NMVO on-boarding guide

DISCLAIMER

This on-boarding guide for NMVOs and the related PowerPoint presentations (the "Guides") are provided "AS IS" by EMVO. They are provided for your information only and do not amount to professional advice or recommendations from EMVO. No warranty of any kind is made or given by EMVO with respect to these Guides or use thereof, including, but not limited to, as to the accuracy or the completeness thereof. Use of these Guides is at your own risks and perils. To the fullest extent permitted by applicable law, EMVO expressly disclaims all warranties of any kind, whether expressed or implied, including, but not limited to the warranties for hidden or latent defect, of merchantability, fitness for a particular purpose and non-infringement. EMVO shall not be liable for any direct or indirect damage, loss or claims, including loss of use, data, profits, benefits, data, business, opportunity, goodwill, clientele, for third party's claims, or for any other indirect, special, incidental or consequential damages of any kind in connection with or arising out of the use of any information disclosed hereunder, whether alleged as a breach of contract (including grave fault), tort, negligence (including gross negligence), hidden/latent defects, strict liability or any other legal theory, even if the EMVO had been advised of the possibility of such damage. Nothing herein shall, however, operate to limit or exclude any liability for fraud or other liability that cannot be legally excluded. EMVO reserves the right to amend this NMVO on-boarding guide at any time without prior notice.

Table of Contents

1 Introduction

Falsified medicines are a major threat to public health and safety. As falsifications become more sophisticated, the risk that falsified medicines reach patients in the EU increases every year. Falsified medicines represent a serious threat to global health and call for a comprehensive strategy both at European and international level. With the Falsified Medicines Directive and its supplementing Delegated Regulation the legislator has taken the necessary steps to prevent falsified medicines from entering the legal supply chain. One of the measures that is being undertaken to achieve this goal is to mandate pharmaceutical companies and parallel distributors of prescription medicines to apply safety features to the outer packaging.

1.1 Falsified Medicines Directive

Following adoption by the Council and the European Parliament, the Falsified Medicines Directive (Directive 2011/62/EU) was published on 1 July 2011 in the Official Journal of the European Union and applies since 2 January 2013 in all EU Member States. The Directive introduces rules to improve the protection of public health with new harmonised, pan-European measures to ensure that medicines are safe. To this end, these new measures include obligatory safety features on the outer packaging of medicines. These safety features consist of a unique identifier and an anti-tampering device which allow the verification of the authenticity of medicinal products subject to the FMD requirement and protect patients and business alike from the risks of falsified medicines.

1.2 Delegated Regulation

The Delegated Regulation (EU) 2016/161 detailing the characteristics of the safety features, how medicine authenticity should be verified, and by whom, was adopted on 2nd October 2015 and published, after scrutiny by the European Parliament and the Council, on 9th February 2016. The Delegated Regulation, and the new medicine verification system (repositories system) it specifies, will apply as of **9th February, 2019**[1]. The key principle is to guarantee medicine authenticity by an end-to-end verification system supplemented by risk-based verifications by wholesalers according to Article 20 of the Delegated Regulation (EU) 2016/161: Medicines should be systematically verified at the point of supply to the public (e.g. at pharmacy level). To make this possible, a repositories system should be established and managed by stakeholders. As set out in the Delegated Regulation the main tasks of the repositories system are to store the information of the legitimate Unique Identifiers (UIs) and to allow the verification/decommissioning of UIs at any point of the supply chain.

[1] Belgium, Greece and Italy may defer the application of Articles 1-48 of the Delegated Regulation (EU) 2016/161 by up to 6 years but Belgium has indicated that the earlier compliance deadline will be followed.

1.3 European Medicines Verification System

The European Medicines Verification Organisation (EMVO) is a Belgian non-profit organisation representing stakeholders united in securing the legal supply chain from falsified medicines. EMVO has taken responsibility for advancing the formation of the European Medicines Verifications System (EMVS) in accordance with the Falsified Medicines Directive (Directive 2011/62/EU) and the delegated Regulation (EU) 2016/161 to ensure the implementation of a functioning, secure, interoperable and cost-effective medicines verification system across Europe. Its founding members are EFPIA (the European Federation of Pharmaceutical Industries and Associations), Medicines for Europe (the European Generic and Biosimilar Medicines Association), PGEU (the Pharmaceutical Group of the European Union), GIRP (the European Healthcare Distribution Association), EAEPC (the European Association of Euro-Pharmaceutical Companies), HOPE (European Hospital and Healthcare Federation) and EAHP (European Association of Hospital Pharmacists).

Figure 1: EMVO Stakeholders

EMVO is setting up a pan-European infrastructure of repositories centered on the "European Hub (EU Hub)" which is currently operational in a ramp-up mode. The following system landscape has been selected since it ensures effective protection of patient safety and allows the fulfilment of specific requirements in different countries:

