NMVO On-boarding Guide

Revision History

Version Date	Version	Reason For Changes
22-OCT-2017	1.0	Initial document + update to allow UAT against the EU Hub IQE environment
25-OCT-2022	2.0	Update for Operational Phase and Periodic Review

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

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 taken to achieve this goal is to mandate pharmaceutical companies and parallel distributors of prescription medicines to apply safety features to the outer packaging.

Falsified Medicines Directive

Following adoption by the Council and the European Parliament, the Falsified Medicines Directive (Directive 2011/62/EU) was published on 1st 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.

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), 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. The Delegated Regulation (EU) 2016/161 was amended by the Commission Delegated Regulation (EU) 2022/315 of 17 December 2021 as regards the derogation from the obligation of wholesalers to decommission the unique identifier of medicinal products exported to the United Kingdom.

[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 decided to apply the Delegated Regulation (EU) 2016/161 as of the 9th of February 2019.

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), the Delegated Regulation (EU) 2016/161 and its subsequent amendments 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), Affordable Medicines Europe (representing Europe's licensed parallel distribution industry), HOPE (European Hospital and Healthcare Federation) and EAHP (European Association of Hospital Pharmacists).

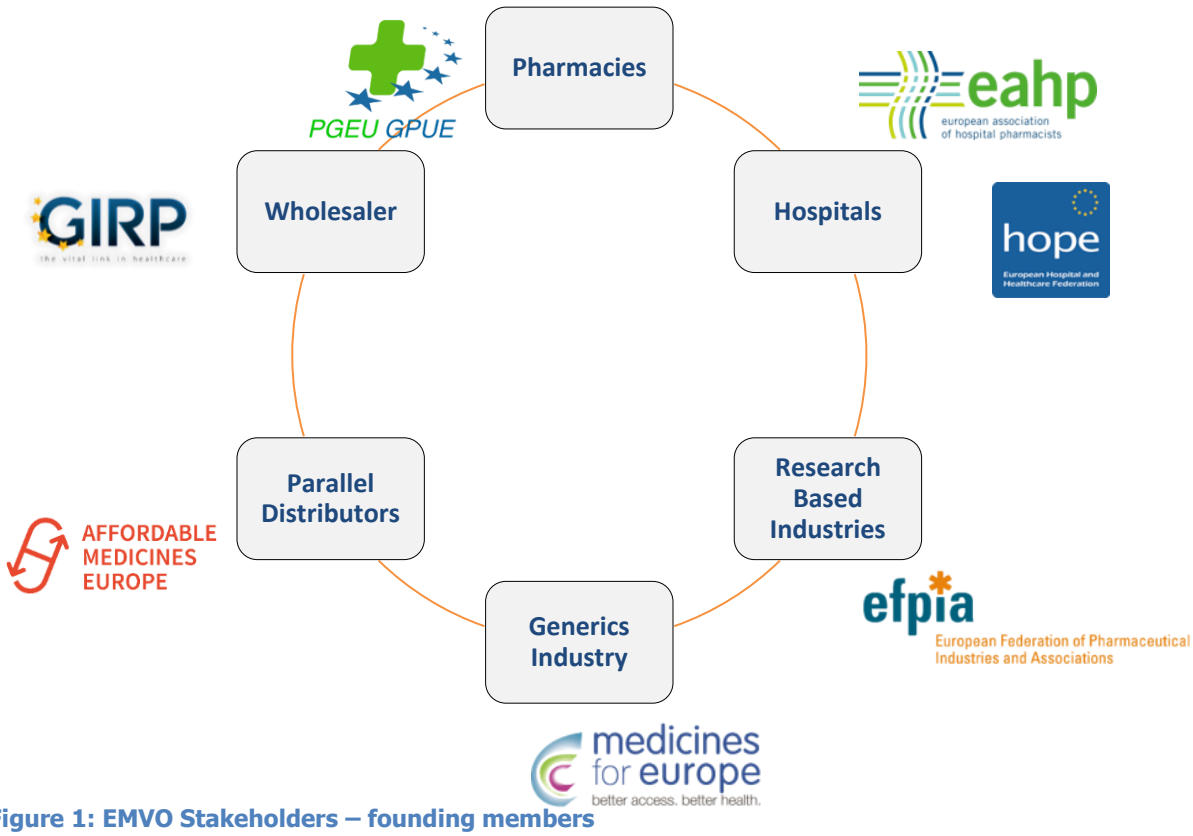

Figure 1: EMVO Stakeholders – founding members

Figure 1a: EMVO Stakeholders – founding members

Figure 1b: EMVO Stakeholders – affiliated members

