Falsified Medicines Directive

FMD error and alert messages guidance notes

To accompany "FMD – scanning and alert messages" chart (v7)

December 2018 – UPDATED GUIDANCE

These guidance notes accompany the "FMD – error and alert messages (for pharmacy and wholesale)" chart (v7) and are based on a workshop held at Walgreens Boots Alliance, Weybridge, on 5th September, subsequent discussions with relevant experts, and feedback from stakeholders. The chart looks specifically at handling of alert messages, focusing on those with "pack in hand" and is intended to inform wider discussions on implementing FMD, including amending Standard Operating Procedures. It will link with other industry guidance on the handling, return and assessment of suspect packs after a "red" (Level 5) alert has been raised and professional guidance on ethical decision making related to FMD.

NOTE: This is a working document and will be updated in light of feedback and experience. It represents current thinking on these issues at this point. Comments and feedback are encouraged. A further version will be issued after FMD goes live to incorporate real-world feedback.

ANTI-TAMPERING DEVICES: All packs bearing safety features will also require their anti-tampering devices (ATDs) to be visually examined before decommissioning. The normal (positive) response assumes that each pack has passed. If operators suspect that packs have been tampered with then they are required to report this to the National Competent Authority (ie, MHRA) in the same way as for a pack that fails a verification or decommissioning scan. See section on "Handling packs that generate alerts".

TERMINOLOGY: An **alert** is a message generated by a response from the NMVS following a scan of a unique identifier. A **warning** is a message generated by a local system. The chart and this guidance captures the main categories of alert (grouped together) and the actions required by end users.

SYSTEM ISSUES: There are a large number of alerts related to the way in which the NMVS operates internally, not all of which are passed to end users. Some are condition-specific (eg, unable to reverse decommissioning after 10 days). These are outside the scope of this guidance. Users should contact their system suppliers, local IT helpdesk or NMVO helpdesk for more information and support if they receive any of these messages.

RETURNS: Products that fail verification or decommissioning should be returned **only when this is specifically requested** as part of a recall or returns process initiated and reimbursed by a manufacturer or NCA.

Products that cannot be verified for reasons not related to FMD (eg, they are out-of-scope for FMD or are older pre-FMD packs without the full set of safety features) **should not be returned to wholesalers** just because they give a negative or "unknown product" alert. Since they will not qualify as returns then they will be destroyed and credit will not be provided. In general, such products can still be dispensed or supplied in line with pre-existing procedures and guidance. See "Not FMD or fails to scan (Amber)" section below.

Positive scan (Green)

It is assumed that the vast majority of all stock being verified and/or decommissioned will produce a positive response from the NMVS. The aim of the process should be to minimise the response or action to be taken by end user operators. There should be a positive confirmation that a scan has taken place (single "beep") in line with other automated processes (eg, supermarket self-checkouts).

Local systems should display a list of all products that have been scanned along with the product details (name, strength, form, etc) derived from the full data product master data, as well as batch, expiry and serial numbers. This should be enabled as the default setting by the NMVO. The most recently scanned product should be at the top of the list displayed by the local system to the end user to enable checking in case an operator is distracted or has to break off from scanning. Preferably there should be at least one screen or display per operator.

The status of the product (and the confirmation of any change of status at decommissioning) should be indicated in the list (using symbols [✓] and colours that are unambiguous) as and when the response is received from the NMVS. This information should be stored in local data audit trails.

When scanning or verifying large numbers of packs, especially in wholesale settings, local systems may also be pre-configured to request or prompt the number of packs to be scanned and indicate when this has been reached.

Scanners and local systems should be set to recognise both "black on white" and reversed "white on black" (or other dark colour) 2D data matrix coding and be able to extract UI data from them.

Not FMD or fails to scan (Amber)

A wide range of products will not require verification or authentication under FMD at any time. This includes non-prescription products, medical devices, non-medicines, specials and other out-of-scope items, as well as POM stock produced and released before 9th February 2019 which do not carry unique identifiers. Local processes and guidance should make it clear that these products can still be dispensed and **do not have to be returned to wholesalers or suppliers** (unless there is some other problem, not related to FMD, that makes this necessary).

Ideally, local systems should be able to distinguish between "right" (FMD) and "wrong" (not FMD) stock by drawing on NMVS master data loaded on to local systems. This would allow a process of "scan everything, system sorts it out". Whenever possible there should be a positive audible confirmation that a scan has taken place.

