Alert Management Procedure

Contents

1. Purpose

The objective of this document is to establish the standard operating procedures for handling alerts generated in the Belgian and Luxembourg NMVS. It sets out decision trees for investigation of alerts and the point at which FAGG-AFMPS (Belgian NCA) or DPM (Luxembourg NCA) must be notified. It also defines the role of end-users, MAHs, and BeMVO and describes communication channels between them, including the NMVSAlerts platform and EAMS.

Data ownership and access to data

These procedures are aligned with the requirements of the Delegated Regulation and the governing principles for the EMVS, as set out in EMVS URS, relating to data ownership and access, where the basic principle is that the anonymity of the end-user is protected vis-à-vis the MAH. Current and future end-user anonymity will remain the same, as has been the case since the EMVS was established.

Please see section 6 (Glossary) for an explanation of abbreviations and terms used in this document, e.g., MAH, Delegated Regulation, etc.

2. Scope

2.1 Audience

These standard operating procedures need to be followed by Belgian and Luxembourg pharmacists, wholesalers, MAHs, and BeMVO who should have in place procedures that enable them to comply with their respective responsibilities in relation to alerts generated in the Belgian and Luxembourg NMVS.

2.2 Alerts

These procedures apply to Level 5 alerts that generate an Alert ID in the NMVS. Appendix 2 sets out the different categories of alerts that need to be investigated.

2.3 Out of scope

NCA investigation of alerts

The process by which FAGG-AFMPS or DPM investigates suspected falsifications reported to them is out of scope of this guidance.

Anti-tampering device (ATD)

The process of verifying ATDs is out of scope of these procedures and where the ATD is missing, damaged or appears to have been interfered with, relevant national procedures should be followed, including notification to the NCA as appropriate.

Damaged packs which cannot be authenticated

Where the packaging of a medicinal product is damaged to the extent that the barcode cannot be scanned and the human readable data cannot be read (to verify by way of manual entry), the pack must not be supplied to the public or returned to saleable stock. The relevant national procedure for product quality complaints should be followed, including notification to the NCA as appropriate.

3. Procedure Content

3.1 Introduction

The generation of an alert in the NMVS represents a potential suspected falsified pack because the NMVS can never determine the falsified status of the pack with absolute certainty. Each alert type that indicates a potential suspected falsification (see Appendix 2) may have several possible root causes and the pack may not actually be falsified. An alert must be investigated by the relevant parties to rule out technical or procedural root causes, such as issues with the NMVS or EMVS, data upload, data quality, incorrect end-user scanning or other similar technical issues. When all such root causes are ruled out, it is then considered a suspected falsification and reported to the NCA.

An alert investigation comprises a series of steps designed to systematically assess and rule out possible root causes (by way of decision trees) until the actual root cause is identified. The parties involved in the investigation will vary depending on the type of alert and how it was generated (end-user vs. MAH transaction).

Article 37(d) of the Delegated Regulation requires the legal entities operating the repositories systems, i.e., EMVO and the NMVO, to provide for the investigation of all potential falsifications. Under this principle, BeMVO will assign different tasks and responsibilities on investigation of alerts to end-users and MAHs as described in this document.

Section 3.2 describes how communications about alerts will be managed, including the role of the NMVS Alerts platform and EAMS.

Section 3.3 describes the process for investigation of alerts by end-users – pharmacies, hospitals, wholesalers and other persons authorised or entitled to supply medicines to the public.

Section 3.4 describes variations to the processes in section 3.3 for wholesalers specifically.

Section 3.5 describes the process that MAHs follow in investigating alerts. **Section 3.6**

describes specific considerations that apply to parallel distributors. **Section 3.7**

describes the additional considerations that apply to IMT alerts.

Sections 3.8 and **3.9** describe the role of BeMVO and EMVO respectively.

3.2 Communications about alerts

Alert management system

End-users, MAHs, BeMVO and EMVO should communicate with each other about alerts via the NMVS Alerts platform or EAMS.

This:

- Facilitates prompt and direct communication between different parties (MAH, NMVO, and end-user) involved in an alert investigation;
- Provides each party with visibility over investigations being carried out simultaneously;
- Preserves end-user anonymity vis-à-vis the MAH;
- Provides for consistent and thorough documentation of alert investigations and resolutions;
- Provides the opportunity for the NCA to be alerted about suspected falsified packs in a timely manner.

In the event of a highly suspicious alert or where there is no alternative pack available for a patient and where speedier feedback is required, BeMVO may need to contact end-users and/or MAHs by phone (and vice versa).

An end-user may decide themselves to contact the MAH (by phone or email) about an alert but there is no obligation or expectation that they should do so. Where an MAH has been contacted by an end-user, the MAH may reply directly to the end-user, rather than using the NMVO as an intermediary.

3.3 Process for end-users

This section and Figure 1 describe the process to be followed by an end-user when a Level 5 alert is generated at their location. Variations to this process for wholesalers are described separately in section 3.4.

Unsuccessful verifications of unique identifiers that generate an exception but not a Level 5 alert are out of scope of this process. Examples include but are not limited to:

- verification of a pack where the pack is not in the expected state, for example, pack scans as ‘supplied’ when verified prior to being dispensed;
- scanning a linear barcode or QR code;
- scanning a 2D data matrix on a medical device;
- scanning an ‘Indian pack’ or other pack of a medicinal product placed on the market prior to 9th February 2019 where the product code is not recognized in the NMVS;
- scanning a pack that has expired or is marked as recalled or withdrawn in the NMVS;
- message that NMVS is unavailable.

These exceptions should be checked by the end-user; the action to be taken will vary depending on the issue.

In the case of an alert generated at an end-user location, the alert investigation should be initiated by the end-user to determine if they have caused the alert.

Overview of end-user investigation of an alert

The level of detail the end-user receives about the alert will depend on how their end-user software has been implemented; at a minimum, they will be aware that the pack has not been successfully verified and/or decommissioned and that an alert has been generated.

Alerts confirmed to have been generated by end-users will be closed in the NMVS Alerts platform (and as a consequence also in EAMS) by BeMVO if the investigation was completed and the cause of the alert was identified as a technical or procedural error on the part of the end-user.

- End-user confirmed to have investigated the alert
- End user confirmed the cause of the alert is on his side
- End-user has indicated that it is an alert caused by a technical issue or procedure error
- End-user has confirmed that the pack is genuine. (in comment field)

Where possible, the root cause of the alert should be corrected, and the pack should be verified again. After successful verification (meaning the verification provides that the UI is active), the pack may be returned to saleable stock[1]. In the case of a pharmacy, hospital or other person authorised or entitled to supply medicines to the public, this means that the pack may now be supplied to the public.

If it is not possible to 'correct' the cause of the alert, for example, where the error arose due to a procedural error such as double decommissioning a pack and it is not possible to reverse it, the investigation and finding should be documented. The pack may be supplied to the public when the pharmacist declares in the NMVS Alerts platform the appropriate checks were done and the product is genuine.

End-User-01a. Pack withheld from saleable stock

When a pack generates an alert, the pack should immediately be set aside while the alert is investigated. Repeated scanning of the pack, in the absence of any information on the root cause of the original alert and action to correct it, should be avoided as each attempt will generate further alerts unnecessarily burdening the system.

The pack may not be placed back into saleable stock until such time as it has either been confirmed as exempt from FMD requirements (see step E-01b) or the investigation is complete, and the pack is not deemed to be a suspected falsification.