EMVO set up a pan-European infrastructure of repositories centered on the "European Hub (EU Hub)" which is currently operational. The following system landscape was selected to ensure effective protection of patient safety and to allow the fulfilment of specific requirements in different countries:

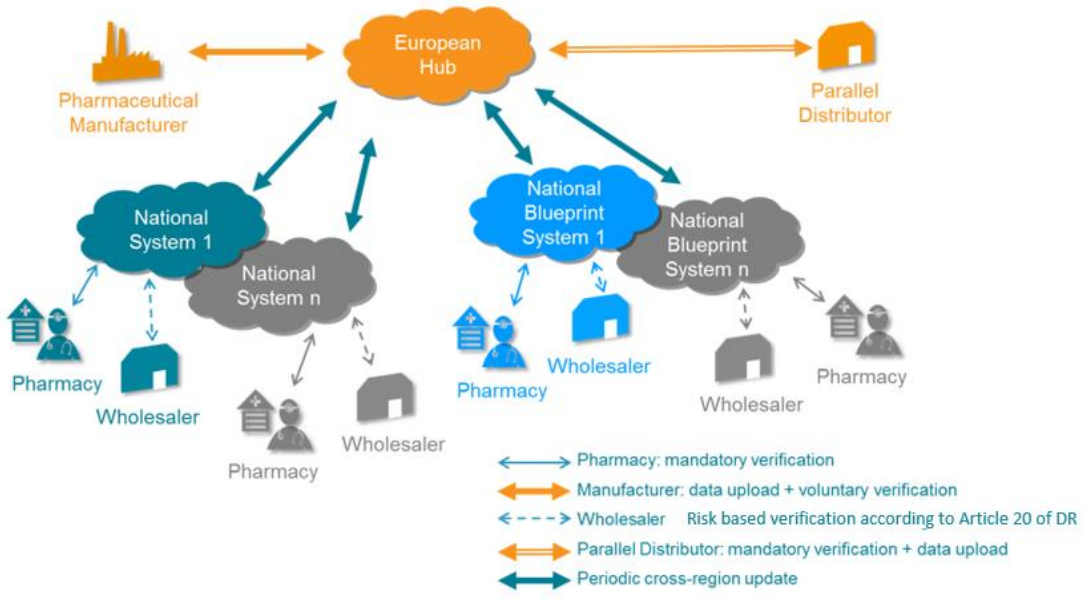

Figure 2: European Medicines Verification Landscape

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

European Hub (EU Hub)

The EU Hub is the central element of the European Medicines Verification System (EMVS).

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. EMVO has robust processes to ensure that each party connecting to the EU Hub has been verified and validated as a genuine connecting partner with valid reasons for injecting data into 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 (Original Pack Manufacturers) 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 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 (Original Pack Manufacturers) 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.

National Medicines Verification Systems

The National Medicines Verification Systems (NMVS) have been 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 relevant product serialization data for this market.
- Receiving revised/new product serialization 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 for wholesalers to verify and decommission packs, 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'.

EU CCB

The mission of the EU CCB is to:

- Ensure solid management of changes to the EMVS.
- Efficient alignment amongst the involved parties as well as firm control over the documentation always within the limits of the EU CCB Terms or Reference.
- The main objective of the EU CCB is to achieve and maintain system stabilization and reduction of false (technical) alerts.
- All Requests for Change and Release Requests to the EMVS (Hub and NMVS) must be introduced to, discussed and approved by the EU CCB before implementation and managed according to the EMVS Change Management Process – General *EMVO-01462* Standard Operating Procedure.

