Falsified Medicines Directive
Procedure for managing Alerts generated by the verification system

I. PURPOSE

The objective of this document is to clarify the procedures that the different stakeholders, involved in the process of medicines verification, have to follow. Important to note that this version of the document is based on the current set up of the system and agreed procedures. The evolution of the system and future 'real life' practices might lead to updated versions of this document.
The Delegated Regulation and the Q&A of the EU Commission indicate that only a 'verified falsification' needs to be escalated to the relevant National Competent Authority (NCA). This implies that a process is required that excludes all possible technical and procedural causes are excluded before a 'potential falsification' is communicated to the relevant NCA as a 'verified falsification'.
This document describes this process agreed by all stakeholders.

II. ALERTS management

II.1 Accepted and known cases

The following cases are accepted and do not require further process description:

PC	LOT	EXP	SN	Action
Active	Active	Correct	Active	Good Case
Active	Active	**Expired**	na	Batch expired, follow current procedure
Active	**Recalled**	na	na	Batch recalled, follow current procedure
Withdrawal	na	na	na	Product withdrawn, follow current procedure

Good case:
The Product code (PC), the batch number (LOT) and the serial number (SN) are known and active in the system, and the expiry date (EXP) scanned in the 2D matrix is corresponding to the EXP loaded in the verification system.
Other cases:

- the case where the EXP in the system is past current date,
- the case where the batch is marked as recalled in the system,
- the case where the product is marked as withdrawn in the system.

In these cases the current procedures need to be followed.

II.2 Potential falsification cases

The cases where a potential falsification requires further investigation are:

PC	LOT	EXP	SN	Case
Not Found	na	na	na	Product code not found in entire EMVS
Active	**Not Found**	na	na	Batch code not found
Active	Active	**Different**	na	EXP in query is different from NMVS
Active	Active	Correct	**Not Active**	Serial Number is not set to active
Active	Active	Correct	**Not Found**	Serial Number not found

Falsified Medicines Directive
Procedure for managing Alerts generated by the verification system

A potential falsification is defined as:

- The product code scanned from the pack is not found in the verification system
- The batch number is not found in the verification system
- The expiry date in the 2D code on the pack is different from the expiry date loaded in the verification system
- The serial number in the 2D code on the pack is no longer active in the system
- The serial number in the 2D code on the pack is not found in the verification system

For these cases, the Alert handling procedure needs to be applied.
this procedure is detailed in chapter II.3 hereafter.

II.3 Alert handling procedures

The fact that the verification system is returning an alert message does not necessarily mean that the concerned pack is an actual falsification. Other elements, related to the verification process itself, might be the cause of the received alert by the end user.

Potential root causes

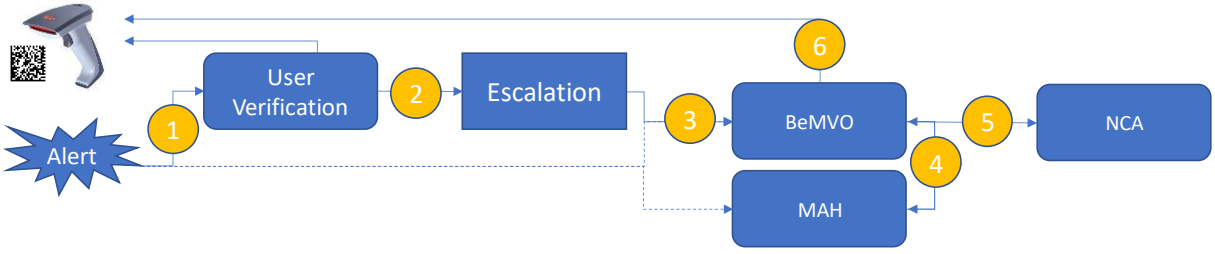
Besides the fact that the concerned pack that is triggering the alert is really a falsification, several other elements, caused by one of the stakeholders, can be at the origin of the received alert.

- USER: error entry by user (scanner not working correctly, wrong manual entry, user's system issue), pack not in scope, …
- MAH (Marketing Authorisation Holder): data not loaded, wrong data loaded, invalid data (not-accepted characters, invalid date), MAH did not further act on rejected files/records, …
- EMVS (verification system): system bug where available data are not correctly retrieved, rejection of not-accepted data and no error message, wrongly applied transactions, …

Therefore it is important that these elements are first checked before escalating the alert to the relevant authorities.

When an alert is triggered, not only the user is receiving the alert message, but that same message is also directed to the concerned MAH (if known, because in case of an unknown product code, the MAH is not identified by the system) and to the BeMVO who is managing the verification system.

In order to avoid unnecessary investigations by the competent authorities where the alert would be caused by an issue at the level of the User, the system or the MAH, the different stakeholders, in alignment with the relevant NCAs of Belgium and Luxembourg, agreed on the following flow.



1. The user receives the alert. The user performs a number of checks to verify if the alert was not triggered by another element than the pack itself, such as an issue with the user's system, error made by the user, … (see list of checks hereafter in section II.4).
2. After verification and no issue is identified at the level of the user, the user confirms that the alert was triggered by the pack and escalates the alert to BeMVO by email (Alerts@bemvo.be) with email subject starting with "ALERT:" as a 'potential falsification'. With this escalation the user provides a set of additional information elements.
   The user keeps the pack aside until a decision is communicated to the user.
3. The BeMVO receives the information from the user (and might request additional information). After reception of the escalation, the user will receive confirmation of reception of the alert from BeMVO. In case the user is located in Luxembourg, LMVO will also be informed about the received alert and information.
4. a) BeMVO checks if the verification system is working properly (see check list hereafter) and if other similar alerts have been received. The BeMVO adds additional information if needed and communicates to the MAH.
   b) The MAH is verifying (see check list hereafter) his production stream (packs) and the different processes used for loading the data in EMVS.
5. Depending on the outcome of these investigations, the MAH or BeMVO (depending on the findings) contacts the NCA when no system issue or pack/data load issue is identified, indicating this raised alert concerns a 'verified potential falsification'. BeMVO is providing the codes needed for the audit trail to the concerned authorities. Also, if these investigations take more than 3 working days to reach a conclusion, the relevant NCA has to be notified of the pending issue.
   The relevant NCA is to provide a decision on next steps, also depending on the category of the incident allocated by the concerned authority.
6. The affected user(s) is informed by the MAH, BeMVO or the relevant NCA (depending on the case) on how to proceed based on the results of the investigation and/or the decision from the relevant NCA.