[1] Note: If an alert has occurred while decommissioning a pack to take it out of the supply chain, e.g. decommissioning as destroyed, the end-user should continue with the intended action (i.e. destroying the pack) after the alert is resolved and NOT return the pack to saleable stock.

End-User-01b. Exemptions from FMD

The NCA may provide for exemptions from FMD for a product or batch[2]. Where this applies, the pack may be supplied to the public notwithstanding that an alert has been generated.

If there is no exemption from FMD, the next step is to attempt to verify the pack by manual entry of the human readable data (End-User-01c).

End-User-01c. Manual entry

Manual entry is **not** recommended in the following situations as it may lead to a further alert without offering any new information to help resolve the original alert:

i. If the **alert message relates to the pack state and suggests a procedural error**, e.g., "pack already in requested state" or similar (the information about the alert that is available to the end-user on screen or in another readily accessible format will depend on how their software is programmed); or

ii. The unique identifier **data from the barcode displayed to the end-user matches the human readable data** on the pack.

Note: If the MAH has, with the agreement of the NCA, released the product to market with a known batch-level quality defect in the barcode, such that there is a mismatch between the data in the barcode and the human readable data, the only way to successfully verify and decommission the pack is by manual entry.

If the pack is successfully verified and decommissioned after manual entry, it may be supplied to the public.

If the manual entry attempt is not successful, the end-user should check that the data entered matches what is printed on the pack and if not, then attempt to type it again correctly. If the pack has been successfully verified and decommissioned after repeating manual entry, itmay be supplied to the public. If not, then the pack must continue to be withheld from saleable stock and the investigation continues to the next stage – end-user technical error (End-User- 02a).

End-User-02a. End-user technical error

If the alert was generated as a result of scanning the barcode (rather than manual entry), the next stage is for the end-user to determine if the alert was caused by a technical error. This step is intended to be an initial check by the end-user for technical issues relating to the scanner that they may be able to quicky resolve themselves. Examples of such errors include:

- Problem with scanner settings;
- Incorrect scanner configuration that causes alerts with certain keyboard settings (y/z mismatch, caps lock on, etc.);
- Other potential issues related to scanner.

To check scanner configuration settings, the end-user may use the scanner check page published on the BeMVO website.

[2] An example of this is the MAH applying an irreversible state change in error, such as setting the status of a batch to recalled, and the NCA allows the packs to be supplied to patients to avoid a shortage.

If end-user technical error is confirmed, the scanner's keyboard settings or scanner configuration should be corrected or a different scanner used, or other action taken to fix the scanner issue to prevent further alerts being generated. The end-user's IT department or, if there is no IT department, the end-user's IT software provider or supplier of the scanner may be able to provide support for this step.

A further verification scan must be undertaken to determine if the corrective action has been successful. If the scanner is found to be working correctly (i.e., the verification confirmed that the unique identifier is active), the pack may be decommissioned and supplied to the public.

If a technical issue has been identified but cannot be quickly resolved, an attempt should be made to verify and decommission the pack by manual entry and if successful, the pack may be supplied to the public. Otherwise, the pack must continue to be withheld from saleable stock until the technical issue is resolved.

If an end-user / technical error is ruled out, the pack must continue to be withheld from saleable stock and the investigation proceeds to the next stage – end-user procedural error (End-User-02b).

End-User-02b. End-user procedural error

Procedural errors by end-users arise for various non-technical reasons, for example:

- Repeated attempts to decommission the same pack as supplied in same location beyond applicable national limits (currently an L5 alert is generated in Belgium when a product is scanned a second time for decommissioning 3 months after the first decommissioning or at the 5th scan for decommissioning);
- Attempt to decommission pack that was previously decommissioned in a different location;
- Any other procedural issue.

The information that is provided by the end-user's software when an alert is generated may, if sufficiently detailed, help to identify procedural errors. The end-user themselves may realise they made such an error, for example, accidentally decommissioning a pack more than once. In the NMVS Alerts platform the end-user will receive the information if the original decommissioning was done in his pharmacy or not.

In the case of an alert caused by attempting to decommission a pack that was previously decommissioned in a different location, BeMVO will need to be involved in the investigation as the end-user has no visibility over where the pack was previously decommissioned.

The procedural error should be documented by the end-user with the result of investigation and where the root cause has been established and there are no concerns about the authenticity of the pack, the pack may be supplied to the public. When the end-user has provided sufficient information to warrant a safe dispense BeMVO will close the alert.

If the pack is flagged in the NMVS as expired, recalled, withdrawn, intended for destruction or stolen on a repeat scan to verify that a technical issue has been resolved, it must not be supplied in any circumstances[3].

[3] The only exception to this is where the NCA has granted an exemption that permit a pack to be supplied notwithstanding that it is already irreversibly set to one of these states (see End-01b Exemptions from FMD).

If procedural error has been ruled out or cannot be identified, the pack must continue to be withheld from saleable stock and the investigation continues to the next stage – IT investigation (End-User-02c).

End-User-02c. IT investigation

This step is intended to be a check by the end-user for software or other IT issues that they cannot diagnose or resolve themselves. The end-user's IT software provider or IT department (where applicable) should be contacted by the end-user to check if there is a problem with the end-user software or other IT issue and to assist with resolving it.

A further verification scan should be undertaken to determine if the corrective action has been successful. If the software is now working, the pack may be decommissioned and supplied to the public.

If an IT issue has been identified but cannot be quickly resolved, an attempt should be made to verify and decommission the pack by manual entry and if successful, the pack may be supplied to the public. Otherwise, the pack must continue to be withheld from saleable stock until the IT issue is resolved.

If an IT issue is ruled out, the pack continues to be withheld from saleable stock to await the outcome of the MAH's investigation (End-User-03).

End-User-03. Await feedback on MAH investigation

Where the MAH's investigation of the alert, in accordance with the process described in section 3.5, is not completed within 2 working days [4] of the alert being generated, the MAH will provide an update to the NMVO and the end-user (via the NMVS Alerts portal) on the status of the investigation at that point.

The MAH may require a photo of the pack to assist in its investigation (see MAH-06. Request Photo of Pack step). The photo(s) supplied by the end-user should show the 2D barcode and the human readable text.

The pack must continue to be withheld from saleable stock at the end-user location until such time as:

- **End-User 04a.:** The MAH (or BeMVO[5]) indicates that the root cause for the alert has been identified and the pack is not considered to be falsified or,

- **End-User-04b.:** The MAH requests that the pack be sent back to them to carry out further investigations to establish if it be a suspected falsification. In this situation, the MAH will provide details of the process for sending back the pack. If the MAH requests the pack to be sent back via a wholesaler, the wholesaler must be notified in advance of the return by the MAH or end-user. In such instances, the return must be treated as a product quality complaint, rather than a standard business return, and therefore the pack should not be verified by the wholesaler.

In specific situations where the pack has expired or is damaged, the end-user should destroy the pack in accordance with applicable national procedures, unless they have been asked to send it back to the wholesaler or the MAH.

[4] i.e. alert is generated on day 0 (e.g. Tuesday), feedback is expected by close of business on day 2 (Thursday). Working days are defined as Monday-Friday, excluding public holidays.

Communication of alert investigation results

Where required, end-users should inform BeMVO if the alert has been caused by technical or procedural error on their part and provide assistance to the NMVO where required to resolve an alert.

End-users are not required to proactively contact the MAH if the alert has been caused by technical or procedural error on the end-user's part.
The MAH will be able to see the results of the investigation if inputted by the end-user in the NMVS Alerts platform.

3.4 Process for wholesalers

This section describes the variations to the process for end-users described in section 3.3 when an alert is generated at a **wholesaler** location. Alerts generated by wholesalers should be managed as part of their product quality complaints processes.

