Questions and Answers about securPharm for Pharmaceutical Companies

The FAQ collects questions addressed to securPharm e.V. by pharmaceutical companies or their service providers. The answers are not legally binding but represent the opinions and the state of knowledge of securPharm e.V. at the time they were generated.

The term *marketing authorisation holder (MAH)* or *pharmaceutical company* describes a company or another legal entity that has an authorisation for marketing a pharmaceutical in one, several or all member states of the European Union.

For questions regarding the implementation of the Falsified Medicines Directive and connection to the securPharm system, pharmaceutical companies may contact ACS PharmaProtect GmbH (ACS), the operator of the database system of the pharmaceutical industry, at info@pharmaprotect.de.

Change log

Current version 2021-03-31 securPharm FAQs pharmazeutische Unternehmen v4	As of: 31 March 2021
Previous version 2020-09-02 securPharm FAQs für pharmazeutische Unternehmen v3	As of: 2 September 2020
Changes compared to the previous version	New: 6.16 Changes: 1.2, 2.1, 2.2, 2.7, 2.8., 3.1, 4.1, 4.5, 5.2, 5.7, 6.6, 6.10, 6.12, 6.13

1. General questions

1.1: Who is securPharm e. V.?

securPharm e. V. is the German organisation for the authentication of pharmaceuticals and responsible for operating the authentication system for prescription drugs pursuant to the requirements of the Falsified Medicines Directive and the Delegated Regulation. The organisation is sponsored by ABDA, BAH, BPI, PHAGRO and the vfa. securPharm e. V. is the German component in the EU-wide network EMVS against falsified pharmaceuticals.

1.2: How do pharmaceutical companies connect to the securPharm system?

The database system of the pharmaceutical industry (MAH system) is operated by ACS PharmaProtect GmbH (ACS). Pharmaceutical companies (marketing authorisation holders: MAH) that launch pharmaceuticals in the German market, which must bear the new safety features pursuant to Delegated Regulation (EU) No. 2021/161, connect to securPharm via ACS. If you are interested in participating, please contact the company directly at info@pharmaprotect.de.

1.3: Who is ACS PharmaProtect GmbH (ACS)?

ACS is the operating company for the database system of the pharmaceutical industry (MAH system) and therefore part of the data repository and access system in securPharm's responsibility, which is required by Delegated Regulation (EU) 2016/161 for implementation of the Falsified Medicines Directive. The managing partners of ACS are the pharmaceutical associations BAH, BPI, Pro Generika and vfa.

2. Contracts

2.1: Why do I need a contract with ACS PharmaProtect GmbH (ACS)?

The complete pack data, which remain in the possession of the marketing authorisation holders, are stored in the database system of the pharmaceutical industry (MAH system) for the German market and are retained for the verification at the pharmacy. Each pharmaceutical company that launches pharmaceuticals subject to mandatory verification in the German market must upload its pack-related data via the EU Hub.

2.2: Who is the contractual partner of ACS PharmaProtect GmbH (ACS)?

For each pharmaceutical company which has a drug in its portfolio that is to bear the new safety features in accordance with Delegated Regulation (EU) 2016/161, a connection to the database system of the pharmaceutical industry (MAH system) is required. Please contact ACS directly to connect (info@pharmaprotect.de).

Membership in an association is not a prerequisite. The contractual partner of ACS indicates the IFA provider number (address number) as the $\mathrm{MAH\ ID}$ with a maximum of 5 digits as part of the master data upload via the EU Hub. This is explained in the [EMVS Master Data Guide](#), which is provided by the EMVO.

2.3: Can I conclude a contract with ACS PharmaProtect GmbH (ACS) jointly with my subsidiary?

No, this is not possible if the subsidiary releases pharmaceuticals in Germany on its own responsibility. ACS individually concludes a separate agreement with each marketing authorisation holder.

2.4: Can I, as a contract manufacturing organisation (CMO), conclude a contract with ACS PharmaProtect GmbH (ACS)?

ACS only concludes an agreement with pharmaceutical companies that market their medicinal products in Germany. Companies that only act as contract manufacturing organisations will therefore be unable to conclude a contract with ACS. However, the CMOs can and must be included in the serialisation process by their clients. If you are a CMO, please talk to your client about this.

2.5: Who bears the responsibility for connecting to the securPharm system?

The marketing authorisation holder is responsible for the implementation of processes within the pharmaceutical company and the connection to the securPharm system and the EU Hub.

2.6: What is the cost of participation in securPharm e.V. and what is the composition of these costs?

ACS PharmaProtect GmbH (ACS) has developed a fee model that also takes into account the concerns of small and medium-sized companies. The fee model of ACS PharmaProtect GmbH is based on a one-time set-up fee and a fee that is calculated based on annual turnover and the sales of the respective company's pharmaceuticals that are subject to mandatory verification. Additional information can be obtained from ACS (info@pharmaprotect.de).

2.7: How do the data get into the ACS MAH system?

ACS concludes an agreement with the pharmaceutical companies. As part of the master data upload and the product data upload via the EU Hub, the ACS MAH system adopts the provided data.

2.8: What must pharmaceutical companies do before being able to connect to ACS PharmaProtect GmbH (ACS)?

The Delegated Regulation (EU) 2016/161 requires a legitimacy check for pharmaceutical companies before they can connect to the national database. As a result, ACS is obligated to check the identity, role and legitimacy of each user. As part of the legitimacy check, ACS requests the required documents.