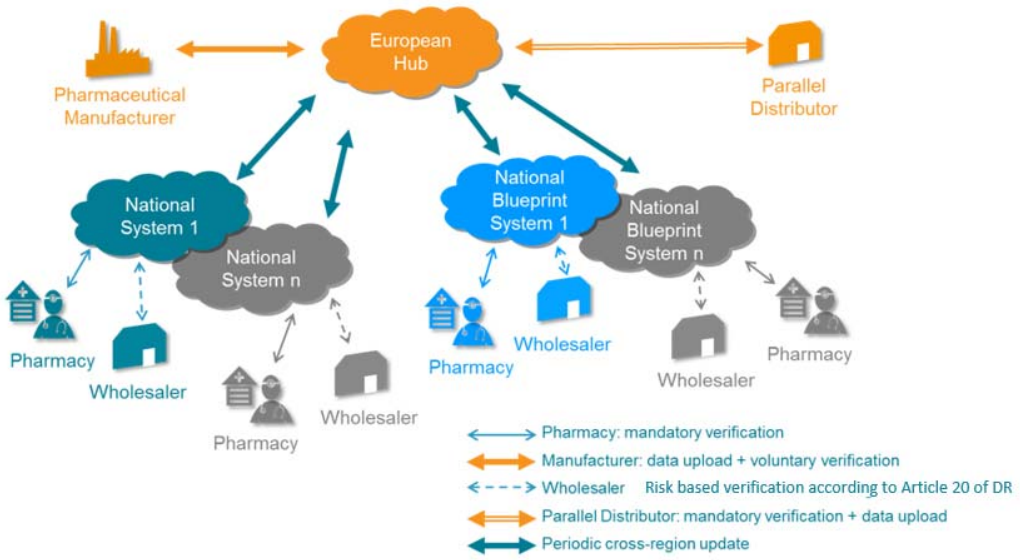


Figure 2: European Medicines Verification Landscape

The European Medicines Verification Landscape as depicted in the figure is composed of a central information and data router (EU Hub) and national systems (most of these will be so-called national Blueprint systems i.e. built to a standard template specified by EMVO).

The Organisation Chart of EMVO can be consulted in Appendix 7.1 Appendix 1: Organisational Chart.

1.3.1 European Hub (EU Hub)

The EU Hub is the central element of the European Medicines Verification System (EMVS). The EU Hub has been operational since 2014 and is currently in ramp-up mode.

The primary purposes for the EU Hub are to centralise the uploading of data thereby minimising the number of technical interfaces that have to be supported by all connecting clients, to implement and maintain a set of standardised interfaces that in turn support the overall principles of system interoperability and to serve as a single, fundamentally secure entry point for all EMVS master data. The EU Hub has robust processes to ensure that each party connecting to the system has been verified and validated as a genuine connecting partner with valid reasons for injecting data in to the overall EMVS. By providing the EU Hub with these primary attributes, the overall system cost can be minimised due to the centralised security process and the centralised and minimised number of interfaces that must be maintained.

The EU Hub as the core component of the EMVS performs the following tasks:

- It provides a single-entry point for MAH without parallel distribution activity and MAH with parallel distribution activity (Parallel Distributors) to upload their product serialisation data.

- It provides a single access point from which national systems can obtain revised/new product serialisation data.
- It provides a centralised location for the storage of master data and master data regarding the connected national systems.
- It provides a means by which multi-market packs can be systematically marked as 'decommissioned' in all affected markets once a pack has been dispensed in one market.
- It provides a means to decommission packs by MAH without parallel distribution activity and MAH with parallel distribution activity (Parallel Distributors).
- It provides a verification gateway for parallel distributors to access the repositories of the source markets for verification of authenticity.
- It provides a central point from where information concerning product recalls can be transmitted in addition to the established recall procedures.
- It provides a mechanism by which exported and imported products can be reconciled at a dose level as they are used by parallel distributors in repackaging / relabeling.
- It provides a central point from which alerts, that cannot be handled solely at the national level e.g. issues in different countries with multi-market packs, can be managed. This includes providing response e.g. to the appropriate company/regulatory authority etc.
- It provides a platform permitting cross-country inquiries, in accordance with Article 34(2) of the Delegated Regulation (EU) 2016/161, in order to verify whether a UI that was not found in a national repository is stored elsewhere in the repositories system.

1.3.2 National Medicines Verification Systems

The National Medicines Verification Systems (NMVS) are currently being established in all participating Member States. The main purpose of the National Medicines Verification Systems is to serve as the verification platforms that pharmacies or other registered parties such as wholesalers, self-dispensing doctors or hospital pharmacies will use to check a product's 'authenticity'. All data necessary to perform this and other relevant transactions are stored in the respective NMVS.

The key tasks of the National Systems are:

- Hold the relevant product serialisation data for this market.
- Receiving revised/new product serialisation data from the EU Hub.
- Serving as the verification platform for pharmacies or other registered parties such as wholesalers and hospitals to check for a product's authenticity.
- Serving as the platform wholesalers in the case of member states application of Article 23 of the Delegated Regulation (EU) 2016/161.
- Serving as the platform for wholesalers to mark a product pack as 'decommissioned' e.g. 'exported out of EU'.

2 Objective of this NMVO on-boarding guide

The objective of this NMVO on-boarding guide is to provide all NMVOs information on the formalities to be taken into account, including the system assessment, to establish a connection between the productive NMVS environment and the productive EU Hub environment. This guide will also provide information on the quality assurance goals which the NMVO is expected to meet and the approach to the audits which are planned to be executed by EMVO.

3 On-boarding process of an NMVO

3.1 Introduction to the on-boarding process

As EMVO promotes to have the NMVS's connected to the productive EU Hub as soon as possible and thus allow the Pilot to start for each NMVO as soon as possible. Therefore, EMVO allows the technical on-boarding of a NMVS even before all quality assurance goals have been met. NMVO's are responsible in achieving their quality assurance goals in line with local (timing) requirements.

