Alert Management Guidance

Table of contents

1. Introduction

1.1. Scope of guidance

The objective of this document is to outline the process for handling Level 5 alerts[1] generated in the Irish Medicines Verification System (IMVS) by wholesalers, pharmacies and hospitals[2] (collectively known as 'end-users') and by MAHs (pharmaceutical companies).

A key principle underpinning this guidance is that an alert does not automatically mean that a pack is falsified. An alert represents a **potential falsification** and requires investigation by the relevant parties to establish its root cause and to rule out technical, procedural and European Medicines Verification System (EMVS) related errors.

This guidance describes the overall framework for alert investigation, covering all types of Level 5 alerts whether generated by end-user or MAH transactions. It sets out step-by-step process flows for the investigation of alerts and identifies the point at which the HPRA must be notified of confirmed falsifications. It also defines the role of end-users, MAHs and IMVO and describes how communications between them will be managed.

The guidance provides the basis for on-screen 'Alert help' available to end-users when a specific alert is generated in their FMD software. These on-screen help pages should be the first point of reference for an end-user when investigating an alert as the information provided is tailored to the relevant alert type.

1.2. Out of scope

The following are out of scope of this guidance:

- Activities relating to the **investigation of alerts other than Level 5 alerts**. These alerts can be differentiated from Level 5 alerts by the fact that the error message will **not** contain a unique Alert ID. Some of these non-Level 5 alerts may generate red or amber responses from your FMD software screen and will require follow-up. However, these alerts are not considered to represent a potential falsification and the IMVS does not report them to IMVO, the MAH or HPRA. Separate guidance will be provided on how to deal with these alerts.

- **HPRA processes**, i.e., HPRA processes for handling suspected quality defect reports related to safety features and following up on reports of suspected and confirmed falsifications.

[1] Level 5 alerts are generated when the EMVS detects a potential suspected falsification. Level 5 alerts contain a unique Alert ID and are flagged as 'red' where the FMD software is applying the Red/Amber/Green exception classification system recommended by IMVO. For more information about different 'levels' of exceptions and alerts in the EMVS, please see Appendix 1.

[2] References to 'pharmacies and hospitals' in this guidance should be read as encompassing all persons authorised or entitled to supply medicinal products to the public who are required to verify and decommission safety features before supplying packs to patients.

- **Alert prevention activities** undertaken by IMVO, end-users, MAHs and EMVO to reduce and prevent alerts. It is expected that all parties will seek to minimise avoidable alerts and the investigation burden for everyone.,

- **Arrangements relating to credit/refund/replacement of packs which generate alerts** and cannot be supplied to patients. These arrangements are not covered by the Delegated Regulation and are outside the remit of IMVO, HPRA and PSI. They are a matter for discussion between the relevant parties in the supply chain.

1.3. Review of guidance

This guidance will be reviewed and updated if required.

2. Glossary

Term/Acronym	Definition
Alert	An alert is an exception which is deemed as critical and therefore should be notified. Alerts, therefore, produce notifications. See also *Appendix 1 Overview of alerts*
Alert code	A code used to denote different categories of alerts, e.g., A2 - pack not found, A7 - pack already decommissioned. The alert code is included in the alert messages sent to NMVOs and MAHs, who use these codes to support their alert analysis. End-users' alert messages do not include the alert code. See Appendix 1 for a list of alert codes
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 also known as the 'Unique Alert Return Code' (UPRC), which is physically related to medicinal packs as part of a returns process
AMS	Alert management system
Audit trail	Also known as Pack Disclosure (Stakeholders) Report (PDR) – see definition below
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
Delegated Regulation	Commission Delegated Regulation (EU) 2016/161 on safety features the packaging of medicinal products for human use
EMA	European Medicines Agency
EMVO	European Medicines Verification Organisation
EMVS	European Medicines Verification System. The EMVS comprises the EU Hub (managed by EMVO) and connected NMVS (which are managed by NMVOs)
End-user	Wholesaler, pharmacy, hospital or any other person authorised or entitled to supply medicinal products to the public in Ireland who is obliged under the Delegated Regulation and the Medicinal Products (Safety Features on Packaging) Regulations 2019 (S.I. No. 36 of 2019) to be connected to the IMVS for the purpose of verifying and decommissioning unique identifiers on medicinal products in accordance with their obligations under the Delegated Regulation
FMD software	Software used by an end-user to connect to the IMVS. 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
FMD software provider	Provider of the software used by an end-user to connect to the IMVS
HPRA	Health Products Regulatory Authority
IMVO	Irish Medicines Verification Organisation
IMVS	Irish Medicines Verification System. The IMVS is the national medicines verification system for Ireland. It is connected to the EU Hub and part of the EMVS
MAH	Marketing Authorisation Holder. For the purpose of this document, the term 'MAH' refers to and includes, as appropriate, the following: • The On-Boarding Partner (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. The HPRA (and in some cases also the PSI) are designated by the Medicinal Products (Safety Features on Packaging) Regulations 2019 as competent authorities for Ireland for the purposes of the Delegated Regulation
NMVO	National Medicines Verification Organisation
NMVS	National Medicines Verification System
NMVS Alerts	Name of alert management system for Ireland (managed by IMVO)
OBP	On-Boarding Partner. A company or organisation that represents the affiliated entities (MAHs) 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

Term/Acronym	Definition
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 EMVS 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
PSI	Pharmaceutical Society of Ireland
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
Return a pack to saleable stock	The pack may either be supplied to a patient now or placed back on the shelf for sale or supply at a later stage
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 ID • expiry date
UPRC	Unique Pack Return Code (see 'Alert ID' definition)
Working days	'Working days' are defined as Monday-Friday, excluding public holidays

3. Checking the anti-tampering device

3.1. Pharmacies and hospitals

In addition to scanning the barcode on the pack, pharmacies and hospitals must, at the time of supplying the pack to the public, examine the anti-tampering device (ATD) to see if it has been tampered with.

Even if the barcode scan has been successful, a pharmacy or hospital that has reason to believe that the packaging has been interfered with, based on their examination of the ATD, must report their concern to the HPRA (as a suspected quality defect via the usual reporting mechanisms[3]) and not supply the pack.

3.2. Wholesalers

Wholesalers are not required by the Delegated Regulation to inspect the ATD of each pack that they scan, except where they are decommissioning packs supplied to customers on foot of Article 23 of the Delegated Regulation. However, if they have any reason to believe that any pack has been tampered with, they must report their concern to the HPRA (as a suspected quality defect via the usual reporting mechanisms[3]) and not move the pack into saleable stock.