The different steps in the process need to be executed with the highest priority. The run through time however will depend on the complexity of the research needed to verify if all processes went correctly or if the alert was caused by an issue/error at the level of one of the stakeholders. The response time will also depend on the time required by the competent authorities for further investigation.

II.4 Checklist for USERS

Before escalating the alert, the user needs to check if the alert is not caused by another element. A non-exhaustive list of possible verifications by the end user is:

- **Is the product in scope for FMD in the country?**
  The user needs to verify if the scanned product is in scope for FMD. This can be done based on his internal product database (or other external source file) or by exporting the product list from the verification system. Otherwise, the user might receive many alerts when

scanning medicines out-of-scope that for some reason are also serialized using the same standards.

- **Is the scanner of the user working properly? Is the user's system working as expected?**
  Is the data sent by the scanner to the user's system correct? The user can verify by comparing the scanned with the printed information. He can also verify by scanning-verifying a completely different product and also for that one check if an alert is received and that the scanned data are equal to the printed codes. Such check on a completely different product can also help identifying if any other malfunction in the user's system is causing the alert.
- **In case of a manual entry, was there no typing error made?**
  The user should verify the code he entered. He can re-enter the code and verify is there is still an alert.
  To avoid the case of a wrongly entered Product code (also if scanned), the FMD module in the user's system should always run a check on the check-digit included in the product code.
- **Did the user himself execute an invalid transaction?**
  This can be the case where the user scans and decommission the same pack 2 times. In such case, the message will also indicate if the user had decommissioned the pack himself before or not. If decommissioned by himself, the alert should not be escalated. (if he decommissioned the pack less than 10 days before and the decommissioning was not a Destroy or Stolen, the user can undo the decommissioning if needed).

If no issue is identified at the level of the user, the user needs to escalate the alert and provide a set of information elements to BeMVO. These information elements are required to allow further investigation by BeMVO and the concerned MAH.

Information elements to be provided:

- Product code (GTIN & CNK)
- Product/pack description
- MAH
- Element that caused the alert (product code, batch, …)
- Scanned Batch, EXP & SN data
- Printed Product Code, Batch, EXP & SN data – if different from the scanned information

II.5 Checklist for MAHs

With reception of the alert ticket and the information from the user and BeMVO, the concerned MAH needs to start immediately the investigations on his side. The MAH should perform the investigation in close collaboration with the Qualified Person of the manufacturer responsible for affixing the unique identifier on the pack.
The escalation will go to a dedicated person at the MAH with a backup person in copy.

Depending on the type of escalated alert, following potential root causes of the alert need to be investigated by the responsible MAH (non-exhaustive list):

- Verify if the product code was loaded for Belgium
- Verify if any error messages were received at the load; if yes, were they properly managed?

- Have there been update loads of the product information and what is the current product version number in the system?
- Verify if the batch was loaded; was the batch loaded with the correct batch number?
- Was the expiry date loaded with the batch correct?
- Is it still the initial batch upload in the system or have there been batch data updates loaded subsequently? Were these change loads successful?
- Have (all) the pack data been loaded?
- Were there any error messages, were certain (or all) codes rejected (double codes, rejected records e.g. for use of special characters, …) and have these error messages been managed correctly?
- Verify the physical pack and compare the printed and 2D information with the load files
- Check if similar alerts for that product were received in other countries
- …

The MAH needs to communicate his findings to the BeMVO (email) and/or further align with the investigations done by BeMVO.

II.6 Checklist for BeMVO

In parallel with the investigations being done by the MAH, BeMVO will also further verify if any issue in the verification system could be the potential cause of the triggered alert.

Depending on the type of escalated alert, following potential root causes of the alert need to be investigated by the BeMVO:

- Check if other alerts from other users for the same case have been triggered in the system
- Check if an atypical high number of alerts were triggered by that same user
- Check the overall status of triggered alerts compared to historical data
- Check if any error messages (rejected files, records, …) were recorded in the system for the different loads related to the alert element(s)
- Check any technical issues with the system (system performance, …)
- …

II.7 Escalation to the National Competent Authority (NCA)

BeMVO will align with the concerned MAH about the findings on both sides.
If no issue or error was identified at the level of the user, the verification system or the MAH, then the alert can be considered as a **Verified Potential Falsification**.

For Belgium, all relevant information is escalated to FAGG/AFMPS by email to RapidAlert@fagg.be / RapidAlert@afmps.be

For Luxembourg, all relevant information is escalated to “Direction de la Santé - Division de la Pharmacie et des Médicaments” (“DPM”) by email to fmd@ms.etat.lu

III. Post-investigation actions and decision process

The "Verified Potential Falsification" is escalated to the authorities with all relevant information that was received from the user and the outcomes of the investigations by BeMVO and the concerned MAH.

After further investigation, the relevant NCA will discuss and communicate the decision to BeMVO and the concerned MAH.
MAH, BeMVO or the NCA (depending on the case and expected action) will provide the appropriate information to the concerned user(s).

Version 1/10/2018