20 September 2018

AIDE MEMOIRE FOR INSPECTION

Member State Supervision of the National Medicines Verification System (NMVS)/National Medicines Verification Organisation (NMVO)

Explanatory Note:

The supervision activities may involve on-site based inspections at the premises of the NMVO/NMVS and/or remote desk-top based inspections. Inspection reports should clearly indicate whether the inspection was on-site or remote.

The inspection frequency will be risk based taking a number of criteria into account, e.g. time period since establishment (i.e. more frequent inspections may occur initially), whether the previous inspection was on-site or remote, compliance rating following inspection, complexity of the organisation/repository (i.e. national vs. supranational), following the notification of compliance or other issues from EU Member States or from stakeholders etc.

Certain aspects of this aide memoire may be applicable to the initial inspections only. The intent is to provide a comprehensive document with particular focus on the initial inspections.

Area of Operations/Items	**Provide Answer/Explain**	**Delegated Regulation (DR) Article(s)**
NMVO	Organisation • Organogram/Structure • Members • Board of Directors • Roles & Responsibilities • NMVS Service Provider • Funding	Art 31.1 & Arts 31.3 - 31.5 & Art 35.1 (b)
Obligations of NMVO	Is the repository physically located in the Union?	Art 35.1 (a)
	Is the repository a 'national' or a 'supranational 'repository?	Art 32.1 (b)
	Has the NCA been informed when the repository became fully operational?	Art 37 (a)
	Where are the servers for the repository physically located?	Preamble (41) & Article 35.1 (a)
	Is an audit trail available to the NCA upon request – complete record of all operations concerning a UI, including the users performing those operations and the nature of the operations?	Preamble (36) & Art 35.1 (g) & Art 37 (f)
	Are reports available to the NCAs upon request, to enable the following: • Verification of compliance of stakeholders with the DR • Investigation of potential incidents of falsification	Art 36 (j) & Art 37 (g)
NMVS	Is the system a blueprint, a customised blueprint or bespoke system?	

	Blueprint: Configured system Customised Blueprint and Bespoke: Bespoke system	
	Contract between NMVO & NMVS Service Provider	
	NMVS Service Provider - Supplier Assessment	
	Was a Pilot carried out prior to the go-live date? Were the learnings from the Pilot followed through to satisfactory completion?	
	System Description (detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures). IT Infrastructure (i.e. the hardware and software such as networking software and operation systems, which makes it possible for the application to function)	
	System Interfaces:- • Description – how the systems interact, what they each provide and what they require? • Interface(s) with users, Interface(s) with other systems (how is data exchanged, provided, used?) • Security of the Interfaces	
	Qualification/Validation • Qualification Plan/Validation Plan • Risk Assessments • Specifications:- User Requirement Specification, Requirements Traceability, Functional Specification, Configuration Specification, Software Module Specification, Interface Specifications including expectation of the User system interface. • Testing/Verification Roles & Responsibilities Test Strategy/Plan, Execution, Reporting Supplier Test Activities Automated Testing Installation Testing Software Module Testing, Software Integration Testing, Configuration Testing, Functional testing, Requirements Testing, Interface Testing, Business Process Testing, Data Integrity Testing, Regression Testing.	
	Connection to EU Hub • Contracts/Agreements between NMVO & EMVO • System connection acceptance testing	
	Connection of End User IT Software Providers to NMVS • Contracts/Agreements • System connection acceptance testing	

Registration/Connection of Stakeholders to NMVS	Listing of registered/connected entities:- • MAH's • Wholesalers • Pharmacies • Hospitals (ID, Name, Address, Stakeholder Type, Operations Permitted)	
	Security Procedures –registration/connection of stakeholders	Art 37 (b)
	Contracts/Agreements	
	Bona Fide/Legitimacy Checks/Records	
Quality System	Quality Manual/Controlled Document Listing	
Change Management	Process/procedure for managing changes List of changes executed How are front end and back end changes controlled?	
CAPA Management	Process/procedure for handling CAPAs	
Complaint Management	Process/procedure for complaint handling List of complaints received	
Quality Risk Management	Process/Procedure/ Life Cycle Approach List of risk assessments conducted/Register	
Information Security Management	Process/Procedure	
	Has an IT security audit of the system been conducted?	
System Access Management	Process/Procedure How is Front End and Back End Access controlled?	
Training	Process/Procedure/Records	
Business Continuity	Risk Assessment Process/Procedure Is there an alternative system? Has it been tested/qualified? How is Database size/growth managed? How is system performance managed? How is system interruption mitigated? How does this impact the User's System?	
Audit Management	Process/Procedure for audit of NMVS	
	Are regular audits of the repository carried out to verify compliance with the DR? (At least annually for first 5 years and at least every 3 years thereafter)	Art 37 (e)
	Are audit reports available to the NCA upon request?	Art 37 (e)
Management of Incidents/Potential Incidents of Falsification	Process/Procedure for managing incidents List of incidents raised	
	Is the repository continuously monitored for events alerting to potential incidents of falsification? Who gets notified? How/by what means?	Art 37 (c)