Note that this NMVO on-boarding guide will focus on the sign off of a contract between the NMVO and the EMVO, the system assessment and the Technical on-boarding. In figure 3 below this approach is visualized with the dark-blue arrows. The Start, Pilot- and the Ramp-up (light blue arrows) are added to frame the dark blue steps.

The Pilot will start when the productive environment of a NMVS is technically connected to the productive EU Hub environment. At this moment, the system is technical live. During the Pilot, End Users are on-boarded sequentially to allow lessons learned to improve the on-boarding process.
When a high degree of confidence has been established in the End User on-boarding process, the Ramp-up starts. In this Ramp-up, different End Users may on-board in parallel.

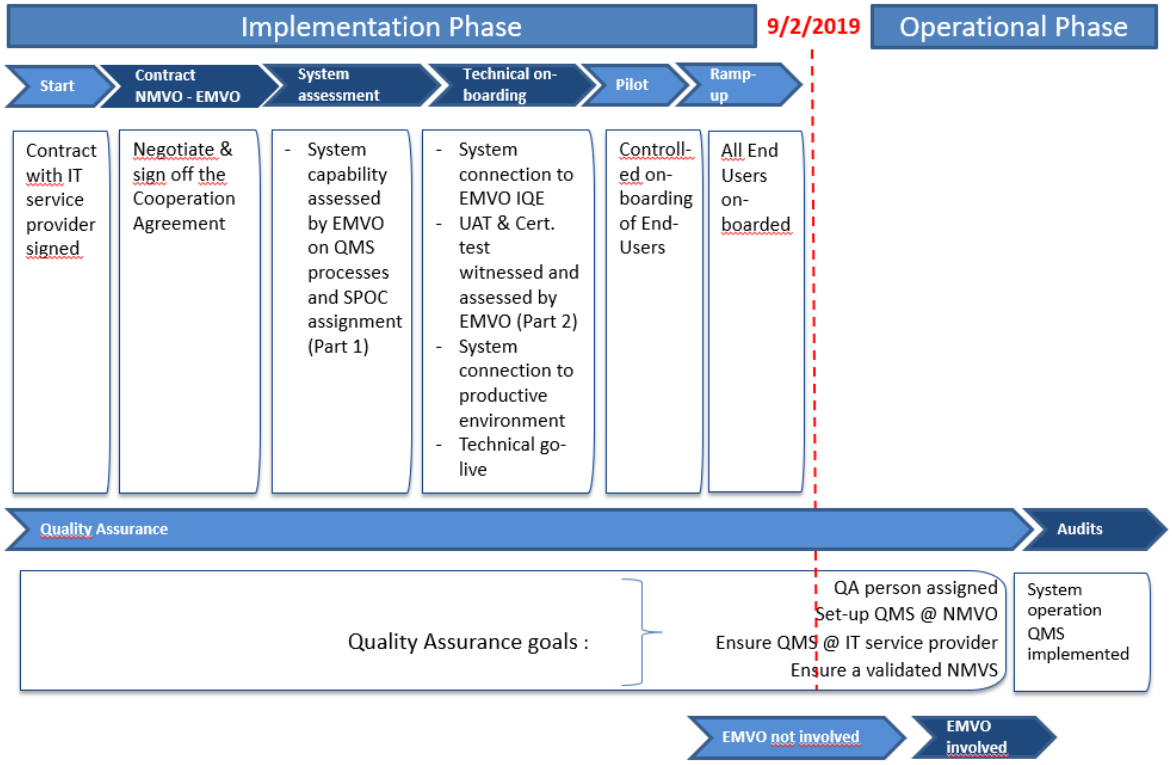


Figure 3: on-boarding process steps

3.2 Contractual: EMVO-NMVO Cooperation Agreement

Before an NMVO can on-board its NMVS to the EU Hub, a Cooperation Agreement has to be in place between EMVO and the NMVO. This Cooperation Agreement can be obtained from EMVO on request. The Contract Agreement will only be signed if the NMVO is compliant with Article 31 of the Delegated Regulation (EU) 2016/161.

The NMVO will also have to have a contract in place with an IT service provider which ensures the development of the NMVS and the future maintenance. This maintenance will have to respect agreed service levels as defined in SLA's.

As the IT service provider contract is likely to be in place at the moment of reading this NMVS on-boarding guide, we will not further elaborate on this.

3.2.1 Negotiate & sign off the EMVO-NMVO Cooperation Agreement

This Cooperation Agreement will set the contractual framework during the EMVS Implementation Phase for the cooperation between the European Medicines Verification Organisation A.S.B.L. at 1040 Brussels – Belgium ("EMVO") and the National Medicines Verification Organisation ("NMVO") – the legal non-for profit organisation of that country. Note that in case of a national two-tier structure, the affiliate of the NMVO (bound jointly and severally with the NMVO) – e.g. a limited company (Ltd.) governing the NMVS and its operations: all involved parties are directly bound to the provisions of the Cooperation Agreement.

This contract will set the parties' respective rights and obligations in relation to the development, implementation, testing and operation of the NMVS, the connection between the EU Hub and the NMVS, and the use of the EU Hub and NMVS to transfer data between them as well as the other use cases as specified in the EMVS URS as provided by EMVO.

The target is to allow End Users to verify authenticity of medicines in accordance with the Falsified Medicines Directive and Delegated Regulation latest on the 9th of February 2019. As part of the EMVS Implementation Phase it is agreed that the EMVS or any of its components may be substantially changed or amended.

