DG SANTE

Audit Framework

eHealth

Document Control Page

Settings	Value
Document Title:	**eHealth Audit Framework**
Project Title:	**eHealth**
Document Authors:	**eHDSI Solution Provider**
Doc. Version:	**1.1.0 Operations Ready**
Sensitivity:	**Routine business information**
Release Date:	**05/12/2017**

Document Approver(s) and Reviewer(s):

NOTE: All Approvers are required. Records of each approver must be maintained. All Reviewers in the list are considered required unless explicitly listed as Optional.

Name/role	Action	Date

DRAFT Document history:

Changes to this DRAFT document are summarized in the following table:

Revision	Date	Author	Short Description of Changes
0.10	09/09/2017	eHDSI Solution Provider	Initial Version
0.20	14/02/2017	eHDSI Solution Provider	Review of initial version and comments.
0.30	21/02/2017	eHDSI Solution Provider	Implementation of review comments and final internal review
0.40	23/02/2017	eHDSI Solution Provider	Revised version
0.51	01-03/03/2017	Tapani Piha; Marcello Melgara; Klara Jirakova; Lília Marques; Konstantin Hyppönen	General revision
0.60	16/03/2017	eHDSI Solution Provider	Implementation of reviewers comments
1.00	20/03/2017	eHDSI Solution Provider	Revision and send for approval
1.10	29/09/2017	eHDSI Solution Provider	- Implementation of review comments contributed by MS (FI, DE, FR, MT, SE, CH) - Implementation of review comments contributed by European Commission Auditors (DG SANTE Unit F)
1.1.0	05/12/2017	eHDSI Solution Provider	Candidate version with minor corrections
1.1.0	06/12/2017	eHDSI Solution Provider	Doc. Version: change "Release Candidate" to "Operations Ready". No other changes

The version and revision integer x.y.z increase as follows:

- eHDSI Solution Provider internal revision: y increase by 1
- Revision by other than Solution Provider: z increase by 1
- Revisions send for approvals: x increase by 1

TABLE OF CONTENTS

Contents

Site left intentionally blank

1 INTRODUCTION

This document describes the eHealth Digital Service Infrastructure (eHDSI)[1] **Audit Framework** for the initial audit of a National Contact Point for eHealth (NCPeH).

The initial audit provides the NCPeH with objective information about its conformity with the eHealth Readiness Criteria. This information is relevant for decisions to be taken by the Member States on whether the NCPeH should *go live* in the Cross Border eHealth Information Services (CBeHIS) Network.

1.1 Purpose of the document

The purpose of this document is to provide guidance for the planning, conduct and follow-up of the initial audits.

1.2 Objectives of the Audit Framework

The Audit Framework aims at the following:

(1) Establish a common understanding and initial audit methodology between the participating Member States;

(2) Establish a common structure for planning, conducting, reporting and follow-up of initial audits.

1.3 Clarifications

(1) This Audit Framework has been developed for the initial audit. The eHDSI Audit Framework is mandatory for the initial audit and may be re-used, customised and improved for NCPeH internal assessments.

(2) The operational audits, covering all services operated by the NCPeHs, have been defined by the eHDSI Organisation Requirements to be performed every two years after the NCPeH entered into operation in the CBeHIS Network. Operational audits are outside of the scope of this Audit Framework.

(3) The decision making process to *go live* is not part of this Audit Framework. The decision to *go live* is handled under the Recommendation to join the eHealth Network in the Joint Action to support the EHealth Network (JAseHN) D5.6.3 Policy Paper on Assessment and Decision Procedures under the Connecting Europe Facility (CEF) Funding.

(4) This Audit Framework does not provide the process for Certification or Certification Audits according to international or national standards, although the initial audit follows the principles of international standards including: ISO 19011:2011 for Auditing Management Systems; ISO/IEC 27001:2013 for Information Security Management Systems; and ISO/IEC 20001-1:2011 and the best practice model ITIL® v3 for Service Management Systems.

[1] eHDSI Glossary available at: *https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Glossary*

1.4 Definitions

Initial audit is the independent Readiness Assessment to be performed by auditors from the European Commission in order to confirm the state of conformity of the NCPeH with the Readiness Criteria.

Internal audit is a self-assessment conducted by the NCPeH or on its behalf by another entity, in order to evaluate its state of conformity with the Readiness Criteria.

Follow-up are the activities to evaluate a corrective and preventive action plan and the assessment of its implementation. Depending on the nature of the findings, the follow-up activities can be desk based and/or on-site.