Where this is not technically possible then end user operators should have access to visual training guides that distinguish between "right" and "wrong" products in order to minimise scanning errors. Draft guidance is available on FMD Source (www.fmdsource.co.uk) and may also be provided by other bodies, including end user organisations, systems suppliers, NMVOs and trade associations.

Excessive "amber warning" pop-up boxes saying that certain packs do not need to be verified should be avoided in case they cause operator alert fatigue.

Some products may fail to scan because of damage to the 2D data matrix. SOPs should indicate that a lack of audible confirmation should prompt the process for manual data entry. In general, damaged packs should be a rare occurrence. Where a product is expected to be FMD-compliant but has multiple packs that fail to scan, this should be reported to the wholesaler, supplier or NCA as a defective medicine using existing procedures.

NOTE: See "data error" red alert for packs that do scan but contain incorrect data.

Warnings generated by local systems (Red)

These warnings can be generated in response to data held within a unique identifier 2D data matrix (eg, expiry data) or in response to end user operator actions (eg, double scans of same pack). They do not require a live connection to the NMVS at the time of scanning to generate a warning, however, the NMVS will also generate an alert message, if the data is sent on to the NMVS, when or if connected.

Out of date As a minimum, local systems should warn operators about products that have passed their expiry date by cross-referencing with calendar date. It would be preferable and a major benefit for systems to also warn about products that are close to their expiry date (eg, less than three or six months or another user-defined period). Local system suppliers may decide to filter out-of-date warnings and not to send information on to the NMVS.

Double scan A double scan occurs when the same pack is scanned more than once at the same location, often in quick succession. Agreement should be reached with system suppliers and the NMVO on how many repeated scans, and how frequently, is an acceptable limit.

Local systems should capture and warn operators about this, requiring an acknowledgement. Local limits should be agreed after which operators' local management is alerted (to prompt training or process improvement). Local system suppliers may decide to filter double-scan warnings and not to send information on to the NMVS.

If a national limit is to be set on the number of double scans permitted before an alert is raised with the NMVO (and/or NCA) then this should be set at a very high level for the initial phase following the start of FMD authentication. This will avoid swamping the system with unnecessary alerts. The permitted level could be reduced in due course once experience is gained across the supply chain.

Alerts generated by NMVS (Red)

These alerts are generated when UI data from packs is compared with the data and status information held on NMVS. They require a live connection to the NMVS.

Recalled pack The status of the pack in the NMVS is set to "recalled" or "withdrawn". This may be at a pack or batch level. In these circumstances end users should follow existing procedures for the return or disposal of affected packs, including processes for reordering and reimbursement/refunds.

Status error The status of the pack in the NMVS is set in such a way that the product cannot be decommissioned and supplied. This includes packs marked as "stolen", "sample (not for commercial sale)", "free sample", "exported from EU", "for destruction" or "checked-out" (part of the parallel import process). These indicate packs that should not be in circulation in the supply chain and should not be supplied or dispensed. See below for guidance on handling these packs. A status of "clinical trial supply" may be added to this list in future. See also "undoing actions" section below.

Data error The data on the pack does not match corresponding data held in the NMVS or the data on the pack has gaps or missing fields (ie, missing one or more of serial, product, batch, expiry or national reimbursement number, where relevant). This also includes packs where data is encoded using formats or characters that are not permitted by EMVO or other relevant authorities (eg, GS1). Manufacturers are expected to scan all 2D data matrix codes as they are produced to avoid such errors. Improper coding may indicate falsified packs. See below for guidance on handling these packs.

Data errors may also occur if packs are released to market before data uploads to EMVS are successfully completed. Pre-emptive verification scanning prior to dispatch (at least one pack per batch) by manufacturers or their logistics agencies, or by wholesalers or pharmacies on receipt, is not mandatory but would help reduce the chances of large numbers of such packs reaching end users.

Batches of products with large numbers of packs that return data error alerts should be reported to the NMVO and NCA as defective medicines.

Already used The UI data is correct but the status indicates that it has already been decommissioned at another location, either in the same country or in another country. This could indicate duplication of UIs and potential falsification. This is different to the "double scan" error which only occurs when packs are re-scanned at the same location. See below for guidance on handling these packs.