The EU CCB brings the following Customer Groups together to govern new changes and approve deployments of new releases. Each Customer Group represents NMVOs which use the same Blueprint system within the EMVS. Currently, the following Customer Groups exist:

1. EMVO CG for the EU Hub
2. Arvato Customer Group for all National Systems using the Arvato Blueprint system
3. Solidsoft Customer Group for all National Systems using the Solidsoft Blueprint system

The InterOperability Tests are performed under the umbrella of the EU CCB, which assigns the skilled resources for the test activities on the interoperability tests.

When a National System based on the EMVO Blueprint, developed by a new IT Service Provider is to be connected to the EMVS, a new Customer Group is to be established.

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 assessment of processes, 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.

On-boarding process of an NMVO

Introduction to the on-boarding process

This NMVO on-boarding guide will focus on the sign off of a contract between the NMVO and the EMVO, the Process Assessment and the Technical on-boarding. In figure 3 below this approach is visualized with the dark-blue arrows.

When the technical on-boarding ended (this is when the NMVS is connected to the productive EU Hub environment), the system is technical live (PRD Live). As of then, the End-Users are on-boarded by the NMVO during the Ramp-up in line with the defined End-User on-boarding process.
When a high degree of confidence has been established in the End User on-boarding process, different End Users may on-board in parallel and then the phase Business As Usual (BAU) starts.

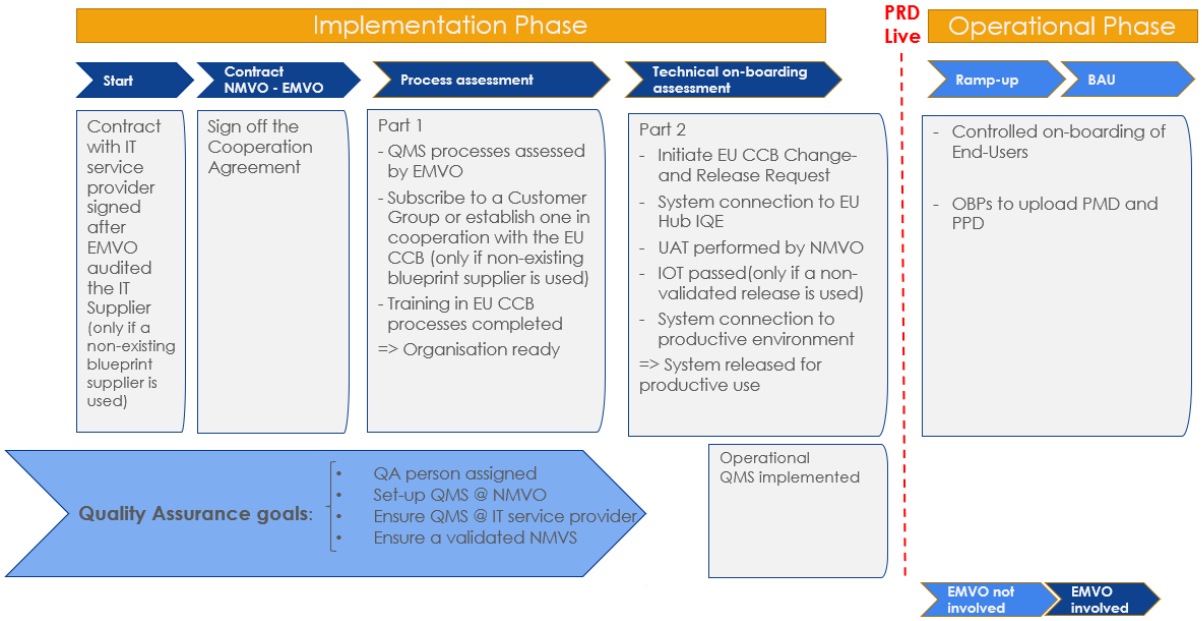

Figure 3: on-boarding process steps

National prerequisites

A National Medicines Verification System (**NMVS**) must be set up and managed by a non-profit legal entity (National Medicines Verification Organisation – **NMVO**) established by national stakeholders in accordance with Article 31 of the Delegated Regulation ("DR")

The establishment of the NMVO requires **alignment** between all national stakeholders, the creation of **Articles of Association** and communication to the relevant **competent authority(ies)** etc. as per Article 37 of the DR.

