FiMVO

Suomen Lääkevarmennus

Verification processes in the supply chain

Workshop for MAHs, Helsinki, 18 Sep 2018

Teijo Yrjönen, FiMVO

FiMVO
Suomen Lääkevarmennus

Legislative background

- Directive 2011/62/EU (Falsified Medicines Directive)
- Commission Delegated Regulation (EU) 2016/161
- Falsified Medicines Directive will be implemented in the Medicines Act in Finland

FiMVO
Suomen Lääkevarmennus

Legislative background

Requirements for:

1) manufacturers (MAHs),
2) wholesalers,
3) persons authorised or entitled to supply medicinal products to the public (pharmacies, hospital pharmacies, dispensaries),
4) legal entities establishing and managing a repository which is part of the repositories system (national medicines verification organizations, NMVOs)
5) national competent authorities (NCAs)

FiMVO
Suomen Lääkevarmennus

Legislative background

Obligations of manufacturers

- Placing unique identifiers (UIs) and anti-tampering devices (ATDs) on the packaging of (prescription) medicinal products
- Uploading the UIs to the repositories system before the medicinal product is released for sale or distribution by the manufacturer

Obligations of wholesalers

- Verification of the UIs of medicinal products 1) returned to the wholesaler by pharmacies or other wholesalers and 2) received from wholesalers who are not manufacturers or MAHs of the products or wholesalers not designated by MAHs
- Decommissioning of the UIs of medicinal products 1) intended to be distributed outside EU, 2) returned to the wholesaler by pharmacies or other wholesalers which cannot be returned to saleable stock, 3) intended for destruction, 4) requested as a sample by competent authorities and 5) intended to be distributed to veterinarians

Legislative background

Obligations of persons authorised or entitled to supply medicinal products

to the public (pharmacies, hospital pharmacies, dispensaries)

- Verification of the safety features and decommissioning of the UI of any medicinal product bearing the safety features they supply to the public
- Verification of the safety features and decommissioning of the UI of any medicinal product 1) that cannot be returned to wholesalers or manufacturers, 2) are requested as samples by competent authorities, 3) which they supply for subsequent use as authorised investigational medicinal products or authorised auxiliary medicinal products

FiMVO
Suomen Lääkevarmennus

Legislative background

Obligations of legal entities establishing and managing a repository which is part of the repositories system

- Informing the relevant NCAs of the intention to physically locate the repository or part of it in their territory and notify them once the repository becomes operational
- Putting in place security procedures ensuring that only users whose identity, role and legitimacy has been verified can access the repository or upload the information
- Monitoring the repository for events alerting to potential incidents of falsification
- Providing for the immediate investigation of all potential incidents of falsification flagged in the system and for the alerting of NCAs, EMA and the Commission of confirmed falsifications
- Carrying out regular audits of the repository
- Making the audit trail immediately available to NCAs upon their request
- Making the reports available to NCAs upon their request

How verification changes supply chain processes

- Changes in the internal company/corporate procedures for all parties due to the legislative requirements described on previous slides

