eHealth Network

Draft Recommendation Report to Go Live for Malta

Drafted and adopted by eHMSEG on 16.05.2019

Purpose of this document:

On 6th May 2019, the Information Management Unit of the Ministry of Health, the entity formally designated to operate the National Contact Point for eHealth (NCPeH) of Malta, submitted to the secretariat of the eHealth DSI Member State Expert Group (eHMSEG) an application to 'go-live' for the services Patient Summary – country A (PS-A) and Patient Summary – country B (PS-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 has evaluated the application. This document contains a summary of the evaluation and recommendations to the eHealth Network.

Section 1 Executive summary

The eHMSEG recommends that Malta:

Goes live with observations, provided that all recommendations of the Follow up audit report Reference No: 2019-6828 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.
- 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.

The reports submitted demonstrate that the NCPeH has passed the necessary conformance and functional tests.

Section 2.2 Main findings of the Follow-up audit report

The initial audit of the NCPeH, against the readiness criteria checklist (version 1.19), took place in September 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 Patient Summary - country B, including sub-contracted parties. A follow-up audit was carried out from 11 to 12 February 2019.

The follow-up audit report concluded that:

“The NCPeH in Malta is in compliance with the readiness criteria pertaining to contractual compliance, organisation, semantics and technical interoperability.

However, actions remain to be completed in relation to service operations and information security. The Service Level Management Plan of the NCPeH is incomplete as it does not include provisions for asset and configuration management. This could limit the control of the organisation over its service operations.

The most significant gaps in the information security domain are related to information security policies and to the user identification, authentication and authorisation system. In this regard, the findings identified pose significant risks to safeguarding the confidentiality and integrity of patient data”

Section 2.3 Evaluation

No further actions are required in relation to conformance and functional testing.

The report of the follow-up audit 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	Recommendation	Corrective action proposed by the NCPeH
1	OS.1 [critical]: The NCP has a Service Level Management Plan in place; however specific elements, such as asset management and configuration management, were not included in this plan.	The missing elements in the service level management plan and the absence of documented methods to monitor service capacity create risks for the availability of services during operations.	To elaborate further the Service (Level) Management Plan to ensure that it includes all the required elements and processes for the operation of the National Contact Point for eHealth, in line with readiness criterion OS.1.	More detail is needed in Service Operation Plan. Asset register needs to be prepared. Action: Malta IT Agency (MITA) and Gnomon to provide asset and configuration data with respect to infrastructure and software elements under their control; Ministry Information Management Unit to collate Asset Register and update Service Operation Plan.
2	OS.8 [critical] and IS.8 [critical]: The NCP has a documented incident management procedure and an incident management tool is in place; however, the scope of this procedure is limited to information technology (IT) related incidents only.		To ensure that the incident management procedure includes provisions for all the types of incidents, in line with readiness criteria OS.8 and IS.8.	Details on management of non-IT incidents need to be included in Service Operation Plan. Action: Information Management Unit to amplify the procedure and update Service Operation Plan.
3	OS.11 [major]: Changes to correct the underlying cause of incidents/problems are not managed via the current change management process, with the exception of those related to IT.		To put in place a change management process able to manage the corrections of all underlying causes of incidents/ problems, in line with readiness criterion OS.11.	Details on management of changes related to non-IT issues need to be included in Service Operation Plan. Action: Information Management Unit to amplify the procedure and update the Service Operation Plan.
4	OS.21 [major]: The NCPeH has no documented method to monitor its service capacity.		To ensure that the National Contact Point for eHealth is able to monitor its service capacity for the cross-border Information Technology services, in line with readiness criterion OS.21.	Specific text on service capacity monitoring is required. Action: Information Management Unit to prepare the specific document on Service Capacity.
5	IS.4 [critical] & IS.29 [critical]: The NCPeH has a comprehensive list of security controls in place. However, the audit team noted that these controls are not assigned to the assets relevant to the cross-border exchange of health data.	Gaps identified in the information security policies and implementation, pose risks to the confidentiality and integrity of the data exchanged in the cross-border eHealth information services.	To establish a comprehensive list of identified, applicable and implemented security controls in place ("Statement of Applicability") applicable to the cross-border exchange of health data, in line with readiness criteria IS.4 and IS.29.	Security controls are listed in the eHDSI (Malta) Security policy but need to be explicitly mapped to the assets in the new asset register (cf. Rec. 1). Action: Information Management Unit will update Security policy

	Non compliance	Audit conclusions	Recommendation	Corrective action proposed by the NCPeH
				document after feedback from MITA and Gnomon.
6	IS.6 [critical]: The NCPeH has no documented governance procedure to ensure that no cross-border data are transmitted to an entity that does not belong to the CBeHIS network.		To ensure that no cross-border data are transmitted via their services to an entity that either does not belong to or is not allowed within the Cross-Border eHealth Information System network, in line with readiness criterion IS.6.	Already the case, but not well demonstrated in writing. Action: Information Management Unit to explicitly document the administrative procedure it follows to instruct MITA to route network traffic from the National Patient Summary infrastructure exclusively to the NCPeH-A and from there exclusively to the NCPeH-B.
7	IS.7 [critical]: There is a complete list of logs collected by the NCP but the security policies applicable to collecting, analysing, storing and retaining logs are missing (e.g. access and analysis rights, retention period).		To ensure that there are security policies on how audit logs should be collected, analysed, stored and retained, in line with readiness criterion IS.7.	Policy text on audit logs needs to be amplified, clearly covering how the relevant logs are handled. Action: Information Management Unit to amplify the policy text on audit logs.
8	IS.20 [major]: The NCPeH's documented policies contain insufficient detail on how personally identifiable information is being safeguarded.		To amend the documented policies in order to define how personally identifiable information is safeguarded, in line with readiness criterion IS.20.	Text on safeguarding of personally identifiable information needs to be amplified into a full policy document including text from referenced documents. Action: Information Management Unit to prepare a document specifically describing safeguarding of personally identifiable information.
9	IS.24 [critical] and IS.27 [major]: The user identification, authentication and authorisation system as designed can ensure that users are assigned only the necessary rights for performing their specific duties on the systems and services. However, this system is still in the course of being implemented.		To complete the implementation of the user identification, authentication and authorisation system in order to ensure that users are assigned only the necessary rights for performing their duties on the systems and services, in line with readiness criteria IS.24 and IS.27.	Technical implementation was completed by the time the follow-up audit report was received. Action: Information Management Unit to carry out formal user acceptance testing (UAT). UAT report and software demo will be provided to the audit team.

Section 3. Recommendations to go live for Malta

The eHMSEG recommends that Malta:

Goes live with observations, provided that all recommendations of the Follow up audit report Reference No: 2019-6828 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.
- The NCPeH can then enter routine operations without the need for further approval.