[3] Reports of packs being tampered with are to be submitted as suspected product quality defects via HPRA's online reporting system https://www.hpra.ie/homepage/about-us/report-an-issue/suspected-medicinal-product-defect

4. Exempt medicinal products / unlicensed medicines

The following guidance has been agreed with the HPRA in relation to handling exempt medicinal products / unlicensed medicines (ULMs) with 2D barcodes:

- **If you know the pack** is a ULM, **do not scan it** as the IMVS may not recognise the pack;
- **If you inadvertently scan a ULM and get an alert,** you may supply the pack unless:
  - you have overriding concerns that a falsified medicine is involved or believe the pack has been interfered with; or
  - the pack as flagged as expired, recalled, withdrawn, stolen or destroyed;
- Always check the **anti-tampering device** (if there is one) – if you have any reason to believe the pack has been interfered with, please report this to the HPRA as a product quality defect and do not supply the pack.

5. Communications about alerts

Timely communications between the different parties involved in an alert is key to speedy resolution of alerts and to minimise any delays getting packs to patients. On the very rare occasion where an alert has been generated due to the pack being falsified, prompt communications ensure that the falsification is quickly identified and follow up action taken by the relevant authorities.

5.1. NMVS Alerts

This guidance has been written on the assumption that IMVO, end-users and MAHs will use the *NMVS Alerts* alert management system (AMS). This web-based system facilitates efficient handling of alerts by allowing the relevant parties to:

- Manage, track and document alerts. It provides real-time information on the status of alerts based on information entered by the end-user, MAH and/or IMVO. The system may be accessed on a 24-hour basis;
- Quickly communicate with other parties about an alert, while preserving end-user anonymity vis-à-vis the MAH[4], which is a core principle of the EMVS and *NMVS Alerts*;
- Maintain an audit trail of their actions for inspection purposes.

End-users and MAHs can create an account in *NMVS Alerts* free of charge. They can then log in to see a list of all their own alerts and report any information they have to add about the alert (e.g. 'our scanner wasn't working'; 'we accidentally decommissioned the pack/marked it as supplied or dispensed several times').

When an alert is generated, an automated email will be issued to the end-user with a link to the relevant alert record in *NMVS Alerts*. It is not necessary to have an account in *NMVS Alerts* to receive or access this link. The end-user should use this link to provide feedback about a particular alert if they do not have an account in *NMVS Alerts*.

5.2. Email and phone contacts

If an organisation chooses not to use *NMVS Alerts*, communications will have to take place with other parties by email or phone. This is not recommended, as it will significantly slow the speed of investigation in those cases.

If MAH needs to communicate with an end-user that is not currently using *NMVS Alerts*, IMVO will act as an intermediary as the MAH does not know the end-user's identity or location.

IMVO may be contacted by email (alert.support@imvo.ie) or phone (-353-1-5715320) during the following times:

[4] Neither the end-user's identity nor location are disclosed to the MAH by the EMVS or *NMVS Alerts*.

Days	Time
Monday-Friday	08.00-20.00
Saturday	09.00-18.00
Sunday and public holidays	11.00-18.00

It should be noted that if a query needs to be escalated internally to second line support or if IMVO needs to contact another party such as the MAH to get further information, an immediate response may not be possible, particularly outside standard business hours (09.00-17.00, Monday-Friday). Please note also that IMVO has no authority to direct that the pack may be supplied in circumstances where an alert remains unresolved.

5.3. Internal communications in pharmaceutical companies

Alerts relating to an MAH's products are sent to their OBP. Where the MAH is different to the OBP, 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.

6. Summary of alert management process

An alert investigation comprises a series of steps designed to systematically assess and rule out possible root causes 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). Root causes include:

- Procedural errors (e.g., double decommissioning, incorrect manual entry)
- Technical errors (e.g., scanner not configured correctly, FMD software issues)
- Data upload errors (e.g., data not uploaded by MAH, incorrect data uploaded)
- EMVS errors (e.g., IMVS or another component of EMVS not working correctly)

End-users and MAHs are expected to initiate simultaneous investigation of alerts generated when end-users scan packs[5] - **see section 7 (End-users) and section 9 (MAHs)**. MAHs must also investigate alerts generated from their own transactions via their EU Hub connection on packs for which data is held in the IMVS **(see section 9)**.

When an end-user is investigating an alert, they should look for errors relating to matters under their control such as procedural issues or scanner or software errors **(see section 7).** If the end-user establishes that the alert is due to a procedural error on their part, the pack may be returned to saleable stock. Similarly, if the end-user identifies a scanner or software error and is able to fix it and verify the pack correctly, the pack may be returned to saleable stock. In all situations where the pack is to be returned to saleable stock, the end-user must document the outcome of their investigation.

MAHs should look for data upload issues and issues with the EMVS. MAHs are expected to provide feedback within two working days[6] to IMVO and the end-user. Further progress reports must be provided if the alert is not resolved at that stage **(see section 9)**.

If there is no action by/feedback from the end-user or the MAH in *NMVS Alerts* within two working days of the alert being generated, IMVO steps in to ensure that the alert is investigated, with assistance as required from both parties. If the root cause has already been identified by one party, they are asked to update *NMVS Alerts* so the other party is aware of this **(see section 11).**

The end-user must withhold the pack from saleable stock until the root cause has been identified by themselves or the MAH and the pack is not deemed to be falsified. The MAH may request a photo of the pack. There are three possible outcomes of the MAH's examination of the photo – (i) no indication of falsification **(see section 9, MAH step 5a**); (ii) data, procedural and technical issues are ruled **(suspected falsification – MAH step 5b)**, or (iii) the packaging is falsified **(confirmed falsification – MAH step 5c).**

[5] MAHs are not required to investigate certain categories of alerts generated at end-user locations – as these are typically due to end-user error - unless asked to do by NCA, NMVO or end-user (see section 9 for details)

[6] Alert is generated on day 0 (e.g., Tuesday), feedback is expected by 23.59 (Irish time) on day 2 (Thursday).

The MAH then requests that the suspected falsified pack be returned to them for examination and will advise the end-user on the procedure for the return. The MAH will also request the return of packs confirmed as falsified when the pack photo was examined.