Readiness Criteria are the set of required controls for managing risks to information confidentiality, integrity and availability. These include a system of documented processes and procedures, legal, organisational, technical, operational and semantical requirements, and policies, as set out in the eHealth Network documentation and agreements.

Finding is evidence regarding the state of a conformity or non-conformity with the readiness criteria.

Major finding is evidence of a non-conformity with the readiness criteria which constitutes a potential risk to information confidentiality, integrity or availability, and therefore weakens the reliability of the NCPeH and/or the CBeHIS Network. Combined major findings may constitute a critical finding.

Critical finding is evidence of non-conformity with the readiness criteria which constitutes a significant risk to information confidentiality, integrity or availability, and therefore undermines the reliability of the NCPeH and/or the CBeHIS Network.

Supplier audit is an audit performed by the NCPeH or on its behalf by another entity, of a supplier or contracting party on aspects relevant to the NCPeH's conformity with the readiness criteria.

1.5 Auditors

Initial audits are carried out by lead auditors of DG SANTE Directorate F (Health and Food Audits and Analysis) of the European Commission with the assistance of experts from other Commission Services and/or the EU/EEA Member States.

2 AUDIT METHODOLOGY

2.1 Purpose of the initial audits to NCPeH

The purpose of the initial audit is to assess compliance of the NCPeH with the Readiness Criteria, in particular:

- Assess and verify compliance with the eHDSI legal, organisational, business, services, operational, technical, semantic and information security requirements, the mutual agreements and the legal frameworks, as appropriate;
- Assess whether written procedures and policies are adequate and are being followed;
- Assess that all necessary security and operation controls within the scope of the NCPeH are in place, adhered to and fulfil the agreed requirements;
- Assess whether the performed activities provide sufficient proof about compliance against the criteria or whether additional efforts are necessary by the NCPeH to fully cover the Readiness Criteria.

2.2 Audit Scope

The scope of the initial audit covers the organisation of the NCPeH and its activities in relation to the services implemented (ePrescriptions A/B and/or Patient Summaries A/B), including sub-contracted parties in governing and operating the NCPeH within the CBeHIS Network. Connectors with the national healthcare system are within the scope of the intial audit. While the national healthcare system is outside the scope of the audit, the audit report will contain a brief description of the organisation of the health system in the country and include background information on the proportion of national health care provision currently connected to the NCPeH for the services implemented.

2.3 Language regime

The working language of the initial audits will be English, with interpretation provided by the European Commission to and from one official language of the NCPeH, if necessary.

Certain documentation accompanying a request for the initial audit will need to be provided in English.

2.4 Audit Process

The initial audits will follow a specific audit life-cycle. The phases will include audit planning, audit conduct, reporting, and follow-up activities, as described below:

2.5 Planning of Audits

Once an NCPeH considers itself ready to *go live*, its chief executitve will submit a written request for an initial audit to the director of DG SANTE Directorate F. The request should include a statement regarding the services for which the NCPeH is ready (ePrespcription A, ePrescription B, ePatientSummary A, ePatientSummary B)

The request should be accompanied with:

- a description of the organisation of the NCPeH (including, notably, structure, legal entity, staffing level, quality management system, information security management system, and IT service management system);
- the report of the most recent internal audit; the completed self-assessment (against the Readiness Criteria) together with relevant supporting documents; and summaries of supplier-audit reports;

The European Commission Auditors will assess the information provided and will decide whether the documentation provided demonstrates the NCPeH's readiness for the audit to take place or whether the NCPeH needs to provide additional written information.

Subsequently, the European Commission will liaise with the NCPeH in order to establish mutually agreeable dates for carrying out the audit. The audit will take place over a maximum period of 5 working days. Once the dates for the audit have been agreed, the European Commission will formally announce the audit to the NCPeH. This formal announcement will include a detailed agenda for the audit and the name of the auditors that will be involved. The auditors may request for additional information/documentation to be submitted prior to the audit.

2.6 Performing Audits

2.6.1 Opening meeting

The initial audit will commence with a formal opening meeting. The meeting should be attended by the representative from the NCPeH who will accompany the audit team throughout the audit, NCPeH staff responsible for the areas under evaluation and, where appropriate, representatives of suppliers. The purpose of the opening meeting is to:

- introduce the audit team to the NCPeH representatives;
- confirm the audit plan, including the scope, objectives and the schedule of visits to different departments or involved areas;
- establish official communication lines between the audit team and the NCPeH during the course of the Audit;
- confirm that resources and facilities needed by the audit team are available;
- confirm the time, date and location of the closing meeting;
- discuss questions in relation to the documents received prior to the audit.