Communications about alert investigation results

Wholesalers will use the NMVS Alerts platform to communicate the outcome of the investigation to all relevant parties including the MAH and BeMVO.

- **Alerts caused by data uploading errors or PMD errors** – contact MAH.
- **A7/A24 alerts relating to pack state changes** –contact BeMVO who will provide assistance in investigating these alerts. When verifying returns, packs that are flagged as already decommissioned cannot be placed back into saleable stock. The party that returned the pack should be informed that it was previously decommissioned in another location and the wholesaler should return the pack to them.

If a wholesaler is contacted by a pharmacy, hospital or other party about a pack supplied to them which generated an alert when it was scanned by the pharmacy, hospital or other party, the wholesaler should:

- In the case of an **A7/A24 alert (PCK 19, PCK 22, PCK 27, PCK 06)**, investigate if the alert has arisen because of an error by the wholesaler while the pack was in their possession, e.g., pack decommissioned as supplied or destroyed in error. If the alert is not due to an error on the part of the wholesaler, BeMVO will need to take over the investigation as it alone has access to the Pack Disclosure Report which contains the information needed to identify the root cause of the alert.
- For **all other alerts**, refer the person contacting them to BeMVO for further assistance with the investigation.

[5] If BeMVO has become involved in the alert investigation – see section 3.8 for details of when this will occur.

3.5 Process for MAHs

If an MAH is acting in the capacity of a wholesaler, they should follow the process described in section 3.4. Otherwise, the MAH should follow the process described in this section and in Figure 2.

MAHs will be required to act differently depending on the alert type.

MAH-01. Determine alert type & source

An important principle underpinning alert investigation by MAHs is that the end-user anonymity is preserved[6].

A7, A24, and A68 Alerts (PCK 19, PCK 22, PCK 27, PCK 06, LOT 13)

MAHs are not required to investigate A7, A24 and A68 alerts except in the following circumstances:

a. MAH is aware they have caused the alert(s) due to repeating decommissioning transactions when packs are under their control;
b. An end-user contacts them about such an alert;
c. The NMVO contacts them about such alert(s), for example, in the case of an A7, A24 or A68 alert generated by an end-user where no end-user root cause can be identified;
d. FAGG/ BeMVO requests them to investigate such alert(s).

The reason for this approach is that A7 and A24 alerts generated by end-users will rarely be due to errors on the part of the MAH. Similarly, the vast majority of A68 alerts generated by end-users are due to end-user software or scanner issues.

In relation to a. above, the MAH can determine if they generated the alert themselves by checking the alert's Event Message. A reference to 'Market: EU' will confirm that the alert was generated via an MAH transaction in the Hub and the MAH should examine the Client ID in the Event Message to ascertain if they themselves caused the alert[7]. The other possibility is that the alerts were generated by a parallel distributor when decommissioning the MAH's packs as 'checked out' via the EU Hub prior to repackaging them, in which case the Client ID reported will be different to that of the MAH.

Once it is confirmed that the MAH has generated the A7, A24 or A68 alert(s), the MAH should proceed to the Internal Root Cause Investigation (MAH-03) step.

If BeMVO, the NCA or end-user has requested the MAH to investigate the alert (points b., c. and d.), the MAH should proceed to the Internal Root Cause Investigation (MAH-03).

[6] Except where an end-user has initiated direct contact themselves with the MAH about an alert associated with

MAH-02. MAH documents alert, no further action required

The MAH should check if an BeMVO or end-user has informed them that an A7, A24 or A68 alert is due to end-user error. If this is the case, the MAH must document the information received but is not required to take any further action.

A2, A3 and A52 Alerts (PC 02, LOT 03, LOT 12)

For A2, A3 and A52 alerts, the initial step by the MAH is to determine if the MAH themselves generated the alert.

The MAH may have generated an alert when carrying out a transaction via the EU Hub, but the root cause of the alert may lie elsewhere, e.g., if an MAH attempted to verify a pack but an alert was generated due to an issue with the Hub. Similarly, the MAH may be responsible for causing an alert, but may not have generated the alert themselves, e.g., an end-user raised an alert when decommissioning a pack due to the data not being uploaded by the MAH.

The MAH should check if an NMVO or end-user has informed them that the A2, A3 or A52 alert is due to end-user error. If this is the case, the MAH must document the informationreceived but is not required to take any further action (step MAH-02).

Unless the MAH is specifically aware that the alert is due to end-user error, the MAH should proceed to the Internal Root Cause Investigation (MAH-03) step.

All Alert Types

For all alert types where the MAH needs to carry out an investigation, the steps are as follows:

MAH-03. Internal root cause investigation

[7] The Client ID may be checked by the MAH in the OBP Portal.

The MAH should investigate whether or not the alert was caused by an MAH data or procedural error. Due to the varied nature of systems and processes in use by MAHs, each MAH will be required to develop its own procedure for performing this step. Some examples of errors that could be uncovered at this stage include:

- Incorrect Product Master Data uploaded for a product;
- Sending a pack to a market before uploading the Product Pack Data for the batch;
- Sending a pack to a market for which the wrong batch ID or expiry date has been uploaded;
- Adding a market to the Product Master Data for a batch after it has been uploaded;
- Repeated decommissioning of a pack or batch while under MAH control; MAH-

03a. MAH takes corrective action & informs BeMVO

If the MAH determines that they were the cause of the alert, the MAH should take corrective action as quickly as possible and inform BeMVO (and end-user if the end-user has contacted them directly about the alert) within 2 working days of the alert being generated. A progress report should be provided after 2 working days if the investigation is not completed at that stage.

If the MAH determines that they were not the cause of the alert, the MAH should proceed to perform an EU Hub investigation (MAH-04).

MAH-04. EU Hub investigation

The next step is for the MAH to investigate whether or not the alert was caused by an issue related to the EU Hub (e.g., system downtime during transfer of data from EU Hub to an NMVS resulting in data not reaching the NMVS even though MAH has received a 'distributed' callback). If necessary, the MAH should contact the EMVO Helpdesk for support.

MAH-04a. MAH informs BeMVO of Hub issue

If the MAH determines that the alert was caused by an issue with the EU Hub, they should inform BeMVO (and end-user if in contact with them) within 2 working days of the alert being generated.

If the MAH determines that the alert was not caused by an issue with the EU Hub, they should proceed to the MAH Requests BeMVO Support (MAH-05) step.

MAH-05. MAH requests BeMVO support

If the MAH has found that the alert was not caused by MAH procedural or data error, or an EU Hub issue, the MAH should contact BeMVO, and ask them to investigate if there is a root cause at national system level or at end-user level.

MAH-05a. BeMVO feedback

If BeMVO finds that the alert was caused by the national system or end-user issue, BeMVO will inform the MAH and the end-user.

If BeMVO cannot confirm that a national system or end-user error has occurred, BeMVO will inform the MAH and the MAH should proceed to the next stage of the investigation and request a photo of the pack (MAH-06.) step.

MAH-06. MAH requests photo of Pack

If the MAH has not previously been in contact with the end-user, and if either the MAH orthe end-user is not connected to an AMS, BeMVO can act as an intermediary to request a photo of the pack and any other relevant information needed for the investigation and send it to the MAH.

MAH-06a. MAH confirms there is no indication of falsification and informs BeMVO

If, after examining the pack photo, the MAH can confirm that there is no indication of a falsification / the data is plausible, the MAH should inform BeMVO (and the end-user if in contact with them) which allows BeMVO to close the alert. The pack may then be returned by the end-user to saleable stock.