If MAH cannot confirm that a suspected falsified pack is genuine on foot of their examination of the pack, it is deemed to be a **confirmed falsification**. Various parties including IMVO and the HPRA must be informed **(see section 9 – MAH step 7)**. Notifying the HPRA is the responsibility of the MAH (IMVO confirms that the relevant notification has been made). End-users should **not** report alerts in isolation as suspected product quality defects to the HPRA.

In addition to overseeing individual alerts, IMVO monitors the IMVS for large numbers of alerts and unusual patterns of alerts by product, batch or end-user location or linked with a specific FMD software system. IMVO contacts the relevant MAH or end-user or FMD software provider to request that they take corrective action and preventive action to prevent further alerts. The objective here is to ensure that issues leading to large numbers of alerts at a given end-user location, with a particular product/batch or FMD software system are quickly identified and resolved with support from IMVO **(see section 11).**

In the case of IMT alerts generated on packs for which there is no data in the IMVS, the investigation is overseen by IMVO, as the pack will have been scanned in Ireland. For certain alerts, information may be required from the NMVO in the market where the uploaded data for the pack are to be found and IMVO will liaise with the relevant NMVO **(see section 14).**

7. Procedure for end-users

7.1. Steps in alert investigation

The procedure for investigating an alert that arises in an end-user location includes a number of steps, with different responsibilities for each party (end-user/IMVO/MAH) depending on the nature of the alert. See *Figure 1* for an overview of the process for end-users.

If the cause of the alert is established in any given step, the investigation can end there and does not need to proceed to the next stage.

Alerts on packs in isolation should **not** be reported as suspected product quality defects to the HPRA by end-users. The only situation where an end-user should submit such a report to the HPRA is where they suspect the pack has been tampered with based on their examination of the anti-tampering device (see section 3 - *Checking the anti-tampering device*).

End-user step 1 – Withhold pack from saleable stock

When a pack generates an alert, you should immediately set the pack aside while the alert is investigated. The pack may not be placed back into saleable stock until the investigation is complete and falsification has been ruled out.

The HPRA has confirmed that packs that have generated alerts must not be returned by pharmacies or hospitals to wholesalers while an alert investigation is ongoing, as such packs could be falsified and should not be put back into the supply chain. This applies even if you have ruled out a technical or procedural error on your part.

Do not try to clear the alert by rescanning the pack as this may lead to further alerts.

End-user step 2 – Follow the link in the alert message to IMVO 'Alert help pages'

FMD software providers, at the request of IMVO, have incorporated quick links from the onscreen alert message to 'Alert help pages' on the IMVO website. Here you will find guidance on how to deal with the specific type of alert that has been generated which will assist you in identifying the root cause quickly and what to do next. The advice in those help pages reflects the fact that the steps involved vary depending on whether the alert relates to a pack state mismatch or a data mismatch (see table 1).

Table 1 – Steps in alert investigation by end-user

Type of alert	Example of error message on screen	Steps involved
Pack data mismatch *There is a mismatch between the data scanned from the pack barcode and what is held in the IMVS database for that pack*	• Pack not found • Batch not found • Batch ID mismatch • Expiry data mismatch	• Check for procedural error *(End-user step 3)*
		• Check if there is any information about the alert from IMVO or the MAH *in NMVS Alerts (End-user step 4)*
		• Technical error check by end-user themselves *(End-user step 5)*
		• External technical support sought *(End-user step 6)*
Pack state mismatch *The pack is not in the expected state (active/decommissioned etc.) and therefore a request to change its status cannot be completed*	• Pack is already in the requested state • Pack was already decommissioned in another location	• Check for procedural error *(End-user step 3)*
		• Check if there is any information about the alert from IMVO or the MAH *in NMVS Alerts (End-user step 4)*

An overview of **all** possible steps in the alert investigation process for end-users is described below. The 'Alert help' page guidance that you access on screen for any given alert will only list the steps that are relevant for that alert. If a root cause for the alert is established in any given step, the investigation can end there, and you do not need to proceed to the next step.

End-user step 3 – Check for procedural error

The type of procedural errors that cause alerts vary depending on whether the alert relates to a data mismatch or a pack state mismatch.

End-user step 3a – Procedure error where there is a data mismatch

If your alert relates to a **data mismatch issue**, the two most common procedural errors that may have caused this are:

i. *Manual entry:* If an alert arose when you entered the data manually, rather than scanning the pack, check that the data entered matches what is printed on the pack. If not, then attempt to type it again correctly. If the pack is successfully verified and decommissioned after repeating the manual entry attempt, it may be returned to saleable stock. If not, continue to withhold the pack from saleable stock and proceed to the next step – *Check NMVS Alerts for IMVO/MAH feedback (End-user step 4).*

ii. *Linear and 2D barcode data being captured in a scan*: Check if there is a linear barcode close to the 2D barcode on pack. If you suspect your scanner might have scanned the two

barcodes at the same time, contact IMVO for support. These alerts are uncommon and can be avoided by covering the linear barcode with your thumb when scanning the 2D barcode.

End-user step 3b – Procedure error where there is a pack state mismatch

If the alert relates to a **pack state mismatch**, it may be due to a procedural error, for example:

- Decommissioning bulk/split pack as supplied more than once
- Decommissioning a pack that was previously decommissioned at another location, for example, a pack borrowed from another pharmacy or hospital
- Trying to decommission a pack as destroyed when it was already decommissioned as supplied

If you are certain that you caused the alert, for example, by scanning a pack several times, the investigation does not go any further and the pack may be returned to saleable stock. For this type of alert, it is usually not possible to 'correct' the alert and it is important to document the root cause of the alert and your decision to supply the pack, ideally in *NMVS Alerts*.

Please contact IMVO for support with these alerts if there is no immediate obvious reason why the alert would have occurred, for example you get a 'pack already decommissioned in another location' alert but the pack was not borrowed from another pharmacy or hospital.

If you conclude that no procedural error occurred, continue to withhold the pack from saleable stock and proceed to the next step – *check NMVS Alerts for IMVO/MAH comment.*

End-user step 4 – Check *NMVS Alerts* for IMVO/MAH feedback

In some cases, IMVO or the MAH may become quickly aware of the root cause of an alert, or of multiple related alerts on a particular product or batch and may already have marked this in *NMVS Alerts*. If you can see from *NMVS Alerts* that the root cause has been established by the MAH (or IMVO) and the alert has been resolved, no further action is required by you and the pack may be returned to saleable stock. Otherwise, please proceed to the next step – *end-user technical check*.