	Is there a provision for immediate investigation of all potential incidents of falsification flagged in the system?	Art 37 (d)
	Is there a provision for the alerting of the NCA(s), EMA & Commission of confirmed incidents of falsification?	Art 37 (d)
	What alert is triggered in the system in case of a verification failure to verify that a UI is authentic? (*exception: where the product is indicated in the system as Recalled, Withdrawn or intended for Destruction*)	Art 36 (b)
	How is this event flagged in the system, e.g. push alert to NMVO, pull alert through reporting, etc.?	Art 36 (b)
	Can any information on a given UI immediately be provided to the NCA/EMA upon request?	Art 36 (i)
Data Upload	Is the following data stored in the repository system after upload and is it accessible to all parties required to verify the authenticity of products? (a) data elements of the UI (product code; serial number; national reimbursement number, if required; batch number; expiry date (b) coding scheme of the product code (c) name & common name of the product, pharmaceutical form, strength, pack type, pack size (d) Member state(s) where the product is intended to be placed on the market (e) code identifying the entry corresponding to the product in the EMA database, where applicable (f) name & address of the manufacturer placing the safety features (g) name & address of the MAH (h) list of wholesalers designated by the MAH, to store and distribute the product on its behalf	Preamble (38) & Art 33.2
	Is the data upload performed through the EU Hub or through the national/supranational repository? If data upload is through the national/supranational repository, is a copy of the information referred to in (a) – (d) above, with the exception of the serial number, immediately transferred to the EU Hub?	Art 33.3
	Is the uploaded data referred to above stored in the repository for at least one year after expiry or five years after release, whichever is the longer period?	Art 33.4
	How is data securely removed and deleted/archived?	
Data Protection & Confidentiality	How is the following guaranteed:- • the protection of personal data? • the protection of information of a commercially confidential nature? • the ownership and confidentiality of the data generated when users interact with it?	Art 35.1 (h)
	How is ensured that users only have access to data it generated when interacting with the repository system?	Art 38.1

	(*Exception: master data information as per Art 33.2 & information on status of a UI*)	
	Is the audit trail and the data contained therein only accessed by the NMVO following written agreement of the legitimate data owners? (*Exception: for the purpose of investigation of potential incidents of falsification flagged in the system*)	Art 38.2
Characteristics of the Repository	Is the repository fully interoperable with the other repositories?	Art 35.1 (c)
	Are Application Programming Interfaces (APIs) available allowing transfer and exchange of data with the software used by wholesalers, pharmacies and hospitals?	Art 32.4 & Art 35.1 (e)
	Are Application Programming Interfaces (APIs) available allowing NCAs to access the repositories system by means of software, in accordance with Article 39.	Art 32.4 & Art 35.1 (e)
	Is the response time of the repository lower than 300 milliseconds in the case of a query for the purposes of verification & decommissioning (in at least 95% of queries)?	Art 35.1 (f)
	Is the audit trail maintained until at least one year after expiry date or 5 years after released for sale, whichever is the longer period?	Art 35.1 (g)
	Are Graphical User Interfaces (GUIs) available providing direct access for wholesalers and pharmacies/hospitals for the purpose of manual verification & decommissioning in the case of failure of their own software?	Art 32.4 & Art 35.1 (i) (i) & Art 36 (h)
	Are Graphical User Interfaces (GUIs) available providing direct access for NCAs for the purposes of supervision of the functioning of the repository, investigation of potential incidents of falsification, reimbursement, pharmacovigilance or pharmacoepidemiology?	Art 35.1 (i) (ii) & Art 39
	Is the change in status of a UI for a multi-market pack immediately notified to the EU Hub? (*Exception: decommissioning by MAH related to products recalled, withdrawn, stolen, supplied as free samples*)	Art 35.2
	How is the upload of a UI with the same product code and serial number prevented?	Preamble (39) & Art 35.3
Operations of the Repository	Can the authenticity of a UI be repeatedly verified?	Art 36 (a)
	Can the verification and decommissioning of a UI be performed in one combined operation?	Art 36 (d)
	Can a UI be identified, verified and decommissioned in another Member State to the one where the pack was placed on the market?	Art 36 (e)
	Can a wholesaler access the list of designated wholesalers uploaded in the Master Data to confirm whether it is required to verify the authenticity of the UI of a given product? How is this access achieved?	Art 36 (g)

	Are reports available/can reports be generated that allow NCAs to verify: • compliance of individual MAHs, manufacturers, wholesalers, parallel importers, parallel distributors and persons authorised or entitled to supply medicinal products to the public (e.g. pharmacies and hospitals) • to investigate potential incidents of falsification • to supervise the functioning of the repositories • pharmacovigilance/pharmacoepidemiology (if required by the NCA) • reimbursement (if required by the NCA)	Art 36 (j) and Art 39
	How is it indicated to a user that a UI has been decommissioned?	Art. 36 (l)
	How is it indicated that a product has been:- • recalled • withdrawn • stolen • exported • requested as a sample by NCA • indicated as a free sample by the MAH • intended for destruction	Art. 36 (m)
	How does the repository provide for the linking, by batches of medicinal products, of the information on UIs removed or covered to the information on the equivalent UIs placed on those medicinal products?	Art. 36 (n)
	How is the synchronisation of the status of a UI between the repositories serving the territory of the Member States where the product is intended to be placed on the market ensured?	Art. 36 (o)