If the MAH cannot confirm that the pack is genuine from the photo, the MAH should proceed to the Request Pack (MAH-07.) step.

MAH-07. MAH requests pack

If the MAH can confirm as a result of its analysis of the pack that it is genuine, the MAH should inform BeMVO and the end-user through EAMS or the NMVS Alerts platform as per step MAH- 06a which will allow the alert to be closed out.

If the MAH cannot confirm that the pack is genuine from the analysis of the pack (i.e., that there is no indication for a falsification or the data is plausible), the MAH should proceed to the Suspected Falsification (MAH-08) step.

MAH-08. Suspected Falsification

In the event that the MAH cannot confirm that the pack is genuine from its analysis of the actual pack, the MAH must mark the pack as ‘suspected falsification’ and immediately inform BeMVO and the NCA (and in the case of a centrally authorised product, the EMA). When the NCA or BeMVO deems it necessary (e.g., in case of a European-wide investigationof alert(s) relating to a unique identifier or batch), it may inform EMVO about the suspected falsification in order to facilitate the investigation process.

MAH Communications

In the event that an MAH chooses not to use an AMS, email or other appropriate communication method should be used. BeMVO will act as an intermediary for communications with an end-user where the MAH does not know the end-user’s identity.

Where the MAH is different to the OBP or to the manufacturer, robust internal communication procedures and technical agreements must be in place to ensure the details of alerts are communicated in a timely way between relevant parties, including the outcome of the alert investigation.

Where an MAH becomes aware of a temporary problem with a batch or part of a batch that will lead to alerts, e.g., data not uploaded, they should inform BeMVO and the designated wholesaler and give an indication of when the problem will be resolved so that scanning of the packs can resume.

3.6 Specific considerations applicable to parallel distributors

Alerts generated when unique identifiers on originator packs are scanned by parallel distributors (when verifying or 'checking out' the packs) which are due to missing or incorrect data in the EMVS require action by the originator MAH so that the packs can be authenticated before repacking operations take place.

If the parallel distributor can rule out an error on their part for alerts generated when originator packs are scanned and wishes to contact the originator MAH regarding these alerts, the process is as follows:

- Where there is no **AMS**, EMVO will provide the parallel distributor with contact details for the originator MAH.
- Where there is an **AMS**, parallel distributor and originator MAH can communicate directly with each other via the AMS.

3.7 IMT Alerts

Overview of IMT alerts

Various parties are involved in IMT alerts, in both the initiating market (country where pack is scanned) and fulfilling market (the country in whose NMVS the pack data is stored) – see Figure 3 for process.

Initiating market:

- **End-user** who has in their possession the pack that generated the alert. The end-user is connected to the NMVS in the initiating market having been onboarded by and signed end-user terms and conditions with the NMVO in that market (initiating NMVO). In terms of FMD compliance, the end-user falls under the remit of the NCA in the initiating market.
- The **NMVO** in the initiating market is responsible for ensuring that alerts generated in their market are investigated and they co-operate with the NCA in the initiating market in this regard. In the event of an IMT alert, the audit trail made available to the initiating NMVO only shows transactions on that pack in their market.

- The **NCA** in the initiating market is responsible for supervision of end-users, the NMVO and the NMVS in that market.

Fulfilling market

- The **NMVO** that operates the NMVS in the country where the product pack data was uploaded ('fulfilling NMVO') has access to the complete audit trail for the pack when an alert is generated, regardless of where it was scanned. The MAH whose pack has generated the IMT alert has signed an MAH agreement with the fulfilling NMVO asthe data for that pack is stored in their NMVS.
- The **NCA** in the fulfilling market is responsible for supervision of the NMVO and the NMVS in the fulfilling market, as well as the MAH who placed the product on the market in that country.

MAH

- The MAH of the product that caused the alert is responsible for the alert investigation even if they do not have a presence on the initiating market where the pack was scanned.

Table 1 outlines what information is provided to the relevant NMVOs and MAHs by the EMVS in relation to an IMT alert.

Table 1: Summary of IMT alert information provided to NMVOs & MAH

	Initiating NMVO (in country where pack is scanned)	**Fulfilling NMVO** (in whose system pack data is stored)	**MAH**	**Notes**
Alert details	Yes	Yes	Yes	Slight differences in details provided to each party, e.g., initiating NMVO sees if transaction that generated alert was manual entry whereas fulfilling NMVO and MAH are not given this information.
Pack disclosure report (PDR)/ audit trail	Yes – but only list transactions on the pack in their own country	Yes – all transactions (including data upload) relating to pack regardless of where they took place	Yes – all transactions (including data upload) relating to pack regardless of where they took place	Each NMVO generates PDR from their own NMVS; they do not 'share' PDRs with each other or with the MAH who generates their own PDR via their connection to the EU Hub.
End-user – location ID (Also known as 'client ID')	Yes	Yes	No – MAH is notified of 'Organisation ID' but not location ID	NB – Alert notifications to NMVOs & PDRs contain the end-user location ID in all cases, but **not** the end- user's name or address. An 'Organisation ID' is allocated to each end-user organisation that has an account in a NMVS. The organisation sets up individual locations (premises) – each represented by a unique location ID - against the organisation's NMVS account. The Organisation ID does not include the name or address of the organisation.
End user – location name & address	Yes - initiating NMVO can look up the name and address of the end-user location using the ID of the end-user	No - fulfilling NMVO does not have access to any information that will identify end-users in other markets	No	

The name and address of an end-user must not be disclosed by the NMVO in the initiating market to the NMVO in the fulfilling market (or to the MAH or EMVO). Contacting the end-user in the initiating market whose scan generated the alert is solely the role of NMVO in that country or the NCA, where it is necessary for the NCA to become involved in the investigation.

Who is responsible for investigating IMT alerts?

The investigation of an alert to determine the root cause must be initiated in the initiating market where the pack was physically scanned and the NMVO in that market is responsible for ensuring that the alert is fully investigated. EMVO may also be contacted to provide support for investigation of IMT alerts, for example when the alert is due to missing data in the EMVS.

As product owner, the MAH must also investigate the alert, even if they are not active in the initiating market.

It is important to note that many alerts can be resolved in the initiating market by the NMVO working with the end-user and/or MAH without any requirement to contact the NMVO in the fulfilling market.

The NMVO in the fulfilling market should only support the alert investigation if requested to do so by the NMVO in the initiating market. This may take the form of disclosing contact information to the MAH or providing supplementary information about transactions for those alerts (mostly A7, A24) where this information is needed for root cause determination. As described previously, the name and address of an end-user who carried out transactions on the pack in the fulfilling market prior to it coming to the initiating market, are never disclosed to the NMVO in the initiating market (or to the MAH or EMVO). If end-user error can be ruled out and a data issue related to unsynchronised batches is suspected, the NMVO in the fulfilling market will need to be involved in the investigation as they alone can check if the batch has been uploaded to the fulfilling NMVS.

Where an **AMS** is used to support alert investigation, the initiating NMVO is responsible for ensuring that the alert investigation is complete. The fulfilling NMVO should not change the alert state to closed.

Where there is **no AMS**, the NMVO in the initiating market shall notify the NMVO in the fulfilling market of the outcome of the alert investigation and whether it has been possible to rule out technical, data or procedural errors. If technical, data or procedural errors have been ruled out, the two NMVOs should then immediately notify their respective NCAs that the pack is a suspected falsification. It is also recommended that EMVO be notified.