2.6.2 On-site Visits

Auditors will interview designated/selected staff members (and can select ad-hoc relevant personnel for spontaneous interviews) and check documents, databases and other sources of information, guided by the Readiness Criteria.

Auditors will on-the-spot discuss with NCPeH representatives the (preliminary) findings collected, in order to reach a common understanding of the outcome of the initial audit.

2.6.3 Closing meeting

The following persons should be present at the closing meeting: i) the audit team, ii) the representative(s) who have accompanied the audit team throughout the audit, and iii) the representatives from the NCPeH responsible for the areas under evaluation.

The purpose of the closing meeting is to present the overall outcome of the audit to the NCPeH. This includes notably an account of any critical findings and major findings, along with their supporting evidence, together with a preliminary conclusions relating to the impact of the findings on the confidentiality, integrity and availability of information transmitted in the context of the organisation's role as NCPeH.

Ideally, the audit team and the NCPeH should reach agreement as to the overall outcome of the audit and the corresponding findings, in particular those that are critical. In case the NCPeH disagrees with certain findings, this will be documented in the audit report.

2.6.4 Report

The initial audit report will be produced in English, in accordance with the Audit Report template [R02]. In case of critical and major findings, the report will contain recommendations to the NCPeH.

Within 15 working days of completion of the audit, the European Commission will submit a draft audit report to the NCPeH.

Within 10 working days of receipt of the Draft Audit Report, the NCPeH will submit comments, in English, on the report, including requests for clarifications and for correction of factual errors.

Any objections on the findings or conclusions will preferably have been discussed during the closing meeting (§ 2.6.3). However, if action has already been taken to address major or critical findings identified in the draft report, the NCPeH may send supporting evidence with their comments on the Draft Audit Report.

Within 10 working days of receipt of comments on the draft audit report, and in light of these comments, the European Commission will produce the final audit report. The final audit report will be submitted to the NCPeH together with a table detailing how each of the comments made on the draft audit report have been taken into account.

2.6.5 Action Plan

Within 15 working days of receipt of the audit report, the NCPeH will submit an Action Plan [R02] to the European Commission, detailing the actions taken and/or planned, including timelines, in order to satisfactorily address the recommendations made in the report. In order to expedite the process, the NCPeH is encouraged to submit the action plan together with their comments on the draft report.

The Action Plan will contain the finding description, the proposed corrective action by the Auditees, the responsible owner of the action and timeframes for completion of the corrective action(s).

Within 10 working days of receipt of the action plan, the European Commission will send, its assessment of the action plan and/or a request for additional clarifications, to the NCPeH.

2.7 Follow-up

The scope of follow-up will be restricted to the recommendations made in the report. This activity will be documented.

3 CONFIDENTIALITY

The European Commission will treat audit reports and information gathered in the context of the audits as confidential information.

Auditors of the European Commission and experts from the Member States and the eHDSI Solution Provider, who are member of the initial audit team, are bound by the confidentiality rules pertaining to staff of the European Commission.

In case that confidential information is sent to the Auditors, the NCPeH should ensure that this is sent through secure and/or encrypted communication means.

Annex A. Applicable and Reference Documents

Reference	Document Title	Version	Date
[R01]	eHDSI Readiness Criteria [2]	1.1	27/09/2017
[R02]	eHDSI Audit Report Template[2]	1.1	27/03/2017
[R03]	Requirements and Recommendations [3]	1.3.0	01/06/2017
[R04]	ISO/IEC 19011:2011 Guidelines for auditing management systems	n/a	2011
[R05]	D5.6.1 Policy Paper on How to Assess Member States Overall Readiness to *go live*	JAseHN 2.0	09/05/2017

Annex B. List of Abbreviations used in this document

Abbreviation	Definition
CBeHIS	Cross-Border eHealth Information Systems
eHDSI	eHealth Digital Service Infrastructure
eHOMB	eHealth Operational Management Board
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
JAseHN	Joint Action to Support the eHealth Network
MS	Member States
NCPeH	National Contact Point for eHealth
NCPeH A	NCPeH of country of affiliation of patient
NCPeH B	NCPeH of country of treatment of patient

[2] https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Audit+Framework
[3] https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Requirements+and+Recommendations