Protection of the system security is one of the guiding principles that shapes the Cooperation Agreement. The Parties shall implement state-of-the-art security measures and at least the security measures as requested in the SDK. SDK and other confidential information is to be provided only on a need to know basis. The use of SDK is restricted to the purposes of the Cooperation Agreement. Each party has the right to disconnect the NMVS from the EU Hub in case it believes that the NMVS immediately or substantially endangers the security or functioning of the EMVS in whole or in part. The exchange of reports on a regular basis is foreseen in the Cooperation Agreement. Legitimacy checks and control are to be implemented for all System Users in accordance with Falsified Medicines Directive (FMD) and Delegated Regulation.

A procedure is foreseen to handle a security breach in a cooperative manner where information is to be provided within 24 hours after awareness. If an investigation is required, full cooperation is required from all parties and all measures are to be taken to solve issues, to mitigate the consequences and to prevent

reoccurrence. If required by applicable law, a notification of public authorities or individuals is made and remedial actions are undertaken.

The Cooperation Agreement stipulates main responsibilities of EMVO as there are:

1. Develop and operate the EU Hub for the purposes in accordance with FMD and Delegated Regulation;
2. Provide documentation and SDK for the development and use of the EU Hub-NMVS interface
3. Provide a contact person for this Cooperation Agreement;
4. Provide information about key facts, project status and project progress on EU Hub interface development;
5. Undertake best efforts to provide EU Hub functionality in a diligent manner and to protect it with state-of-the art security measures;
6. Provide copy of insurance, if any.

The Cooperation Agreement stipulates main responsibilities of the NMVO as there are:

1. Develop and operate the NMVS for the purposes, in accordance with the SDK, the Cooperation Agreement and FMD and Delegated Regulation;
2. Protect its NMVS with state-of-the-art security measures (and at least the security measures set forth under the SDK);
3. Ensure that its IT service provider is subject to equivalent obligations;
4. Carry out legitimacy check and ensure that End Users are held with appropriate terms to use the EMVS;
5. Provide a contact person for this Cooperation Agreement;
6. Be responsible towards EMVO for activities carried out on its NMVS;
7. Provide copy of insurance, if any.

The guiding principle is a back to back provision that:

1. Excludes implied warranties; the EU Hub and NMVS are provided "as is"
2. Excludes indirect or consequential damages
3. Allows a party to recover direct damages from the other party (provided that the other party can itself recover such damages from its IT service provider to the extent it relates to a breach of its obligations by such IT service provider in relation to the design, builds, test and deployment of the Hub/NMVS)
4. Excludes EMVO's liability for inaccurate, incomplete or corrupted data, or any malicious software

The liabilities of all parties will be capped on a level of 20 K Euro.

The Cooperation Agreement will automatic expire on 8th of February 2019. A mutual extension by way of amendment is possible for the Operational Phase. EMVO will set up a working group with some country representatives in 2017 to develop a new contract template for the Operational Phase that is supported by all parties until end of Q1 in 2018. The contract template for the Implementation Phase will be the starting point. The selection of country representatives will be proposed by EMVO stakeholders.
The Cooperation Agreement can be dissolved by either party in case of:

a. Breach of material obligation under the DR;
b. Change of legislation affecting the capacity of a party to operate the Hub or the NMVS;
c. If the other party loses its competence to act in its role.

3.3 System assessment part 1

3.3.1 System assessment part 1 assessed by EMVO

The NMVO's system capability will be assessed by EMVO. This assessment will focus in part 1 on:

- The NMVO processes and their capability to ensure that the minimum quality expectations are met at this stage of the EMVS project for the following topics:
  - Financial stability
  - Information security management;
  - Roles and responsibilities;
  - End User legitimacy check;
  - On-boarding process;
  - Access management;
  - Incident management;
  - Change management.
- The assignment of a Single Point of Contact (SPOC) by the NMVO and optional a 'backup SPOC'. The SPOC is the key contact person for EMVO and is authorized by the NMVO as the responsible for providing the requested information for the NMVO to establish and maintain a connection with the EU Hub.

As per Cooperation Agreement, the NMVO will support these assessments with all reasonably necessary support. The costs of these assessments shall be at the expense of the NMVO, though the EMVO shall provide a cost estimate to the NMVO in advance to obtain informed consent. All documentation is to be provided in the English language.

3.3.2 Request for System assessment part 1, UAT and System assessment part 2.

The NMVO will send an email to helpdesk@emvo-medicines.eu to request the NMVS on-boarding. The NMVO will provide :

a) The planned week of the UAT
b) The planned go-live date

Before the NMVO will submit its request, it will consult the NMVO on-boarding planning as available on SharePoint via NMVO On-boarding Planning. Please note that EMVO will support maximum 1 UAT per week.

EMVO will either confirm the requested week of UAT or inform the NMVO to choose another week to perform the UAT.

An NMVO may provide different dates in sequence of preference in their first request.

3.4 Technical on-boarding

Before the technical on-boarding can start, the Blueprint service provider develops and tests the NMVS against an EU Hub environment that is provided by Solidsoft Reply to the Blueprint service provider who has a Service provider support agreement with Solidsoft Reply in place. It is not EMVO's role to provide this EU hub environment and EMVO will not intervene in these IT provider relationships.