End-user step 5 – End-user technical check

This step involves checking for technical issues relating to your scanner or software that you may be able to quickly resolve yourself, for example:

- Misconfigured scanner
- Caps lock switched on
- FMD software update not completed per your FMD software provider's instructions

Follow the guidance provided in the IMVO help page for the alert on how to fix the problem.

If a scanner or software error is found at this stage and corrected, a verification scan of the pack should be undertaken to determine if the corrective action has been successful. If the verification scan is successful, the pack may be returned to saleable stock. You must now also document the root cause of the alert in *NMVS Alerts (or inform IMVO by email or phone)* so that IMVO and the MAH are aware that the alert has been resolved.

If you have been unable to identify a scanner or software issue yourself, continue to withhold the pack from saleable stock and proceed to the next step – *seek external technical support*.

End-user step 6 – Seek external technical support

This step is intended to be a more detailed check for technical issues with software or scanners by your FMD software provider. If you have an internal IT department, it is advisable that you contact them first so they can check for any other IT issues that might have caused a problem with your FMD software, e.g., firewall upgrade, compatibility issue with other software.

If an FMD software or other technical issue is found and corrected, a verification scan of the pack should be undertaken to determine if the corrective action has been successful. If the verification scan is successful, the pack may be returned to saleable stock. You must now also document the root cause of the alert in *NMVS Alerts*.

If a root cause is still unknown at this stage, the pack must continue to be withheld from saleable stock while you await feedback from the MAH. If the Alert ID[7] is shown in your FMD software, affix this to the pack.

End-user step 7 – Await feedback on MAH investigation

MAHs are expected to investigate alerts generated from their own transactions and also alerts from end-users that may be due to MAH data errors or system issues. They are not expected to proactively investigate categories of alerts that are most likely due to end-user procedural errors or scanner issues (see *MAH step 1 – Determine alert type and source* for details).

The MAH is required to report the outcome of their investigation and any corrective action taken by them to fix the root cause of the alert via *NMVS Alerts* as soon as possible and no later than **two working days**[8] of the alert being generated. If the investigation is not completed at that point, they must provide a status update on the alert in *NMVS Alerts* and revert with the final outcome, once known. IMVO will provide feedback to you about the alert if you are not using *NMVS Alerts*.

The MAH may require a photo of the pack to assist in its investigation (see *MAH step 5 – MAH requests photo of pack).* If you receive such a request, please ensure that the photo(s) supplied shows the 2D barcode and the human readable text on the pack. The simplest way to send a photo to the MAH is by uploading it to *NMVS Alerts*. If you are having difficulty doing this, please email the photo to IMVO[9] and ask for it to be sent to the MAH.

You must continue to withhold the pack from saleable stock at the premises where it was scanned until either:

[7] The Alert ID comprises a country code prefix ('IE' for alerts generated on Irish packs), followed by a string of letters and numbers, e.g. IE-HL2-T38-9XX-ZB2-1LO.
[8] Alert is generated on day 0 (e.g., Tuesday), feedback is expected by 23.59 (Irish time) on day 2 (Thursday).
[9] Please email photo to alert.support@imvo.ie along with details of the alert, including the Alert ID.

- ***End-user step 7a – Pack is confirmed as not falsified*:** The MAH (or IMVO[10]) indicates via *NMVS Alerts* that the root cause for the alert has been identified and that the pack is not considered to be falsified. It may then be returned to saleable stock;

  or

- ***End-user step 7b – Pack is returned to the MAH for examination*:** The MAH requests that the pack be returned to them for further investigation. 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. The pack should not be sent as a standard business return, as it must be processed as a product quality complaint by the wholesaler, which is a separate process to their normal returns process.

7.2. Communication of alert investigation results

When you have identified that an alert has been caused by a technical or procedural error on your part, please document this in *NMVS Alerts* as soon as possible, as this important information will then be immediately available to the MAH, allowing them to stop their investigation. IMVO will also be informed. Otherwise, please inform IMVO by email or phone.

As stated in *End-user step 3 (Check NMVS Alerts for IMVO/MAH comment)*, the MAH or IMVO will also use *NMVS Alerts* to inform you of the outcome of any investigations that they undertake. You may also contact IMVO by email or phone to ask for this information.

[10] If IMVO has become involved in the alert investigation – see section 11 for details of when this will occur

8. Procedure for wholesalers

As 'end-users', wholesalers should follow the process outlined in **section 6** and also comply with the additional guidance in this section.

Alerts generated by wholesalers should be managed as part of your quality management system.

Wholesalers should use *NMVS Alerts* to communicate the outcome of your investigation of an alert to all relevant parties, in addition to following any alert notification procedures in technical agreements that you may have with MAHs.

When verifying returns, packs that are flagged as having been previously decommissioned cannot be placed back into saleable stock.

You may be contacted by a pharmacy, hospital or other party about a pack supplied to them which generated an alert when scanned. The action to be taken varies depending on what type of alert is involved:

- If the alert is due to the fact that the pack was already decommissioned, you should investigate if the alert has arisen because of an error on your part while the pack was in your possession, e.g., pack decommissioned as supplied or destroyed in error.
- For all other alerts, refer the person contacting you to IMVO for further assistance.

9. Procedure for MAHs

All MAHs whose products are marketed in Ireland must register with IMVO and nominate a single point of contact (SPOC) and a back-up SPOC for IMVO to communicate with about alerts. If alerts are managed by a different legal entity to the MAH, 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 details about the outcomes of the alert investigations. It is important that your local affiliate or representative in Ireland (if any) is made aware of any alerts that could impact on stock availability in Ireland.

If you are dealing with alerts generated when scanning packs via your wholesaler connection to the IMVS when acting in your capacity as a wholesaler, please follow the process for end-users described in **section 7** and wholesaler-specific variations in **section 8**.

For all alerts notified to you via the EU Hub, follow the process described in this section. See *Figure 2* for an overview of the process for MAHs.

MAH step 1 – Determine alert type and source

The action you are required to take will vary depending on the alert code:

A7, A24, AND A68 ALERTS[11]

As an MAH, you are not required to investigate A7, A24 and A68 alerts except in the following circumstances:

a. You are aware that you have caused the alert(s), due to repeating decommissioning transactions on packs under your control, e.g. packs marked as 'exported' twice;
b. An end-user contacts you about such an alert;
c. IMVO contacts you 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. The HPRA requests you 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, you can determine if the alert was caused by one of your own transactions 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 EU Hub, and you then need to check if the Client ID in the Event Message is your own Client ID[12]. The other possibility is that the alert was generated by a

[11] Please refer to *Appendix 1: Overview of alerts* for an explanation of these alert codes.
[12] Your Client ID can be found in the OBP Portal within the EU Hub.

parallel distributor when decommissioning your packs as 'checked out' via the EU Hub prior to repackaging them, in which case the Client ID reported will be different from yours.