For an NMVO to connect its NMVS to the EU Hub, the NMVO and the NMVO's Affiliate (in case of a two-tier structure) that agrees to be bound jointly and severally with the (main) NMVO) needs to enter into the **Cooperation Agreement for the Operation of the EMVS with EMVO**.

Contract: EMVO-NMVO Cooperation Agreement

Before an NMVO can on-board and connect its NMVS to the EU Hub, a Cooperation Agreement has to be signed between EMVO and the NMVO. The Cooperation Agreement template can be obtained from EMVO upon request. An NMVO is entitled to enter into the Cooperation Agreement with EMVO provided it meets the requirements set out under Article 31 of the Delegated Regulation (EU) 2016/161.

The NMVO will also have to have a contract in place with an EMVO-approved IT service provider which ensures the development of the NMVS as well as future maintenance.

Negotiate & sign off the EMVO-NMVO Cooperation Agreement

This Cooperation Agreement sets the contractual framework for the cooperation between EMVO and the NMVO. Note that in case of a national two-tier structure, both NMVO related entities need to enter into the Cooperation Agreement with EMVO and be bound by its provisions and obligations.

This Agreement sets the parties' respective rights and obligations in relation to the operation of the EMVS, the connection between the EU Hub and the NMVS, and the use of the EU Hub and NMVS to transfer data between them.

More specifically, the purpose of the Agreement is:

Cooperation between EMVO and the NMVO - including the mutual grant of rights that are necessary for:

- the operation and testing, where necessary, of the EMVS
- the connection between a NMVS and the EU Hub
- their use to transfer Data between the EU Hub and the NMVS

to enable the operation of the EMVS in order to allow End Users to verify the authenticity of medicinal products and the other use cases as set out in the EU Directive on Falsified Medicines and its Delegated Regulation and the EMVS URS.

Protection of the system's 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 Software Development Kit ("SDK"). The SDK and other confidential information is to be provided and used only under the conditions set out in the Cooperation Agreement. Each party has the right to disconnect a NMVS from the EU Hub in concrete cases such as in case the NMVS immediately or substantially endangers the security or functioning of the EMVS in whole or in part. Legitimacy checks and other controls are to be implemented for all system users in accordance with Falsified Medicines Directive (FMD) and Delegated Regulation.

Process assessment

Before the process assessment can take place, the Cooperation Agreement has to be concluded between the NMVO and EMVO.

The NMVO's capability will be assessed by EMVO. Part one of the assessment will ensure that:

- The NMVO processes and their capability to ensure that the minimum quality expectations are met for the following topics:
    - Financial stability
    - Information security management;
    - Roles and responsibilities;
    - End-user legitimacy check;
    - End-user On-boarding process;
    - Access management;
    - Incident management;
    - Change management.
- The NMVO is familiar with the EU CCB processes
    - The NMVO is subscribed to a Customer Group. This means that the NMVO either subscribes to an existing Customer Group or establishes a Customer Group in cooperation with the EU CCB. The latter is required if a non-existing IT Provider is used for the development of the NMVS. Also, the NMVO staff is to be adequately trained in the EU CCB processes
- 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 authorised 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.

Technical on-boarding

Before the technical on-boarding can start, the IT service provider develops and tests the NMVS against an EU Hub environment that is provided by Solidsoft Reply to the IT 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 EU Hub IQE environment.

During the technical on-boarding, the NMVS (NS IQE) will be connected to the EMVO controlled IQE test environment (EU Hub IQE). With these environments connected, the NMVO will perform a UAT of their NMVS to ensure that the system as supplied by the IT system provider meets the requirements of the NMVO.