When the system positively passed the ITAT (IT Acceptance Test, aka as Functional Testing or Integration testing), the NMVO may start the Technical on-boarding to the EU Hub to execute the UAT against the EMVO IQE environment.
During the technical on-boarding, the NMVS (NS IQE) will be connected to the EMVO controlled IQE certification test environment (EMVO IQE). With these environments connected, the NMVO will perform a UAT of their NMVS and a formal certification test.

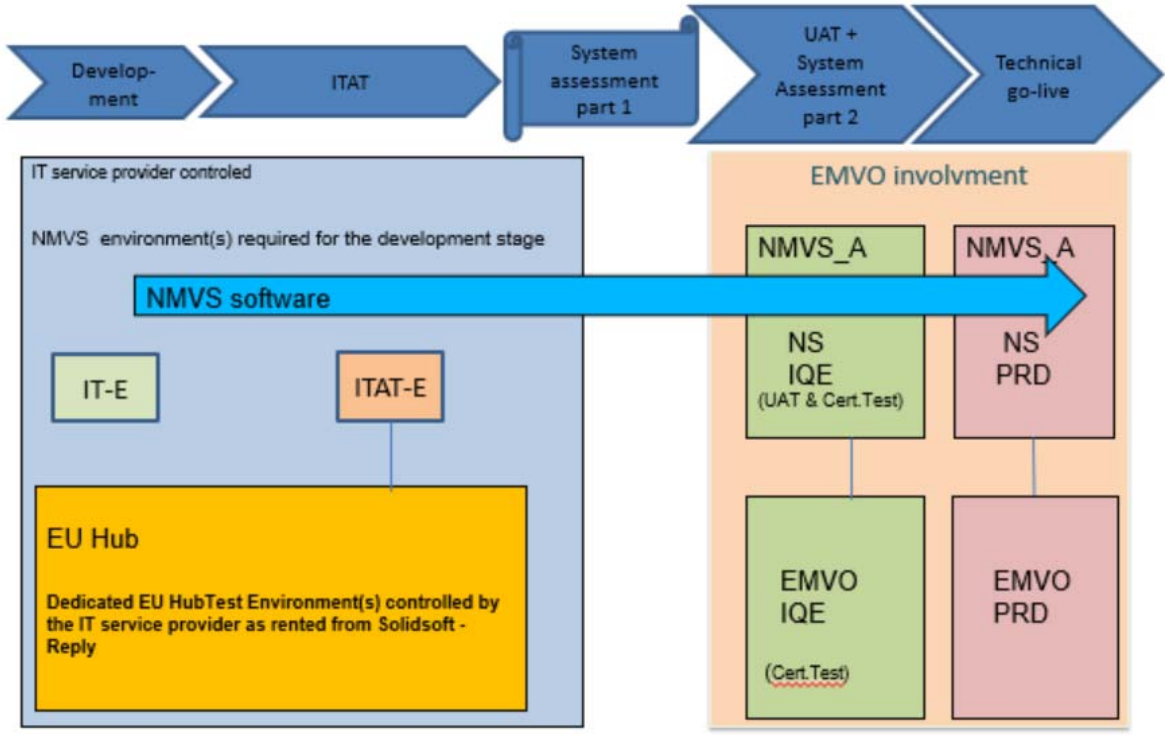


Figure 4: NMVS: from development to technical go-live

3.4.1 System connection to IQE test environment

The technical on-boarding process will be triggered by the NMVO in its role as System owner.

EMVO will now issue an NMVS Connection Request Form (see 7.2 Appendix 2: NMVS Connection Request Form aka CRF) which is to be completed and signed by the NMVO and issued to EMVO under the initially created ticket number.

EMVO will now sign off the NMVS CRF and create a customer ID for the EMVO IQE environment. The NMVO (or its IT service provider) will now create a Certificate Signing Request-file or CSR-file and send this back to EMVO. EMVO will forward this file to the IT service provider of the EU Hub. This EU Hub IT service provider will sign and return the Certificate or CER-file to the EMVO helpdesk who will issue the CER file to the NMVO together with end-point information and an initial security token for EMVO IQE. With this information, the IT service provider of the NMVS can supply access to the EMVO IQE environment of the EMVO controlled EU Hub.

3.4.2 UAT witnessed by EMVO, System Assessment part 2 and the Certification Test

EMVO will witness the UAT for all NMVSs to ensure that the system will meet the requirements as defined in the EMVS-URS as issued by EMVO.

This UAT will be performed within the NMVS IQE environment which is connected to the EMVO IQE environment.

The UAT-test report, the external security audit report and the traceability matrix should be made available by the NMVO to EMVO as it will act as input for the system assessment part 2.

Note: For Blueprint model system implementations, EMVO may decide not to witness the UAT as of the 2nd implementation of the same Blueprint supplier.

The NMVO's system assessment part 2 will now be managed by EMVO and this will focus on:

- the NMVS functionality to ensure that the EMVS requirements are covered.
- the test results from the UAT
- the Certification Test results
- the external security audit report

When the NMVO passed the system assessment part 2, the NMVO can connect its productive NMVS (NS PRD) to the productive EU Hub environment (EMVO PRD). In Figure 4 above, the full NMVS software deployment process is visualized. Please note that EMVO is only involved in the EU Hub environments (EMVO IQE and EMVO PRD) in the beige background (marked with 'EMVO-involvement').

The assessment results will be assessed by EMVO, and if:

1. The assessment outcome is negative, a feedback assessment report will be issued to the NMVO and corrective actions and a retest are requested;
2. The assessment outcome is positive, the connection to the EU Hub productive environment (EMVO PRD) can be granted.