MAH step 1a – No further action is required

If you have not generated the alert(s) and you have not been asked to investigate them by IMVO, the HPRA or an end-user, no further action is required.

MAH step 1b – Further action is required

Please go to the internal root cause investigation step (*MAH step 2*) in the following circumstances:

- It has been confirmed that you have generated the A7, A24 or A68 alert(s);
- You have not generated the alert(s), but IMVO, the HPRA or an end-user has requested you to investigate them (as per points **b.**, **c.**, and **d.** above)

A2, A3, A32 AND A52 ALERTS

For these alerts, the initial step is to determine if you have generated the alert.

You 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., you attempted to verify a pack, but an alert was generated due to an issue with the EU Hub. Similarly, you may be responsible for causing an alert, but you may not have generated the alert yourself, e.g., an end-user may have generated the alert when decommissioning a pack due to the pack data not being uploaded by you.

You should check *NMVS Alerts* to see if IMVO or the end-user has informed you that an A2, A3 or A52 alert is due to end-user error. If this is the case, you are not required to take any further action (*MAH step 1a)*.

Unless you are specifically aware that the alert is due to end-user error, please proceed to the internal root cause investigation step (*MAH step 2*).

All alert types that require MAH investigation

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

MAH step 2 – Internal root cause investigation

You should investigate whether or not the alert was caused by a data or procedural error on your part. Due to the varied nature of systems and processes in use by MAHs, each MAH should 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 packs to a market before uploading the Product Pack Data for the batch. This may happen where the packs are shipped prior to batch release, in which case it is important to

inform the receiving wholesaler, so they know not to scan the packs at goods inwards (and thus avoid alerts due to missing data)

- Sending packs 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 batch has been uploaded;
- Repeated decommissioning of a pack or batch while under MAH control, e.g., decommissioning for export or as locked

MAH step 2a – MAH takes corrective action and informs IMVO

If you determine that a data or procedural error on your part was the cause of the alert, you should take corrective action as quickly as possible and immediately inform IMVO via *NMVS Alerts* when this is complete, but no later than two working days of the alert being generated. A progress report should be provided after two working days if the investigation is not complete at that stage.

If you determine that there was no data or procedural error on your part, please proceed to the next step - *EU Hub investigation*.

MAH step 3 – EU Hub investigation

The next step is for you to investigate whether the alert was due to an issue with the EU Hub. An example here would be where system downtime during transfer of data from the EU Hub to the IMVS resulting in the data not reaching the IMVS, even though you received a 'distributed' call-back confirming that the data was successfully uploaded. If necessary, you should contact the EMVO Helpdesk for support. You may also ask IMVO to check if the data is visible in the IMVS.

If an EU Hub issue is identified as the root cause of the alert, please proceed to the next step – *inform IMVO of Hub issue.*

MAH step 3a – MAH informs IMVO of a Hub issue

If you determine that the alert was due to an issue with the EU Hub, you should inform IMVO via *NMVS Alerts* as soon as possible, but no later than two working days from the alert being generated.

If you determine that the alert was not caused by an issue with the EU Hub, please proceed to the next step - *MAH Requests IMVO Support.*

MAH step 4 – MAH requests IMVO support

If you have found that the alert was not caused by a data or procedural error on your part, or an EU Hub issue, you should contact IMVO and ask them to investigate if there is a root cause at IMVS level or at end-user level.

MAH step 4a – IMVO feedback

If IMVO is able to determine that the alert was caused by an IMVS or end-user issue, IMVO will inform the MAH and the end-user via *NMVS Alerts*. If IMVO cannot confirm that an IMVS or end-user error has occurred, IMVO will inform you via *NMVS Alerts* and you should then proceed to the next step - *MAH requests photo of pack*.

MAH step 5 – MAH requests photo of pack

At this stage**,** you may request a photo of the pack from the end-user via NMVS Alerts if you consider this helpful for the investigation (*see End-user step 7 - Await feedback on MAH investigation*). If the end-user does not upload the photo to *NMVS Alerts*, please contact IMVO who will email the end-user on your behalf.

MAH step 5a – MAH confirms there is no indication of falsification and informs IMVO

If after examining the pack photo, you can confirm that there is no indication of falsification and that the pack data is correct, you should inform IMVO and close the alert in *NMVS Alerts*, marking it as resolved. The pack may then be returned by the end-user to saleable stock.

MAH step 5b – MAH cannot confirm pack is genuine – suspected falsification

If after examining the pack photo, you have ruled out data, procedural and technical issues and cannot confirm that the pack is genuine, it is now considered to be a **suspected falsification.** Please proceed to the step 6 **-** *MAH requests pack for examination.*

MAH step 5c – MAH confirms that the packaging is falsified – confirmed falsification

If, after examining the pack photo, you are satisfied that the packaging is falsified, the pack is deemed to be a **confirmed falsification**, you must now complete the actions in both steps 6 and 7.

MAH step 6 – MAH requests pack for examination

If the alert was generated by an end-user, the request to return the pack should be sent via *NMVS Alerts* or via IMVO. You will also need to advise the end-user of the procedure for the return of the pack - see *End-user step 6 (Await feedback on MAH investigation*).

If you can confirm from your examination of the pack that it is genuine, you should inform IMVO and the end-user (if applicable) by updating *NMVS Alerts* and closing the alert as per MAH step 5a.

If you cannot confirm that the pack is genuine from your examination of the pack (include may include analysis of the contents), the pack is now deemed to be a **confirmed falsification**.

MAH step 7 – Notifying confirmed falsifications

You must now immediately inform the following that the pack is a confirmed falsification:

- IMVO and the end-user (if applicable) via *NMVS Alerts*. Urgent notifications may also be made by phone or email.
- HPRA (via HPRA's product quality defects procedure[13])
- EMA (in the case of a centrally authorised product)

[13] Available at: http://www.hpra.ie/homepage/medicines/regulatory-information/market-compliance-and-surveillance/quality-defects-and-recalls. Reports to be emailed to qualitydefects@hpra.ie

10. 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) 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 about these alerts, the process is as follows:

- Where both parties are connected to *NMVS Alerts*, the parallel distributor and originator MAH may communicate directly with each other in *NMVS Alerts*
- Otherwise, EMVO will provide the parallel distributor with contact details for the originator MAH

11. Role of IMVO in investigation of alerts

This section describes the overall role of IMVO in the investigation of alerts.