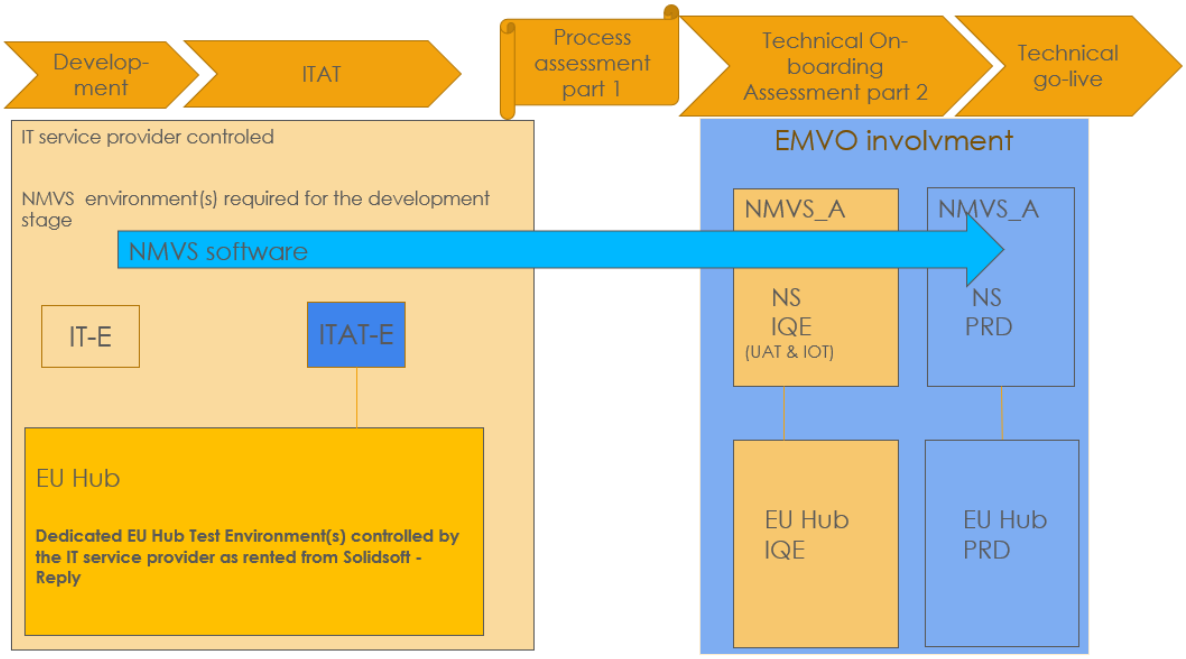

Figure 4: NMVS: from development to technical go-live

System connection to IQE test environment

- The technical on-boarding process will be triggered by the NMVO in its role as System owner by requesting the EMVO Helpdesk the technical onboarding. This is performed by submitting the EU CCB approved Release Request and approved applicable Change Requests to EMVO.
- The EMVO Helpdesk will now issue an 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 an OBP Portal with CP Number and Organization ID for the EU Hub IQE environment. The NMVO (or its IT service provider) will now create a Certificate Signing Request-file or CSR-file following the documentation available in the OBP Portal

and upload this to the OBP Portal. With this information and the session token available at the OBP Portal, the IT service provider of the NMVS can supply access to the EU Hub IQE environment of the EMVO controlled EU Hub.

User Acceptance Test

The NMVO will perform a UAT for its NMVS to ensure that the system will meet the requirements as defined in the EMVS-URS as issued by EMVO as well as local requirements (if applicable).

This UAT will be performed by the NMVO within the NMVS IQE environment which is connected to the EU Hub IQE environment.

To plan the UAT, the NMVO will send an email to helpdesk@emvo-medicines.eu to request the UAT. 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 EMVO to check for resource availability.

A UAT-test report together with an 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 assessment part 2.

When the NMVO passed the assessment part 2, the NMVO can connect its productive NMVS (NS PRD) to the productive EU Hub environment (EU Hub PRD).

If the NMVS is not developed by an existing IT Service provider supplier or the release which is implemented is not already in productive use within the EMVS, the NMVO need to request for an IOT to the EU CCB. This IOT is to be planned in a slot which is determined by the EU CCB. When the IOT is executed successfully, and the EU CCB decides that the NMVS can be connected, the on-boarding process can be continued.