3.8 Role of BeMVO in investigation of alerts

Article 37(d) of Delegated Regulation requires the legal entities operating the repositories systems, i.e., EMVO and the NMVO, to provide for the investigation of all potential falsifications. This section describes the overall role of BeMVO in the investigation of alerts.

BeMVO role in investigation of individual alerts

The process flow for BeMVO involvement in investigation of individual alerts is set out in Figure 4. The general principle is that the BeMVO does not actively intervene within the first 2 working days of an alert being generated to allow the end-user and MAH to undertake their investigations. If an alert appears unusual and BeMVO believes it requires immediate investigation, BeMVO may intervene sooner.

Additionally, BeMVO must support communications between end-users and MAHs about alerts to maintain end-user anonymity if there is no AMS to facilitate direct (anonymous) communications between them.

NMVO-01a. BeMVO notified of alert root cause by MAH within 2 working days of alert being generated

If BeMVO is informed by the MAH that the alert generated by an end-user was due to an error on the part of the MAH, BeMVO will inform the end-user.

NMVO-01b. BeMVO notified of alert root cause by end-user within 2 working days of alert being generated

If BeMVO is informed by an end-user that the alert was due to an error on the part of the end- user, the MAH will receive the information through the NMVS Alerts platform which is also connected to EAMS.

NMVO-02. BeMVO investigates alert if no feedback from end-user or MAH within 2 working days of an alert being generated

The NMVS Alerts platform will allow BeMVO to see that an end-user or MAH is not taking appropriate action to investigate an alert generated in the NMVS. If BeMVO has not received any feedback on an alert from the parties involved (i.e. end-user and/or MAH) via the NMVS Alerts platform, or any other relevant communication channel within 2 working days of an alert being generated, BeMVO should contact the end-user or MAH (depending on where they consider the most likely root cause of the alert to lie) to request that the alert be investigated, via the NMVS Alerts platform or EAMS where this functionality is in place.

If it is not possible to complete the investigation of an alert due to the end-user and/or the MAH failing to provide any essential information or assistance, BeMVO may request the NCA to intervene with the relevant party(ies).

NMVO-03. BeMVO completes investigation of alert

If the root cause has not already been identified by the end-user or MAH, BeMVO will utilise the results of its own investigations and information from other sources including end-users and their software providers, MAHs, EMVO, etc. to determine if alert can be explained by technical issues with the repositories system, the data upload, the person performing the verification or similar technical issues. If this is confirmed, BeMVO closes out the alert.

BeMVO must document the outcome of its investigations, using the NMVS Alerts platform.

NMVO-03a. BeMVO feedback

BeMVO should inform the end-user or MAH as appropriate if the alert has been closed out and provide any relevant information, e.g., inform the end-user that the MAH has uploaded missing pack data or inform the MAH that an end-user technical or procedural issue was the cause of the alert.

NMVO-04. BeMVO ensures that NCA, EMA and Commission is informed of suspected falsification

BeMVO must ensure NCA, the EMA[8] and the European Commission[9] are informed as soon as it is clear that the alert cannot be explained by technical issues with the repositories system, the data upload, the person performing the verification or similar technical issues (i.e., the pack is a suspected falsification) – either by doing so themselves or verifying this has been done by another party.

BeMVO also informs EMVO of a suspected falsification in their market.

Systematic monitoring of alert numbers and patterns by BeMVO

BeMVO also systematically monitor alerts generated in the NMVS to identify:

1. Products/batches of products that have high numbers of alerts associated with them suggestive of a problem with data upload or product master data. BeMVO will contact the relevant MAH to request they investigate the issue and take appropriate corrective action which should be completed within 2 working days of BeMVO's request. If the matter is not resolved after 2 working days, the MAH should provide BeMVO with a progress update at that point and inform the NMVO when the matter is resolved.
2. End-user locations with large numbers of alerts and/or types of alerts that are suggestive of a problem with a scanner or end-user software or procedural errors. Where relevant, BeMVO contacts the end-user to request that they investigate the issue and take appropriate corrective action.
3. If the alert type is suggestive of an end-user software issue, BeMVO will check if similar alert patterns are seen with other locations using the same software and, in this case, BeMVO will contact the relevant end-users and their IT software provider to investigate and take corrective action as this will resolve all alerts generated by the software issue in those locations.
4. If there are patterns of alerts suggestive of an error by the MAH when carrying out transactions on packs in their possession via the EU Hub (e.g., multiple A7 alerts on a batch within short time period), then BeMVO contacts the relevant MAH to seek

[8] By email to QDEFECT@ema.europa.eu
[9] By email to SANTE-PHARMACEUTICALS-B4@ec.europa.eu

confirmation that their assessment is correct, unless the MAH has already contacted them about the matter.

5. Unusual patterns of alerts/alert spikes which depending on the timing of the alerts, how they were generated (end-user scan, MAH transaction, IMT or pack synchronisation process), may indicate an issue with the NMVS, EU Hub or other NMVS in case of IMT or pack synchronisation-related alert. BeMVO will liaise with all relevant parties (including EMVO and the provider of the NMVS) to establish the root cause of the alerts and to identify what corrective and preventive actions are required.

3.9 Role of EMVO in investigating alerts

EMVO provides support to NMVOs and MAHs in investigating alerts, for example, where system issues within the EMVS and the EU Hub are considered to be a factor or when the root cause is not readily obvious to the NMVO or MAH.

EMVO also ensures that alerts generated in the EU Hub that are reported to MAHs but not to NMVOs are fully investigated.

4. Roles and Responsibilities

Role	Responsibilities[10]
EMVO	• Ensures that all alerts generated in the EU Hub that are reported to MAHs but not to NMVOs are fully investigated. • Provides support to NMVOs and MAHs in investigating alerts, particularly where system issues within the EMVS and the EU Hub are considered to be a factor.
End-User	• Investigates alerts generated when they verify or decommission packs to determine if the alert is due to technical or procedural error on their part, in accordance with the procedures defined in this SOP. • Provides support to BeMVO and MAH in their investigation of alerts generated by the end-user.
MAH	• Investigates alerts generated when their products are verified or decommissioned, in accordance with the procedures defined in this SOP. • Takes corrective action (where possible, and as soon as possible) where alerts are due to MAH error and provides feedback to BeMVO, and where applicable to the end-user, within 2 working days of the alert being generated, in accordance with the procedures defined in this SOP. • Provides support to NMVOs and EMVO in investigating alerts relating to the MAH's products.
BeMVO	• Ensures that all alerts generated in their NMVS are fully investigated. • Manages IMT alerts in accordance with the procedures defined in this SOP. • Ensures that NCA, the EMA and the Commission are notified of suspected falsifications.

[10] Current practice in relation to alert handling in some countries may differ to what appears in this document due to national legislation or NCA requirements; in these cases, the relevant national requirements must be followed by end-users, MAHs and the NMVO.

5. Reimbursement of packs that can't be dispensed to the patient

For reimbursement of packs that can't be dispensed to the patient because of the Belgian SOP for Alert Handling the same procedures should be followed as for a pack that shows a quality defect.