11.1. IMVO's role in investigation of individual alerts

The process flow for IMVO's involvement in the investigation of individual alerts is set out in *Figure 3*.

IMVO step 1 – IMVO action immediately after alert is generated

The general principle is that IMVO does not actively intervene within the initial two working day period after the alert has been generated, allowing the end-user and MAH to undertake their investigations first. IMVO will only take action during this period in the following circumstances:

IMVO step 1a – IMVO notified of alert root cause by MAH

If the MAH informs IMVO and the end-user via *NMVS Alerts* that the alert was due to an MAH data or procedural error, the MAH should close the alert in *NMVS Alerts*. No further action is required by IMVO or the end-user. If the notification comes from the MAH by email to IMVO, IMVO will inform the end-user and close the alert in *NMVS Alerts* (if not already done by the MAH).

IMVO step 1b – IMVO notified of alert root cause by end-user

If the end-user informs IMVO that the alert was due to an error on the part of the end-user, IMVO will close the alert in *NMVS Alerts*. No further action is required by IMVO, end-user or MAH.

IMVO step 1c – IMVO determines the root cause of the alert independently

If IMVO establishes the root cause of an alert (or alerts) within the two working day period, independently of any information received from the end-user or MAH, IMVO will mark the alert(s) as closed in *NMVS Alerts* (if not already done by another party) and no further action will be required by the MAH or end-user once this has been done.

IMVO step 1d – IMVO determines that an alert requires immediate investigation

If an alert appears unusual and IMVO believes it requires immediate investigation, IMVO may intervene to request that the end-user and/or MAH take action. IMVO will provide whatever support is required.

IMVO step 2 – IMVO reviews alert after two working days

If IMVO has not received any feedback via *NMVS Alerts* on an alert from the parties involved (i.e., end-user and/or MAH) via *NMVS Alerts* or any other communication channel (e.g. email) within two working days of an alert being generated, IMVO contacts the end-user or MAH (depending on where IMVO considers the most likely root cause of the alert to lie) to enquire if they have identified a root cause for the alert.

- If **YES (i.e. root cause established by either the end-user or MAH)** – go to *IMVO step 1a* or *step 1b* above, as applicable.
- If **NO (i.e. no root cause has established)** – go to *step 3* below.

IMVO step 3 – IMVO requests end-user and/or MAH to investigate alert

IMVO asks the end-user and/or MAH via *NMVS Alerts* to investigate the alert and provides whatever support is required to ensure the root cause can be identified.

If either party fails to provide any essential information or assistance to IMVO, such that IMVO is unable to identify or rule out a root cause on the part of the end-user or MAH, the relevant NCA may be requested by IMVO to intervene with the party involved. Prior to the matter being escalated for NCA intervention, IMVO will make three attempts at specific intervals to engage with the end-user or MAH involved.

If the root cause has not already been identified by the end-user or MAH or they are having difficulty with the investigation, IMVO will proceed to step 4.

IMVO step 4 – IMVO completes investigation of alert

IMVO will utilise the results of its own analysis of the alert and information from other sources including end-users and their software providers, MAHs, EMVO, etc., to complete the investigation. As part of this process, it may be necessary to establish the physical history of the pack, including where it was sourced by the end-user. If IMVO determine that the alert can be explained by a technical issue with the EMVS, a data upload or procedural error or other technical issue, IMVO will ensure that the alert is closed in in *NMVS Alerts*.

IMVO must document the outcome of its investigations via *NMVS Alerts*, and otherwise maintain records and evidence, which will be provided on request to the HPRA.

If IMVO cannot identify a root cause for the alert, the pack is deemed to be a **confirmed falsification** and the next step is to ensure that the HPRA, EMA and Commission are informed (IMVO step 5).

IMVO step 4a – IMVO feedback to end-user and MAH

IMVO will inform the end-user and MAH via *NMVS Alerts* if the alert has been closed and provide any relevant information, e.g., inform the end-user that the MAH has uploaded missing pack data; inform the MAH that an end-user technical or procedural issue was the cause of the alert, etc.

IMVO step 5 – IMVO ensures that HPRA, EMA and Commission are informed of confirmed falsification

IMVO will ensure the HPRA, the EMA and the European Commission are informed as soon as it is clear that the alert cannot be explained by technical issues with the EMVS, the data upload, the person performing the verification or similar technical issues (i.e., the pack is a confirmed falsification) – either by doing so themselves or verifying this has been done by another party such as the MAH.

IMVO will inform EMVO and other NMVOs of a confirmed falsification, unless requested not to do so by the HPRA.

11.2. Systematic monitoring of alert numbers and patterns by IMVO

In addition to overseeing the investigation of individual alerts, IMVO will systematically monitor alerts generated in the IMVS to identify:

i. Products/batches of products that have high numbers of alerts associated with them suggestive of a problem with data upload or product master data. IMVO will contact the relevant MAH to request they investigate the issue and take appropriate corrective action. This should be completed as soon possible and no later than within two working days of IMVO's request. If the matter is not resolved after two working days, the MAH should provide IMVO with a progress update at that point and inform IMVO as soon as the matter is resolved.

ii. 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 repeated procedural errors. Where relevant, IMVO will contact the end-user to request that they investigate the issue and take appropriate corrective action and will provide support if possible.

iii. If the alert type is suggestive of an end-user FMD software issue, IMVO will also check if similar alert patterns are seen with other locations using the same software and contact the relevant end-users and their software provider to investigate and take corrective action. This will resolve all alerts generated by the software issue in those locations.

iv. 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 a short time period due to repeating a decommissioning operation), then IMVO will contact the relevant MAH.

v. 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 either the IMVS, EU Hub (or other NMVS in case of IMT) or a pack synchronisation-related alert. IMVO will liaise with all relevant parties to establish the root cause of the alerts and to ensure that appropriate corrective and preventive actions are taken.

12. 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.

13. IMT alerts

13.1. What is an 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 Ireland for which Ireland was not its originally intended market for sale (in this case, Ireland is the 'initiating market'). When no data is found on the IMVS, 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.

13.2. How can you identify an IMT alert?

An end-user will identify an IMT alert from the fact that the country code in the Alert ID will be something other than 'IE', e.g., 'MT' for packs whose data is held in the Maltese NMVS.