As per Cooperation Agreement, the NMVO will support these assessments with all reasonably necessary support. The costs of these assessments shall be at the expense of the NMVO, though the EMVO shall provide a cost estimate to the NMVO in advance to obtain informed consent.

3.4.3 System connection to productive environment

The NMVO (or its IT service provider) will create a Certificate Signing Request-file or CSR-file and send this back to EMVO. EMVO will forward this file to the IT service provider of the EU Hub. This EU Hub IT service provider will sign and return the Certificate or CER-file to the EMVO helpdesk who will issue the

CER file to the NMVO together with end-point information and an initial security token for EMVO PRD. With this information, the IT service provider of the NMVS can supply access to the productive environment of the EMVO controlled EU Hub (EMVO PRD).

3.5 Quality Assurance goals

As stated in chapter 3.1 Introduction to the on-boarding process of this on-boarding guide, the Quality Assurance goals are the responsibility of the NMVO in its role as System owner of its NMVS. It is the NMVO which must decide how and when these goals are to be achieved. EMVO will not make Quality Assurance a prerequisite for the on-boarding to the EU Hub and thus allow the NMVO to start the Pilot as soon as possible.

We distinguish 4 main Quality Assurance goals for NMVO's. These are:

1. QA person assigned;
2. Set-up QMS for the NMVO;
3. Ensure QMS of the IT service provider;
4. Deliver a validated NMVS.

In this chapter, all 4 Quality Assurance goals will be discussed.

3.5.1 QA person assigned

The assignment of a QA responsible person within the NMVO is the first goal to achieve. In small organisations, it may be decided to combine the QA role with another role. However, to ensure independency of the operations, the QA role cannot be the same person as the operations manager.

The QA person reports directly to the head of the NMVO and is expected to have at least the following responsibilities:

- Establish and maintain a Quality Management System within the NMVO;
- Supervise and follow up the quality management activities of the suppliers and process owners;
- Determine the quality impact related to changes and undesired events;
- Ensure that the NMVS is validated and compliant with applicable regulations;
- Represent the NMVO during external audits.

3.5.2 Set-up QMS @ NMVO

The NMVO also has to have a minimum set of defined processes in place which are documented in the Quality Management System (QMS) of the organization. As minimum requirement for the QMS of an NMVO, EMVO sees following documents to be available as part of the QMS of the NMVO:

1.	QMS manual
2.	NMVO controlled document list
3.	Validation policy
4.	Validation plan template
5.	Validation report template
6.	Document management system
7.	User requirements specification template
8.	Roles & responsibilities

9.	Risk management
10.	Risk management template
11.	Information security management
12.	Initial system assessment template
13.	Test management
14.	Release & deployment management
15.	Change management
16.	Change request template
17.	Training management
18.	Training registration form template
19.	QMS training requirements
20.	Access management
21.	On-boarding process (incl. legitimacy check)
22.	User requirements specification
23.	Incident management
24.	Incident investigation report template
25.	CAPA management
26.	CAPA form
27.	Audit management
28.	Complaint management
29.	Business continuity management

Still the NMVO may decide at any time the composition of its QMS and extend this with other procedures. Also, national regulatory requirements are to be taken into account.

EMVO provides countries which subscribed for the Blueprint model with free of charge QA templates for NMVO's. These templates are expected to form a solid base to develop the QMS for an NMVO. Still tailoring of these templates remains required to ensure processes meet the specific needs of the NMVO. Please note that tailoring service for Blueprint model based countries may be provided by EMVO and are subject to payment.

3.5.3 Ensure QMS of IT service provider

The IT service provider of a NMVS needs to have a QMS in place. This is required to ensure that the IT service provider is capable of delivering validated software and maintain the validated status of the software.

Again, it is the responsibility of the NMVO in its role as System owner to ensure that the IT service provider maintains a QMS which meets the QA expectations of the NMVO.

3.5.4 Deliver validated NMVS

Finally, a NMVS will have to be validated. This falls also under the responsibility of the NMVO in its role as System owner. The validated status should be set and should remain during the life cycle of the system.

3.6 Audits

As foreseen in the NMVO-EMVO Cooperation Agreement, EMVO plans to perform audits.

The purpose of these audits is to verify whether the NMVS, its system operation and support processes are compliant with EMVO's quality expectations and to ensure that the functional scope which was developed and implemented is following the regulations governing the control and release of medicinal products in the EU and with the NMVOs own applicable standards and procedures.

The objectives of the NMVO audits are therefore to verify:

- The NMVO capability from a quality point of view to operate the system in a validated status, including all related qualification activities and required deliverables for validation related functions.
- Achieve high degree of confidence that the functionality implemented will perform according to the specified user requirements and functional specifications in a consistent and reproducible manner.
- Ensure that the quality management processes of the IT service provider are meeting the EMVO quality requirements.
- Compliance of NMVO to Article 31 of the Delegated Regulation (EU) 2016/161.

These audits will be scheduled in agreement with the NMVO and are not a condition for the technical on-boarding of the NMVS to the EU Hub. EMVO will allow NMVO's time to prepare the QA goals in parallel during the Implementation Phase and beyond (see also introduction of the on-boarding process).

As of Q3 2017, audits may be performed on request of the NMVO. When an audit is requested, a timeslot to perform the audit will be agreed between EMVO and the NMVO. Such audits can be requested by contacting EMVO Quality Assurance by email and will always be performed on-site in the offices of the NMVO during an average 2 days visit. All NMVO staff is expected to be available during the audit.

