679/2016, the NCPeH has not identified these parties as data processors as defined in Article 4(8) of the said Regulation.	The incomplete identification of data processors of cross-border patient data, means that the NCPeH cannot demonstrate its accountability towards its stakeholders at national and European Union level.	To identify comprehensively the responsible data controllers and data processors, in line with readiness criterion C.9.	Follow-up Audit (FA). R1. AP1. Review the DPIA in order to identify third parties acting as data processors. Completion date: 17/05/2019 FA. R1. AP2. Preparation and signature of a Protocol with the pharmacies and/or representative organizations, to define their responsibilities in the project. Completion date: 31/05/2019 FA. R1. AP3 Preparation and signature of a Terms and conditions applicable to define the Hospitals' responsibilities in the project. Completion date: 31/05/2019
2	OS.5 [critical]: The NCPeH communication processes with NCPeHs in other Member States do not cover the country-B services. For example, the service desk for foreign patients is not registered in the eHDSI trusted service desks contact list and it has no procedures/guidelines in place to deal with foreign patients. This is not in line with the eHealth Digital Service Infrastructure (eHDSI) Country Service Desk Guidelines adopted by the eHMSEG on 22 June 2018.	The operations services of the NCPeH are largely in compliance with the readiness criteria. However, the lack of preparedness of the service desk for foreign patients may lead to incidents not being adequately addressed, potentially affecting the confidentiality, integrity and availability of the cross-border health services.	To ensure that the NCPeH processes for communication with NCPeHs in other Member States include country-B services, in line with readiness criterion OS.5.	FA. R2. AP1. Define a procedure to support national and foreign patients in the cross-border health services scope. Completion date: 10/05/2019
3	IS.2 [critical]: The NCPeH cannot demonstrate that it follows the eHDSI Security Policies for end user identification and authorisation, and the related security audit.	The lack of implementation of eHDSI Security Policies for end users, inappropriate safeguarding of activity logs and inadequate management of access rights, pose significant risks to the confidentiality, integrity and availability of the data in the cross-border health services.	To ensure that the security measures set out in the eHealth Digital Service Infrastructure Security Policies are followed, in line with readiness criterion IS.2.	FA. R3. AP1. Update rule 4 and 5 from the mapping policies that had been considered out of scope. Completion date: 31/05/2019
4	IS.3 [critical]: End user information systems were not included in the risk assessment and the scope of this assessment was limited to information security.		To ensure that the business impact and risk assessment takes account of end user information systems, in line with readiness criterion IS.3.	FA. R4. AP1.Update the risk assessment in articulation with FA. R6.AP1. Completion date: 24/05/2019

5	IS.9 [major]: The NCPeH disseminates information to staff and has organised *ad hoc* information security training for some staff members in order to raise security awareness. However, there is no policy for providing the necessary security awareness training to all staff and newcomers.		To ensure that security awareness training specifically focused on security controls applicable to the national contact point for eHealth, is provided to all staff including newcomers, in line with readiness criterion IS.9.	FA. R5.AP1. Integrate the cybersecurity/Information Security training in the e-learning platform (eStudo) and confirm that all the project staff enrol in the course. Completion date: 17/05/2019 FA. R5.AP2. Create a procedure to ensure new project members enrol in the cybersecurity/Information Security training. Completion date: 17/05/2019
6	IS.11 [major]: The business continuity plan does not include provisions for the end users (health professionals) for country-B services.		To ensure that the business continuity plan includes the end users, in line with readiness criterion IS.11.	FA. R6. AP1. Analyse the project documentation and prepare a transverse risk analysis. Completion date: 15/05/2019 FA. R6.AP2. Update the BCP with the reviewed risk analysis and include a reference to the protocols established with the pharmacies and hospitals. Completion date: 24/05/2019
7	IS.24 [critical]: The NCPeH has no comprehensive overview of access rights granted to staff members and contractors, as access rights can only be seen per system. This impedes the possibility to manage effectively (i.e. to review, revoke or modify) access rights.		To ensure that users are assigned only the necessary rights for performing their duties on the systems and services, in line with readiness criterion IS.24.	FA. R7. AP1. Consolidation and documentation of NCPeH users´s access rights and profiles. Completion date: 31/05/2019 FA.R7.AP2. Certify and monitor access for NCPeH users´s based on profiles. Completion date: 31/05/2019
8	IS.31 [critical]: System administrators' and system operators' activities logs are only stored in the machine where these logs are generated. The administrator/operator has full access rights to these logs. The logs are thus not appropriately safeguarded. Moreover, there is no policy for reviewing the logs.		To ensure that system administrators and system operators' logs are appropriately safeguarded and reviewed, in line with readiness criterion IS.31.	FA. R8. AP1. Development of log centralization platform for further operationalization. Completion date: 31/05/2019 FA. R8. AP2. Development of logs policy and logs monitoring procedure. Completion date: 31/05/2019
9	SI.7 [critical]: There is no procedure for the approval of the transcoding and translation of clinical vocabularies.	The lack of an approval procedure creates risk to the integrity and availability of data in cross-border health services.	To ensure that the transcoding and translation of clinical vocabularies is approved following a formal procedure, in line with readiness criterion	FA. R9. AP1. Define a Translation and Transcoding process for the Semantic interoperability area that includes a cross-validation of the mapped value sets between elaboration and approval responsibilities. Completion date: 30/04/2019 Exhibit FA.R9.AP1 - Translation and Transcoding process

Section 3. Recommendations to go live for Portugal

The eHMSEG recommends that Portugal:

Goes live with observations, provided that:

1. All recommendations of the Follow-up audit report Reference No: 2019-6846 have been satisfactorily addressed and that this has been verified by the auditors, before entering routine operations.

   - The NCPeH needs to submit a statement of the Auditors to the eHMSEG (via the secretariat) that all recommendations have been satisfactorily addressed.

2. The necessary conformance and functional tests were passed and that this has been confirmed by the Solution Provider before entering routine operations.

   - The NCPeH needs to submit a statement of the Solution Provider to the eHMSEG (via the secretariat) that the necessary conformance and functional tests were passed.

The NCPeH can then enter routine operations without the need for further approval.