13.3. Are these alerts handled differently?

The process for investigation of IMT alerts is the same as for any other type of alert. If the alert message indicates that the pack has already been decommissioned and you cannot confirm that this was due to procedural error in your pharmacy, please contact IMVO for assistance.

13.4. Who is responsible for investigating IMT alerts?

The investigation of an alert to determine the root cause must be initiated in Ireland where the pack was physically scanned ('initiating market'). 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 (i.e. the market in whose NMVS the data for the pack is held).

The NMVO in the fulfilling market only comes involved in the alert investigation if so requested by IMVO. This may take the form of disclosing contact information for the MAH or providing supplementary information about transactions for those alerts where this information is needed for root cause determination (e.g., 'pack already decommissioned in another location' alert). 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 there is no AMS in the fulfilling market, IMVO will notify the NMVO in the fulfilling market of the outcome of the alert investigation and they are responsible for notifying their NCA if there is a confirmed falsification.

14. Roles and responsibilities

Role	Responsibilities
EMVO	• Ensures that all alerts generated in the EU Hub that are reported to MAHs but not to IMVO are fully investigated. • Provides support to IMVO and MAHs in investigating alerts, particularly where system issues within the EMVS and the EU Hub specifically 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 a technical or procedural error on their part, in accordance with the procedures defined in this guidance. • Provides support as required to IMVO and MAHs in their investigations 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 guidance. • Takes corrective action (where possible, and as soon as possible) where alerts are due to MAH error and provides feedback to IMVO, and where applicable to the end-user, within two working days of the alert being generated, in accordance with the procedures defined in this guidance. • Provides support to IMVO and EMVO in investigating alerts relating to the MAH's products. • Notifies the HPRA of confirmed falsifications. • In the case of centrally authorised products, notifies the EMA of confirmed falsifications.
IMVO	• Ensures that all alerts generated in the IMVS are fully investigated. • Manages IMT alerts in accordance with the procedures defined in this guidance. • Informs the relevant regulator if is not possible to conclude an alert investigation due to an end-user and/or MAH failing to provide the required support/information. • Ensures that the HPRA, the EMA and the Commission have been notified of confirmed falsifications.

15. Reference documents

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 Parliamentand 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
S.I. No. 36 of 2019	Medicinal Products (Safety Features on Packaging) Regulations 2019
S.I. No. 270 of 2022	Medicinal Products (Safety Features on Packaging) Regulations 2022

16. Further information

IMVO: www.imvo.ie

- All alert related queries: alert.support@imvo.ie
- All other MAH queries: mah@imvo.ie
- Tel: +353-1-5715320

European Commission Q&A on Safety Features – available on FAQ section of IMVO website

PSI: Falsified Medicines Directive -Medicines Authentication webpage

HPRA: www.hpra.ie/homepage/medicines/special-topics/falsified-medicines-legislation

- Queries: compliance@hpra.ie
- Tel: +353-1-6764971

Appendix 1: Overview of alerts

Overview of notifications from IMVS

When a pack is scanned, a message is returned by the IMVS to the end-user's FMD software which can be classified as either **'information'** or a **'warning/exception'**. The message that is presented depends on the end-user's FMD software and the nature of the message.

A 'warning/exception' occurs where there is a pack data or pack state mismatch. Some warnings/ exceptions raise an **'alert'**, with a unique **Alert ID**. Some warnings/exceptions need to be acted on, even if they are not alerts. Examples of this include unknown product code or 'pack is expired'. These will be flagged on the end-user's screen.

Depending on the situation that has occurred, there are different levels of warnings/exceptions that can arise:

- **Level 1**: The system can handle the exception itself. The end-user is not notified.
- **Level 2**: The end-user receives a notification about the exception.
- **Level 3**: In the case of an exception generated by an end-user system, IMVO as the IMVS system administrator is notified. In the event of an exception generated by an MAH, EMVO is notified instead as the alert will be seen at EU Hub level.
- **Level 4**: Both IMVO and EMVO are notified about the exception.
- **Level 5**: Level 5 exceptions are referred to as an **alert** and represent a potential falsified medicine. An Alert ID is generated by the IMVS, and all parties notified of the alert receive that Alert ID as part of the alert notification. In addition to the end-user, IMVO and EMVO being informed, the following parties also receive details of Level 5 alerts.
    - **HPRA** – all Level 5 alerts
    - **MAHs** – Level 5 alerts generated in relation to their own products.

Alert codes

The information about an individual alert provided to NMVOs and MAHs includes an alert code that denotes what type of alert has been generated (see table below). There are two different sets of alert codes depending on whether the alert has been generated in an NMVS developed by Solidsoft Reply or an NMVS developed by Arvato[14]. The EU Hub has also been developed by Solidsoft and the same alert codes apply to EU Hub alerts as to Solidsoft NMVS alerts.

[14] The IMVS is a Solidsoft Reply NMVS.

Description	Alert codes in Solidsoft Reply national systems (including IMVS) and EU Hub	Alert codes in Arvato national systems
Batch not found	**A2**	NMVS_FE_LOT_03
Pack not found	**A3**	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.	**A32**	NMVS_NC_PC_02
Pack already in requested status	**A7**	NMVS_NC_PCK_19
Attempt to decommission an already decommissioned pack	**A24**	NMVS_NC_PCK_22
Actual pack status does not match the undo transaction (set and undo status must be equivalent).		NMVS_NC_PCK_06
Status change could not be performed (applies only to IMTs)		NMVS_NC_PCK_27
Expiry date mismatch	**A52**	NMVS_FE_LOT_12
Batch ID mismatch	**A68**	NMVS_FE_LOT_13

Appendix 2: Summary of IMT alert information provided to NMVOs and MAHs

	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 tookplace	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 tothe 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 and 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 lookup 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 is not 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 the role of NMVO in that country or the local NCA, where it is necessary for the NCA to become involved in the investigation.