- In case the pharmacist, hospital or wholesaler bought an already decommissioned pack from the MAH, the MAH should reimburse the pack
- In case the pharmacist or hospital bought an already decommissioned pack from the wholesaler, the wholesaler should reimburse the pack
- In case the MAH requests that a pack should be destroyed or returned because he cannot upload correctly the pack in the EU-Hub the MAH should reimburse the pack
- In case the end-user can't guarantee the authenticity of the pack and he didn't buy the pack directly from the wholesaler or MAH, the end-user will bear the costs of the pack
- In case of a falsification the entity who brought the pack into the supply chain will assume the costs

6. Reference Document

Document ID	Title
Commission Delegated Regulation (EU) 2016/161	Commission Delegated Regulation (EU) 2016/161 of 2 October 2015 supplementing Directive 2001/83/EC of the European Parliament and of the Council by laying down detailed rules for the safety features appearing on the packaging of medicinal products for human use
Directive 2001/83/EU	Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (as amended)
Directive 2011/62/EU	Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into thelegal supply chain of falsified medicinal products

7. Glossary

Term/Acronym	Definition
Alert	An alert is an exception which is deemed as critical and therefore should be notified. Alerts, therefore, produce notifications.
Alert ID	An Alert ID is an identifier for a single instance of an alert. One pack can be associated with one or many Alert IDs. This term is commonly called by 'Unique Alert Return Code' (UPRC), which is physically related to medicinal packs as part of a returns process.
AMS	Alert Management System that is accessible via NMVS for end-users and EU Hub for MAHs.
ATD	Anti-tampering device means the safety feature allowing the verification of whether the packaging of a medicinal product has been tampered with.
Barcode	The two-dimensional (2D) data matrix placed on the outer packaging of a medicinal product in which the manufacturer has encoded a unique identifier pursuant to Article 5 of the Delegated Regulation.
Commission Q&A on Safety Features	A document which is published and regularly updated by the European Commission setting out frequently asked 'questions and answers' regarding the implementation of the rules on the safety features for medicinal products for human use.
Delegated Regulation	Commission Delegated Regulation (EU) 2016/161.
EMVO	European Medicines Verification Organisation.
EMVS	European Medicines Verification System.
End-users	Pharmacy, hospital, wholesaler or any other person authorised or entitled to supply medicinal products to the public who is obliged under the Delegated Regulation and relevant national legislation to be connected to an NMVS for the purpose of verifying and decommissioning unique identifiers on medicines they supply to the public.
End-user's software system	Software used by an end-user to connect to an NMVS. It may be a standalone application or a FMD module within an existing application.

Term/Acronym	Definition
Falsified Medicines Directive (FMD)	Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products.
IMT alert	An alert generated as a result of an intermarket transaction (IMT) is known as an IMT alert. The term 'intermarket transaction' describes the functionality that occurs when a pack is scanned in a market that was not its originally intended market for sale (initiating market). The scanned pack is not immediately reported to the end- user as 'unknown' by the relevant NMVS but instead a query is sent to the EU Hub and the Hub then sends a directed query to the NMVS in the market originally intended for the sale of the pack scanned (fulfilling market), allowing the pack to be authenticated in a market that holds the data for the pack.
'Indian pack(s)'	Packs manufactured in India prior to 9th February 2019 and serialised according to the Indian Track and Trace system for exports of pharmaceuticals (coded using GS1 standards).
Investigation	Article 37(d) of the Delegated Regulation requires the investigation of all potential incidents of falsification flagged in the EMVS. The NMVOs can fulfil their obligation to provide for such incidents to be investigated either directly or by ensuring this task is performed by someone else. The purpose of this investigation is to rule out that alerts triggered in the system have been caused for technical reasons, such as issues with the EMVS, data upload, data quality, incorrect end-user scanning or other similar technical issues.
IT software provider	The provider of the software used by an end- user to connect to a NMVS.

Term/Acronym	Definition
Level 5 alert	A Level 5 alert is generated when the EMVS detects a potential suspected falsification and the following parties are notified about the alert by the EMVS - initiator of the transaction (end- user or MAH), the relevant NMVO (if alert is generated in their NMVS), EMVO and the product owner, the MAH (if not the initiator of the transaction).
MAH	Marketing Authorisation Holder. For the purpose of this document, the term MAH shall be deemed to refer to and include, as appropriate, the following: • The OBP who manages the upload of product master data and product pack data to the EU Hub on behalf of the MAH; • Any party who places the MAH's product(s) on the market in a Member State on behalf of the MAH, including a local affiliate or representative; • Any other party to whom the MAH has delegated responsibility for any of its obligations under the Delegated Regulation; • The authorised manufacturer(s) of the MAH's product(s).
NCA	National Competent Authority is a governmental agency, or any other entity formally designed by a Member State as a (national) competent authority for the Member State for the purposes of the Delegated Regulation. Member States may designate more than one NCA for this purpose so the term 'NCA' as it appears in this document should be taken to refer to all relevant NCAs in country where there are more than one. All references in this guidance to notifying suspected falsifications to NCAs shall be deemed to encompass any intermediate reporting requirements that are in place in individual Member States, including reporting of suspected falsifications by MAHs to government or federal agencies. NCAs are ultimately responsible for the decisions made if a pack is confirmed as being falsified and if it has an impact on public health.
NMVO	National Medicines Verification Organisation.

Term/Acronym	Definition
NMVS	National Medicines Verification System. All references to NMVS should be read as also including supranational repositories.
OBP	On-Boarding Partner. A company or organisation that represents the affiliated entities that hold marketing authorisations for products for which the OBP uploads product and pack data to the EU Hub. The OBP also retrieves from the EU Hub, details of alerts generated in relation to the MAH's products in the EMVS.
Pack Disclosure (Stakeholders) Report (PDR)	A report that contains all information about a pack from creation, including all verification events and status changes, and comprises data from the NMVS audit trails only (i.e. audit trails created per the requirements of Article 35(1)(g) of the Delegated Regulation). MAHs, EMVO and NMVOs may only request a PDR for an alert ID that is transmitted to them.
Product Master Data (PMD)	Product Master Data are considered as the set of data elements associated with a specific product record and contain the elements of information about the product.
Product Pack Data (PPD)	This transactional data is associated with the upload of batches and serial numbers.
Safety features	Combination of unique identifier and ATD placed on the outer packaging of a medicinal product pursuant to Directive 2001/83/EC as amended by the Falsified Medicines Directive.
Unique identifier (UI)	'unique identifier' means the safety feature enabling the verification of the authenticity and the identification of an individual pack of a medicinal product. The unique identifier shall be considered as the combination of: • product code, • serial number, • batch number, • expiry date and if required by the Member State where the product is intended to be placed on the market, a national reimbursement number or other national number identifying the medicinal product.
UPRC	Unique Pack Return Code (see 'Alert ID' definition)

Figure 1: End-user process (see also section 3.3)