After the audit is performed, the auditors will document their observations and findings in an audit summary report. The lead auditor communicates this report to the NMVO for review, feedback and potential corrective actions. The report and NMVO responses are then delivered to EMVO.

As per Cooperation Agreement, the NMVO will support the audits and assessments with all reasonably necessary support. The costs of audits and assessments shall be at the expense of the NMVO, though the EMVO shall provide a cost estimate to the NMVO in advance to obtain informed consent.

3.6.1 System operation

The assessment of the system operation will focus on the operational processes of the NMVS and how these have been applied.

3.6.2 QMS implemented

The implemented QMS will be assessed during the audit for its processes and how these have been applied.

For both system operation and implemented QMS, the following applicable regulation & best practices will be considered during the audit:

- Directive 2011/62/EU and Delegated Act;
- GAMP5, A Risk-Based Approach to Compliant GxP Computerized Syst.;
- Eudralex Volume 4 and Annexes (e.g. Annex 11, Annex 15);
- ISO/IEC 27001: 2013 Information security management systems;
- ISO/IEC 27002: 2013 Code of practice for information security management;
- ISO/IEC 27005: Information security risk management;
- ISO/IEC 38500: Information Technology Governance;
- ISO/IEC 20000: IT service management.

4 Definitions

Blueprint provider	Shall mean arvato System GmbH or Solidsoft Reply Ltd with which EMVO concluded a framework contract related to the implementation of certain aspects of the EMVS
Cooperation Agreement	Cooperation Agreement refers to the contract template document 'EMVO_0081_Template Cooperation Agreement for the implementation of the EMVS'
End Users	End User shall mean any wholesaler, pharmacy or other person authorized or entitled to supply medicinal products to the public as foreseen under the EU Directive on Falsified Medicines and the Delegated Regulation.
Implementation Phase	EMVS project phase which runs till February 2019 and during which all EMVS systems are implemented
IT service provider	
Operational Phase	EMVS project phase which as of February 2019 and during which the EMVS systems are in operational use
Pilot	During this step, the first End Users are on-boarded sequentially to an NMVS.
Ramp-up	During this step, the first End Users are on-boarded in parallel to an NMVS.
System owner	The person ultimately responsible for the availability, support and maintenance of a system and for the security of the data residing on that system.

5 List of Abbreviations

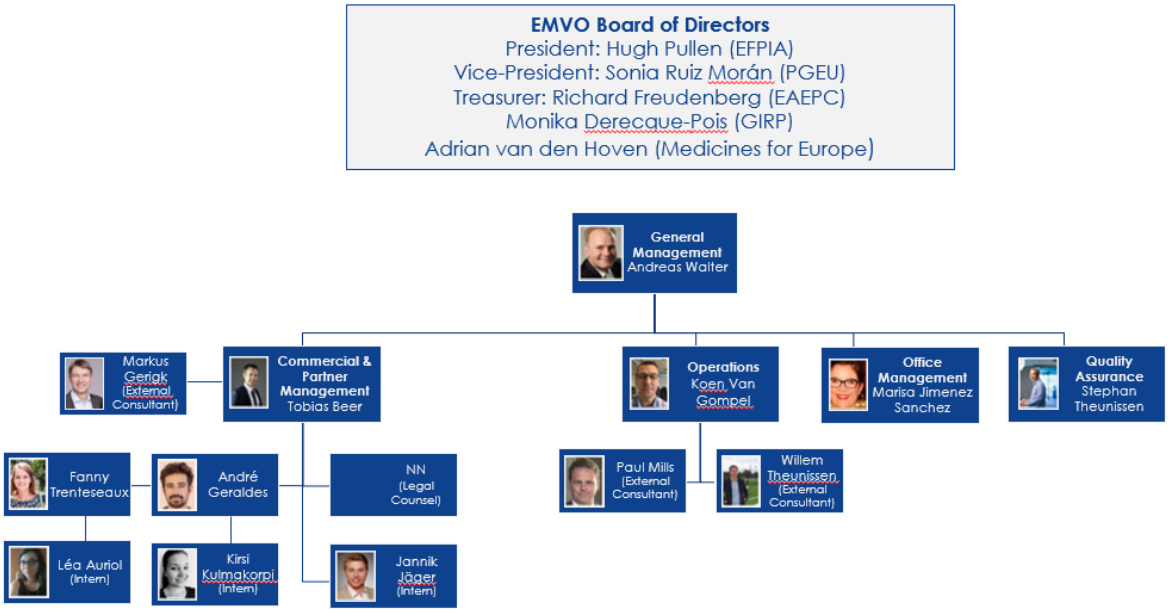
CAPA	Corrective Actions, Preventive Actions
CER	Certificate
CSR	Certificate Signing Request
DR	Delegated Regulation
EAEPC	European Association of Euro-Pharmaceutical Companies
EAHP	European Association of Hospital Pharmacists
EFPIA	European Federation of Pharmaceutical Industries and Associations
EMVO	European Medicines Verification Organisation
EMVS	European Medicines Verification System
EU Hub	European Hub
FMD	Falsified Medicines Directive
GIRP	European Healthcare Distribution Association
GxP	G = Good, x = attention area (e.g. M for Manufacturing or D for Distribution) and P = Practice. General term to refer a set of Best Practices used in the Pharmaceutical industry
HOPE	European Hospital and Health Federation
IQE	Integrated Quality Environment
ITAT	IT Acceptance Test
ITE	Integrated Test Environment
MAH	Marketing Authorisation Holder
NMVO	National Medicines Verification Organisation
NMVS	National Medicines Verification System
PGEU	Pharmaceutical Group of the European Union
PRD	Production Environment
QA	Quality Assurance
QMS	Quality Management System
SDK	Software Development Kit
SLA	Service Level Agreement
SPOC	Single Point of Contact
UAT	User Acceptance Test
UI	Unique Identifier