Figure 1: End-user process flow

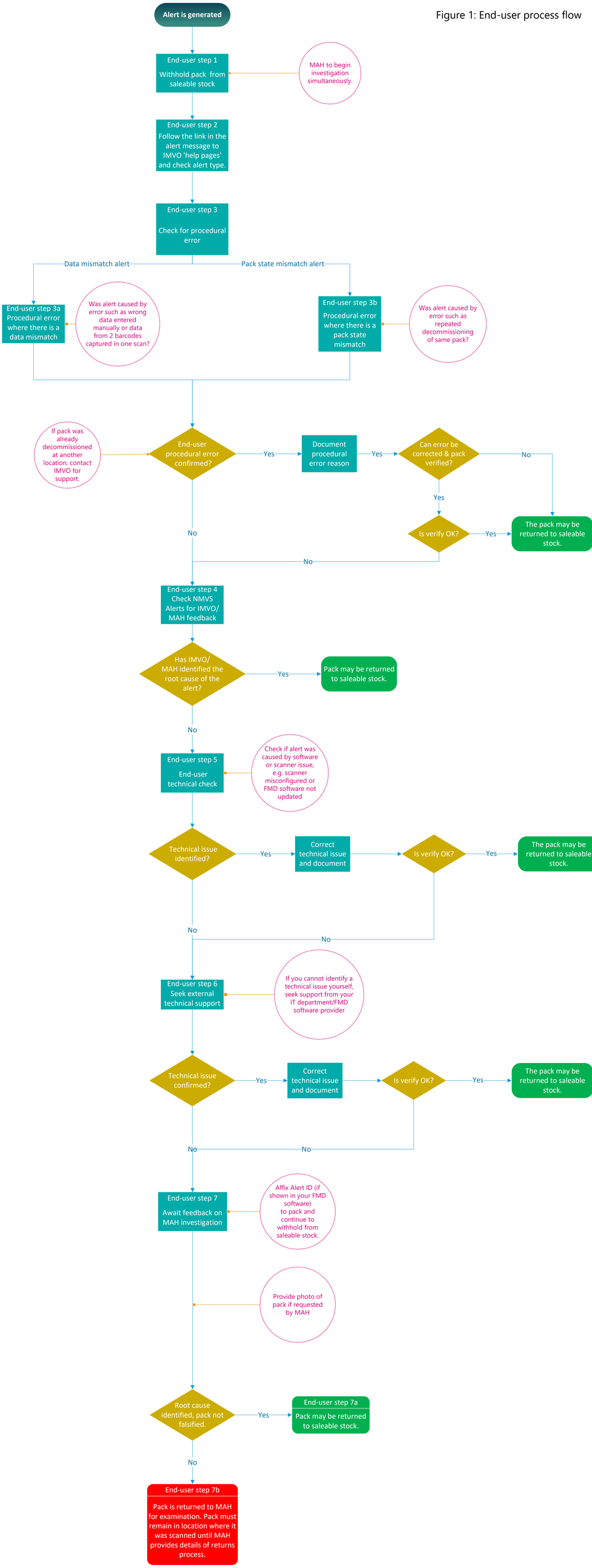

Figure 2: MAH process flow

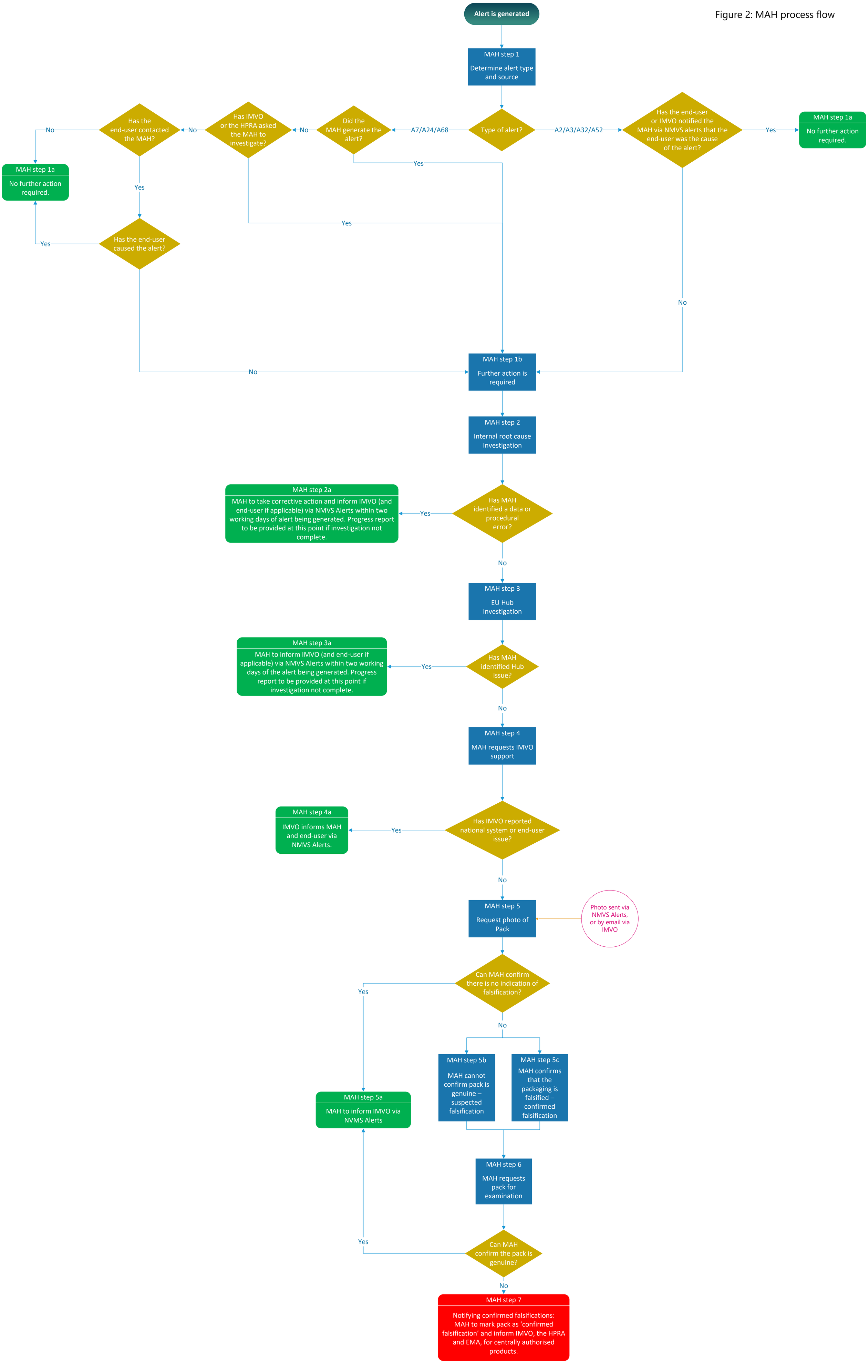

Figure 3: IMVO process flow