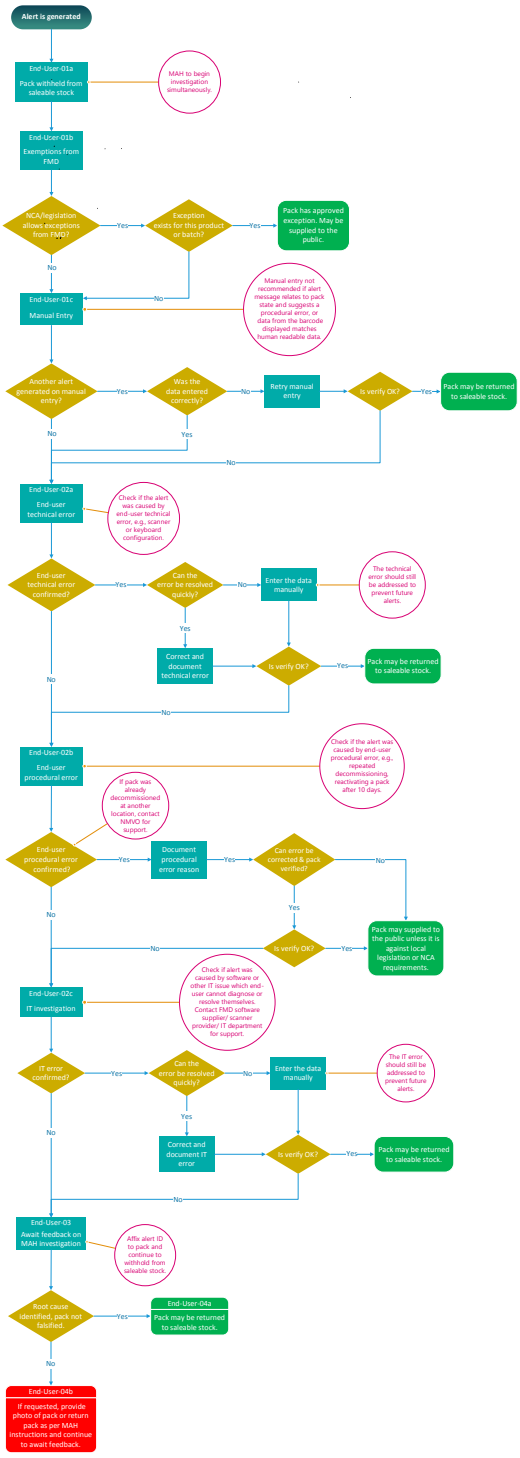


Figure 2: MAH process (see also section 3.5)

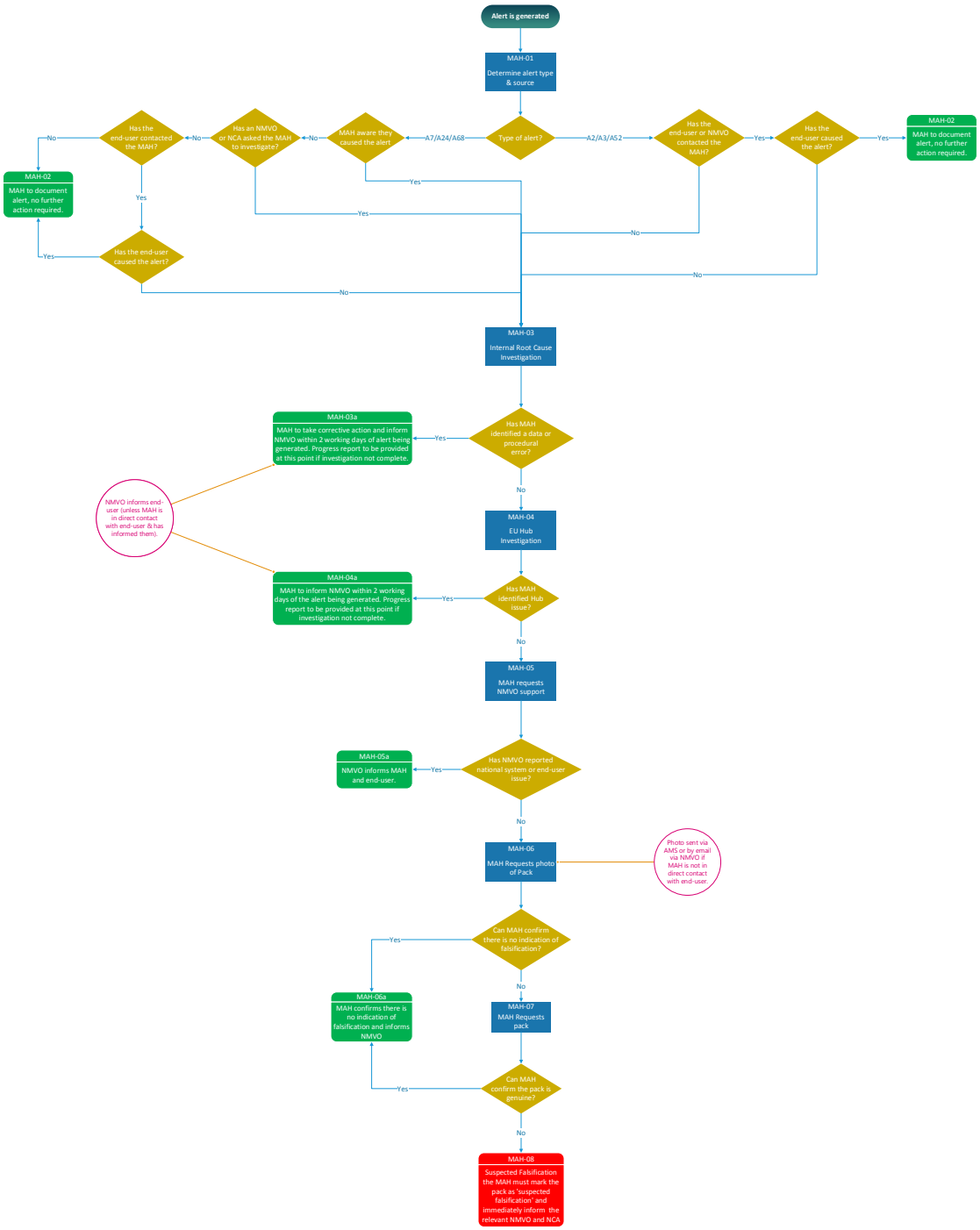


Figure 3: IMT alert process (see also section 3.7)