6 Reference Documents

Reference or version	Title
EMVO_0112	NMVO on-boarding presentation
Eudralex Volume 4, Annex 11	Good Manufacturing Practice - Medicinal Products for Human and Veterinary use – "Computerised Systems"
Eudralex Volume 4, Annex 15 (aka PIC/S PS/INF 11/2015)	Good Manufacturing Practice - Medicinal Products for Human and Veterinary use – "Qualification and Validation"
GAMP5	A Risk-Based Approach to Compliant GxP Computerized Systems
GAMP Good Practice Guide	A Risk-Based Approach to Operation of GxP Computerized Systems
GAMP Good Practice Guide	IT Infrastructure Control and Compliance
GAMP Good Practice Guide	A Risk-Based Approach to Testing of GxP Systems
GAMP Good Practice Guide	A Risk-Based Approach to Compliant Electronic Records and Signatures

7 Appendices

7.1 Appendix 1: Organisational Chart



7.2 Appendix 2: NMVS Connection Request Form

A - Information on the NMVO contracting partner (to be completed by EMVO)	
1. Name of the organisation	*<Indicate the registered name of the NMVO which is the System owner of the NMVS connecting to the EU Hub>*
2. Address of the organisation	*<Registered postal address of the NMVO named above, including country and postal code if applicable>*
3. Contract party number	*<Indicate the number under which the legal entity of the contract party is known in the EMVO contract repository>*
4. NMVO Cooperation Agreement number	*<Indicate the NMVO Cooperation Agreement contract number as per EMVO contract repository>*

B - Information of the requesting organisation	
1. Telephone number of the organisation	*<Phone number of the organisation named above, including country code in parentheses e.g. (44) 1256 375700>*
2. V.A.T.-number and Trade Register number of the organisation	*<The official VAT-number and the Trade Register Number of the organisation named above>*
3. Name of the contact person responsible for the Cooperation Agreement	*<The name of the contact person of the organisation named above who is responsible for the legal aspects of the contract between the above mentioned organisation and the EMVO>*
4. Email address of the contact person responsible for the Cooperation Agreement	*<The email address of the contact person of the organisation named above who responsible for the legal aspects of the contract between the above mentioned organisation and the EMVO>*
5. Telephone number of the contact person responsible for the Cooperation Agreement	*<The telephone number of the contact person of the organisation named above who is responsible for the legal aspects of the contract between the above mentioned organisation and the EMVO>*
6. Name of the Single Point of Contact (SPOC)	*<The name of the Singe Point Of Contact of the organisation named above. This person is responsible for the technical connection between the system to be connected and the EU Hub>*
7. Email address of the SPOC	*<The email address of the Singe Point Of Contact of the organisation named above>*
8. Telephone number of the SPOC	*<The telephone number of the Singe Point Of Contact of the organisation named above>*
9. Hours of availability of the SPOC	*<Hours of availability of the SPOC according CET-time zone (e.g. 9.00 to 17.00 CET>*

C1- Information of Client 1 to be connected to the EU Hub	
1. Name NMVS	*<The name of NMVS for which a connection to the EU Hub is requested>*
2. Connection technology	☒ JAVA ☐ .Net *<Please tick one box only to select the computer language used to develop the interface to the EU Hub is requested>*
3. Name of the IT service provider of the NMVS	*The name of the IT service provider who developed and maintains the NMVS. This can be one of the Blueprint suppliers or another IT service provider (for Non-Blueprint systems)>*
4. Current status of validation of NMVS which will connect to the EU Hub	☐Validated ☐Non-validated *<Please tick the applicable box only. Note: only for informational purposes>*
5. Planned connection date to EMVO IQE	*<Please provide the date you plan to connect your NMVS IQE to EMVO IQE>*
6. Planned connection date to EMVO PRD	*<Please provide the date you plan to connect your NMVS PRD to EMVO PRD>*

D - Signature box of the NMVO requesting connection to the EU-Hub		
Signature of the contact person responsible for the legal aspects of the contract between EMVO and the NMVO	*Signature*	*Date*
Approver statement: By signing this record I hereby confirm that the information as described above is factually correct and the received information has been understood. Belgian law applies and the courts of Brussels are competent.		
Signature of the SPOC	*Signature*	*Date*
Approver statement: By signing this record I hereby confirm that the information as described above is factually correct and the received Information has been understood.		

E - Signature box of EMVO to sign off the NMVS Connection Request Form for Approval		
Signature of the authorized person of EMVO		*Date*
Remarks:		

8 Contact and Support

In case of questions, the following information is available:

1. Frequently Asked Questions (FAQ) on the EMVO website
2. Frequently Asked Questions (FAQ) of European Commission
3. EMVO-helpdesk: helpdesk@emvo-medicines.eu

Published by

EMVO asbl, Rue de la Loi 28, box 21, B-1040 Bruxelles, Belgium ©

***** Document ends *****