In Figure 4 above, the full NMVS software deployment process is visualized. Please note that EMVO is only involved in the EU Hub environments (EU Hub IQE and EU Hub PRD) in the blue background (marked with 'EMVO-involvement'). The IOT is not pictured in Figure 4.

As per Cooperation Agreement, the NMVO will support all 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.

System connection to productive environment

The NMVO (or its IT service provider) will create a Certificate Signing Request-file or CSR-file and upload this to the OBP Portal. With this information and the session token available at the OBP Portal, the IT service provider of the NMVS can provide access to the productive environment of the EMVO controlled EU Hub (EU Hub PRD). For more details on the steps in the OBP Portal, please consult the NMVO On-Boarding Presentation (EMVO-00112).

Quality Assurance goals

As stated in chapter 1 Introduction 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. However, and taken the criticality of good Quality Management processes, EMVO will evaluate the Quality Management System as a prerequisite for the on-boarding to the EU Hub and thus allow the NMVO to start its connection to the EU Hub PRD environment.

We distinguish 4 main Quality Assurance goals for NMVOs. These are:

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

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

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.

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 where e.g. also national regulatory requirements are taken into account.

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.

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.

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, meets the requirements of the Cooperation Agreement and meets 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.

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. The report and NMVO responses with defined CAPA's are then delivered to EMVO.

As per Cooperation Agreement, the NMVO will support the audits and assessments with all reasonably necessary support including availability of the NMVO Staff. 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.

System operation

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

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 latest version of the following applicable regulation & best practices will be considered during the audit:

- The Cooperation Agreement
- Directive 2011/62/EU and Delegated Act;
- GAMP5, A Risk-Based Approach to Compliant GxP Computerized Syst. ;
- Applicable sections of Eudralex Volume 4 and applicable Annexes;
- ISO/IEC 27001: Information security management systems;
- ISO/IEC 27002: Code of practice for information security management;

Definitions

Definition	Description
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.

EU CCB	The governing body of all Change and Fix requests within the EMVS. All Requests are analysed by the EU IT Team and reviewed by the EU QA team. The EU CCB Representatives approve or reject Requests. The EU CCB also aligns on other topics like e.g. the EMVS Roadmap
Implementation Phase	NMVS project phase during which the NMVS onboarding is executed
IT service providers	The NMVOs' supplier responsible for the development, technical structure and maintenance of the NMVS, which builds on the legal and IT architecture deployed by EMVO.
Operational Phase	NMVS project phase during which the NMVS is connected to the Productive EU Hub
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.

List of Abbreviations

AME	Affordable Medicines Europe
CAPA	Corrective Actions, Preventive Actions
CER	Certificate
CSR	Certificate Signing Request
DR	Delegated Regulation
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
M4E	Medicines for Europe
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

Reference Documents

Reference to latest version	Title
EMVO-00112	NMVO on-boarding presentation
EMVO-00298	EMVO-NMVOs Cooperation Agreement for the Operation of the EMVS
Eudralex Volume 4,	EU Guidelines to Good Manufacturing Practice- Medicinal Products for Human and Veterinary use
GAMP5	A Risk-Based Approach to Compliant GxP Computerized Systems
ISO/IEC 27001	Information Security Management Systems
ISO/IEC 27002	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

Appendix

Appendix: 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	
Name NMVS	*<The name of NMVS for which a connection to the EU Hub is requested>*
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>*
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 existing IT Service Providers or another IT service provider (for Non-Blueprint systems)>*
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>*
Planned connection date to EU Hub IQE	*<Please provide the date you plan to connect your NMVS IQE to EU Hub IQE>*
Planned connection date to EU Hub PRD	*<Please provide the date you plan to connect your NMVS PRD to EU Hub 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:		

Contact and Support

In case of questions, the following information is available:

EMVO Knowledge Database on the EMVO website

EMVO-helpdesk: helpdesk@emvo-medicines.eu

Published by

EMVO asbl, Rue du Commerce 123, box 2, B-1000 Bruxelles, Belgium ©