Locked packs Packs can have their status set to "locked" on a temporary basis. Only manufacturers and wholesalers can do (and undo) this. There is no 10-day rule on reversing locked status. However, since dispensing entities cannot undo locked packs they would be unable to dispense them. For this reason, packs should only be locked electronically after they have been physically locked up (quarantined). Those doing the locking should have "pack in hand" at the time. It should never be used for packs that are in transit or which have been widely distributed. If packs are not in the possession of the person wishing to lock them then the recall route should be used instead.

Undoing actions Some actions cannot be undone (eg, marking packs as "stolen" or "for destruction"). There should be an additional confirmation step, preferably using the entry of a one-time code, before such actions, applying to a single or bulk action as appropriate. Other actions can only be reversed within specific conditions (eg, at the same physical location, within 10 days of the first action, by the same class of end user). System issue alerts relating to these actions will be context-specific. Alerts will arise, for example, if an end user incorrectly tries to reverse a previous decommissioning action.

Handling of packs that generate alerts (Red)

Packs marked "recalled" or "withdrawn" should be handled in the normal way for return or disposal, including reimbursement/refunds.

Packs with "status error", "data error" or "already used" alerts need to be quarantined, reviewed, reported and, if required, handed over to manufacturers or NCA inspectors for examination. They should **not be returned to wholesalers**, unless this is specifically requested as part of a recall or return process initiated and reimbursed by a manufacturer or NCA.

Quarantine Suspect packs should be physically quarantined away from normal stocks. Where possible and practicable, suspect packs should be placed in separate plastic bags and labelled with relevant details, including the alert ID number raised by the NMVS.

Internal review An initial internal review should be conducted by a suitable person within the organisation, such as a Qualified Person, Responsible Person (wholesale) or Responsible Pharmacist or Pharmacy Manager (community pharmacy) to rule out any technical or procedural issues, including double scanning or undertaking incorrect actions. Senior managers, such as Chief Pharmacists, Superintendent Pharmacists, Operations Directors, or GP practice partners, should be informed of the outcome, as appropriate. This is not an investigation to determine whether a product has actually been falsified, as this will be carried out by the manufacturer or NCA, if required. The organisation may wish to contact their supplier, the Marketing Authorisation Holder (MAH) or its local affiliate, or the NMVO for further guidance at this point.

External reporting Although the NMVS will generate a report that can be accessed by the NCA, wholesalers and dispensing entities have a duty placed on them by the Delegated Regulation (2016/161, Articles 18 & 30) to report suspected falsification incidents. In the first instance, this should be done through a suitable portal provided by the NCA (such as the Yellow Card scheme in the UK) following appropriate guidance. The NCA should make available and publicise a hotline line for urgent incident reporting. NCAs should indicate publicly, in due course, when they are ready to move over to electronic-only reporting, relying on alerts and reports generated by the NMVS, removing the need for end users to make individual reports.

Analysing packs When requested by MAHs or their On Boarding Partners (OBPs) and/or NCA inspectors, suspect packs should be supplied to them for further analysis. It is up to MAHs to make suitable arrangements with the person holding the pack for its return. Persons returning packs should receive appropriate reimbursement for the cost of the pack and any relevant out-of-pocket expenses incurred from the MAH (or NCA, if they have taken possession of the pack), or via a credit from their wholesaler. The NCA should indicate to the person supplying the suspect pack when or if they might receive any feedback on the investigation, whether directly or through a more general update.

NOTE: Work on a pathway for MAHs and OBPs for handling alerts and analysing suspected falsification incidents is being undertaken by the European Federation of Pharmaceutical Industry Associations (EFPIA) and Medicines for Europe (MfE). This will connect with the “Packs for investigation” route on the “FMD – error and alert messages” chart.

Guidance notes prepared by:

Jonathan Buisson MRPharmS MFRPSII
International Pharmacy & Policy Manager
Walgreens Boots Alliance
(jonathan.buisson@wba.com)

Last updated: 18th December 2018

Further reading

Naughton B, Roberts L, Dopson S, Chapman S, Brindley D. Effectiveness of medicines authentication technology to detect counterfeit, recalled and expired medicines: a two-stage quantitative secondary care study. BMJ Open. 2016 Dec 1;6(12):e013837.

Naughton B, Roberts L, Dopson S, Brindley D, Chapman S. Medicine authentication technology as a counterfeit medicine-detection tool: a Delphi method study to establish expert opinion on manual medicine authentication technology in secondary care. BMJ Open. 2017 May 6;7(5):e013838.