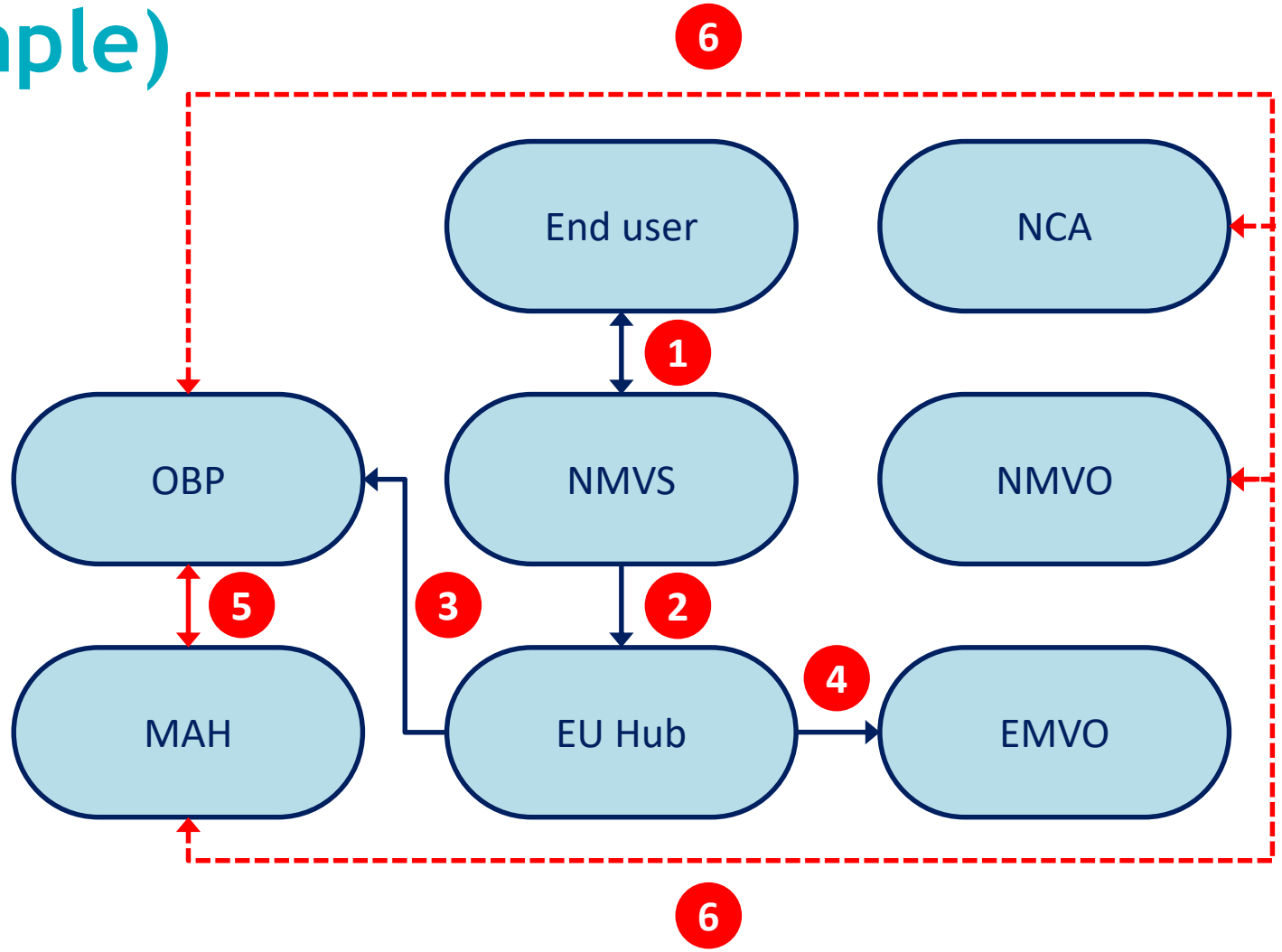
Specific points to consider:

- Manufacturers: cooperation between OBP and MAHs, as well as with NCAs and NMVOs
- Wholesalers: possible additional verification of batches received from approved suppliers
- Pharmacies: reporting requirements of *suspected* falsifications to NCAs, contact details of MAHs
- Hospital pharmacies: how, when and by whom to decommission the medicinal products
- Interplay between the parties in case of exceptions and alerts (!) > who, what, how, when…?

Alert handling (example)

1. End user scans a pack > authentication fails > end user IT system gives an alert
2. EU Hub receives the alert from NMVS
3. OBP receives the alert via EU Hub
4. EMVO receives the alert via EU Hub
5. OBP / MAH investigates > alert explained by technical / data upload / human issues?
6. OBP / MAH notifies NCA and NMVO of the alert (if cannot be explained by any human / system error)
7. MAH / Manufacturer investigates the suspected falsified pack as requested by OBP

Blue arrows > System-to-system messages, red arrows > communication outside EMVS



Alert handling (example)

- What to report to NCA?
  - Only confirmed falsifications (DR 2016/161, Art. 37(d)) > it should, however, be noted that the end user is required to ”*immediately inform the relevant competent authorities*” if “*the verification of the safety features of the medicinal product indicates that the product may not be authentic*” (DR 2016/161, Art. 30)
- When to report to NCA?
  - Once any technical / data upload / human error has been ruled out > it should be noted that potential falsifications are treated as class I product defects
- Who should report to NCA?
  - NMVO responsibility but the task may be delegated (DR 2016/161, Art. 37(d) and Q&A v10, 7.17) > requires always input from OBP / MAH > a practical solution would be that OBP / MAH reports to NCA and NMVO if the falsification is confirmed

Alert handling (example)

Practical questions

- Communication channel(s) between pharmacies and MAHs? > Tamro's Tuovi and Oriola's OriolaPro,…? > need for common agreement on procedures, testing of the procedures, MAHs ready and willing to test the alert procedure?
- Need for alert handling before 9 Feb 2019?
- Role of FiMVO in alert handling?
- Will there be a Fimea Administrative Regulation available before 9 Feb 2019?
- …