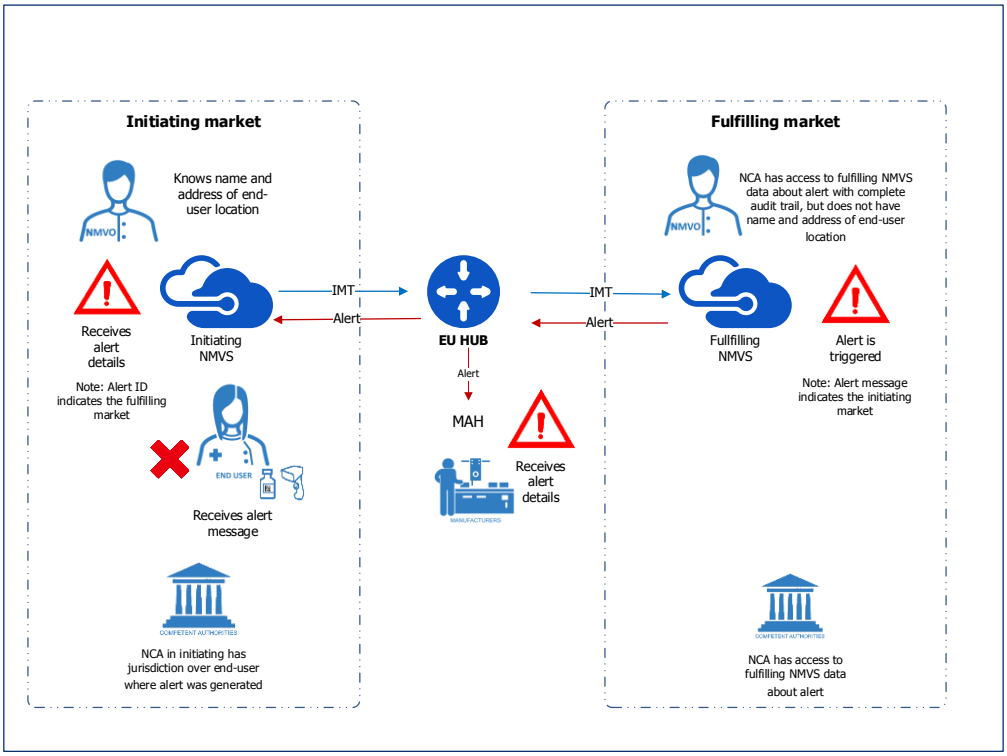
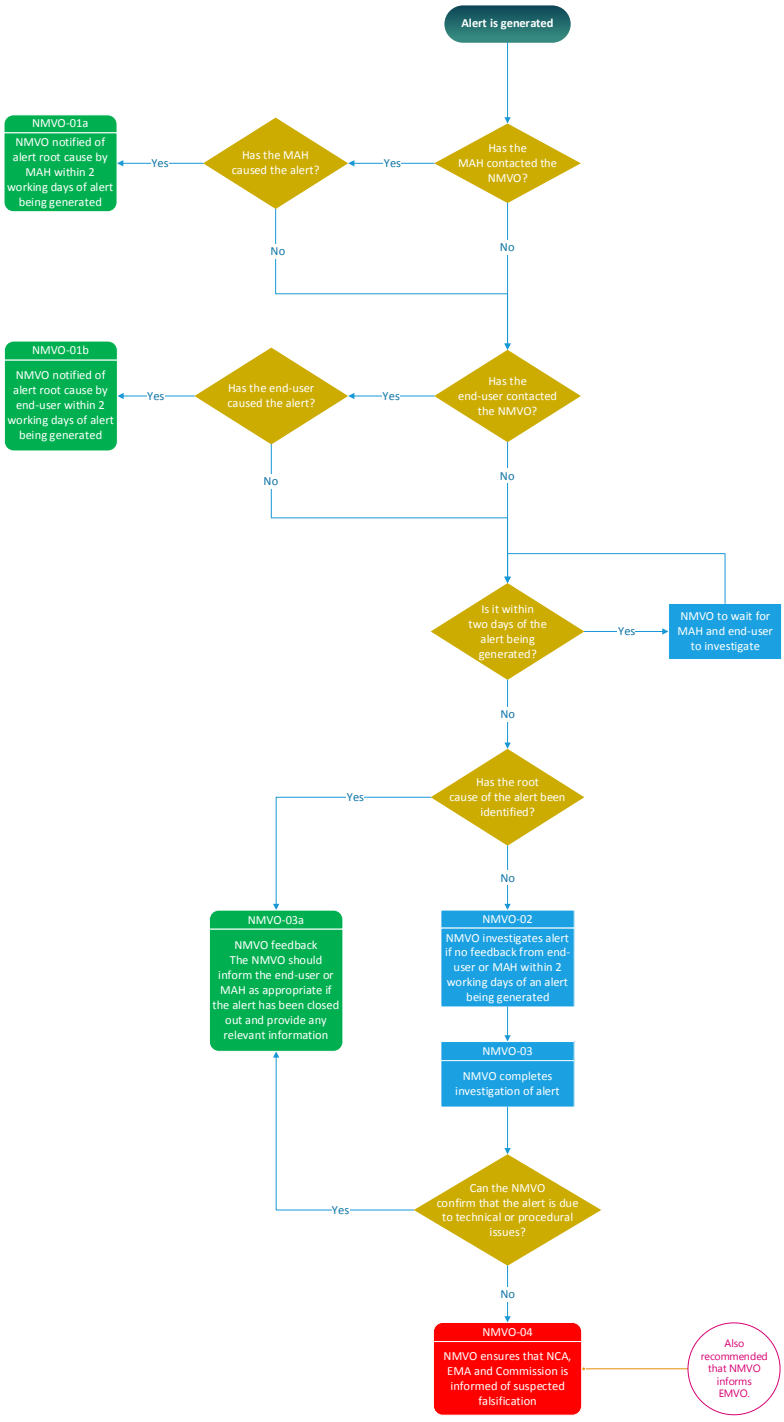


Figure 4: NMVO process (see also section 3.8)



Appendix 1 – Overview of provisions in Delegated Regulation, Falsified Medicines Directive and EMA Guidance regarding alert handling & reporting obligations

The **Delegated Regulation** defines certain responsibilities in relation to handling of alerts as follows:

- Manufacturers (Article 18), wholesalers (Art 24), and persons authorised or entitled to supply medicines to public (Art 30) are obliged to "immediately inform" the relevant competent authority where they have reason to believe that the packaging of a medicinal product has been tampered with, or where verification of the safety features shows that the product may not be authentic.
- Article 32(4) and Article 39 state that NCAs must have access to the repository for the purposes specified in Article 39, one of which is investigating potential incidents of falsification.
- Article 37(d) states that legal entities managing the repositorysystem (NMVOs/EMVO) must provide for the immediate investigation of all potential incidents of falsification flagged in the system and for alerting the NCA, European Medicines Agency and the European Commission should the falsification be confirmed. The Commission has clarified in its Questions & Answers on Safety Features that the term "provide for" in Article 37(d) means that an NMVO must ensure that the NCA, the EMA and the Commission are informed and that the NMVO can fulfil this obligation either directly or by ensuring this task is performed by someone else. The NMVO should ensure authorities are informed as soon as it is clear that the alert triggered in accordance with Article 36(b) cannot be explained by technical issues with the repositories system, the data upload, the person performing the verification or similar technical issues.

Further responsibilities are set in **Directive 2001/83/EC (as amended by the Falsified Medicines Directive**), specifically:

- Article 46(g) states that the manufacturer must in addition to informing the competent authority, notify the MAH immediately if he obtains information that medicinal products which come under the scope of his manufacturing authorisation are, or are suspected of being, falsified irrespective of whether those medicinal products were distributed within the legal supply chain or by illegal means.
- Article 80(i) states that the holders of a distribution authorisation (wholesalers) must in addition to informing the competent authority, where applicable, notify the MAH of medicinal products they receive or are offered which they identify as falsified or suspect to be falsified.

The **EMA** provides further guidance on responsibilities relating to alert handling at falsified medicines reporting obligations:

- The EMA applies the obligation to report confirmed **incidents of falsification flagged by the safety features repository system to the EMA per Article 37** of the Delegated Regulation to MAHs and marketing and manufacturing

authorisation holders**. The guidance that accompanies the EMA's reporting form states that only reports related to Centrally Authorised Products (CAPs) are sent to the EMA and that reports related to nationally authorised products and Mutual Recognition Procedure/Decentralised Procedure (MRP/DCP) should be sent to the relevant NCAs.**

- On being notified of a (suspected) falsified medicine, EMA informs the concerned national competent authorities, who are responsible for investigating the supply chain and deciding on any market action.
- EMA also informs the parallel distribution network about confirmed falsified products or medicine theft. It does so proactively, to prevent reintroduction of illegal units into the supply chain.

Appendix 2: Explanation of alert categories

Alert Code		Description
EU Hub / Solidsoft Reply national systems	*Arvato national systems*	
A2	NMVS_FE_LOT_03	Batch not found
A3	NMVS_NC_PC_02	Pack not found
A32	NMVS_NC_PC_02	Duplicate serial numbers. Note: A32 alerts are only generated with bulk of pack decommissioning or verification requests by end-users. MAH transactions via EU Hub do not generate A32 alerts.
A7	NMVS_NC_PCK_19	Pack already in requested status
A24	NMVS_NC_PCK_22	Attempt to decommission an already decommissioned pack
	NMVS_NC_PCK_06	Actual pack status does not match the undo transaction (set and undo status must be equivalent).
	NMVS_NC_PCK_27	Status change could not be performed (applies only to IMTs)
A52	NMVS_FE_LOT_12	Expiry date mismatch
A68	NMVS_FE_LOT_13	Batch number mismatch

Note: It is not in scope of this document to describe alert categories in detail.