ACS individually concludes a separate agreement with each marketing authorisation holder.

2.9: Are there any additional contracts the marketing authorisation holders must conclude?

To use the entire European verification system, pharmaceutical companies must conclude a contract with the operator of the EU Hub. This is independent of whether they market their pharmaceuticals in just one or several EU member states. The EU Hub is operated by the European Medicines Verification Organisation (EMVO). Additional information is available at www.emvo-medicines.eu.

If companies market affected pharmaceuticals in additional EU member states, said companies will need a contract with the respective national organisation, the so-called National Medicines Verification Organisation (NMVO), for the data repository and access system. For an overview of all NMVOs, please visit https://emvo-medicines.eu/mission/emvs/#countries.

2.10: Do I need a contract with ACS PharmaProtect GmbH (ACS) if I have concluded a contract with the EMVO?

A contract with ACS is nonetheless necessary, because the MAH system stores the serial numbers that are uploaded by the marketing authorisation holder via the EU Hub for the verification and deactivation in Germany. The set-up and further development of the EMVO system is additionally financed with funds that the marketing authorisation holders pay to the national medicines verification organisations.

3. Reporting to IFA

3.1: What data do marketing authorisation holders have to report to Informationsstelle für Arzneispezialitäten – IFA GmbH?

For a successful verification, it is necessary that the pharmaceutical company/supplier report to *Informationsstelle für Arzneispezialitäten* – IFA GmbH the two so-called verification marks for each PZN affected by the Falsified Medicines Directive: *Verification during Mandatory Operation from Date of Upload* and *Verification during Mandatory Operation from Date of Expiry* (see also www.ifaffm.de). In doing so, the IFA reporting deadlines must be observed. With a correct and complete notification, the marketing authorisation holder/supplier creates a(nother) necessary

prerequisite for merchandise subject to mandatory verification to be recognized as such, for the verification to be conducted successfully and for existing merchandise to be dispensed without obstruction.

For additional information regarding reporting to IFA, please consult the [FAQs](#) of IFA.

4. Area of applicability

4.1: Which pharmaceuticals are affected by the Falsified Medicines Directive?

The Falsified Medicines Directive applies to pharmaceuticals that are prescription-only and are not subject to the exceptions pursuant to Annex I of the Delegated Regulation (EU) 2016/161 as well as OTC drugs that are listed in Annex II of the Delegated Regulation. It must be noted that what is considered an OTC drug in Germany may be a prescription drug in other EU countries.

4.2: Can pharmaceuticals that are neither prescription drugs nor included in the Black List bear the unique identifier?

No. Affixing a Data Matrix Code to the package of pharmaceuticals that do not bear the safety features is only allowed if the Data Matrix Code neither contains the unique identifier nor serves the purpose of identification of the pharmaceuticals and as long as the requirements of EU Directive 2001/83/EC Title V are met. Based on the information currently available, this requirement is met if the Data Matrix Code does not include a serial number.

4.3: Can pharmaceuticals that are neither prescription drugs nor included in the Black List voluntarily bear the anti-tampering device?

Yes. This was jointly announced by the German Federal Institute for Drugs and Medical Devices (BfArM) and the Paul Ehrlich Institute (PEI) on 11 April 2017.
https://www.pei.de/SharedDocs/bekanntmachungen/2017/banz-vorabveroeffentlichung-bekanntmachung-pei-bfarm-anti-tampering-device.html. The German Institute for Standardisation has passed the DIN EN 16679:2015-03 standard for the anti-tampering device.

4.4: Do the safety features also apply to pharmaceuticals that are manufactured for research and development purposes?

No, they do not apply to pharmaceuticals that are manufactured for research and development purposes and do not yet have a marketing authorisation.

4.5: What is the procedure for physicians' samples?

Physicians' samples pursuant to Article 96 of Directive 2001/83/EG must also bear the safety features according to the Delegated Regulation (EU) 2016/161 (Articles 2 and 41). The pharmaceutical entrepreneur generates the serial number during the packaging process and uploads it to ACS' database system of the pharmaceutical industry via the EU Hub. Before the pack is dispensed to the physician, the pharmaceutical entrepreneur deactivates the serial number with the status "physicians' sample". This way, he ensures that this pack cannot be dispensed somewhere else. Physicians' samples can be packs taken from the production of retail packages, which are subsequently labelled as physicians' samples. The PZN of the product in question remains unchanged. Alternatively, specific packs with a separately assigned PZN can be produced exclusively for use as physicians' samples. Companies can apply for a PZN for the separate article type "physicians' sample pursuant to the German Medicinal Products Act" with Informationsstelle für Arzneispezialitäten GmbH (IFA). In principle, it is recommended to also apply the PZN in clear text to the physicians' sample pack, since this makes handling and documentation easier at the doctor's office.

4.6: Do these provisions also apply to veterinary pharmaceuticals?

No, the provisions only apply to medicinal products for human use. For questions about veterinary pharmaceuticals or for suspected falsifications of veterinary drugs, please contact *Bundesamt für Verbraucherschutz und Lebensmittelsicherheit* – BVL (Federal Office for Consumer Protection and Food Safety) or the source from which the drug was obtained, i.e. the veterinarian or the pharmacy.

5. Coding

5.1: Who generates serial numbers (SN)? What regulations apply?

The generation of a serial number is the responsibility of each individual marketing authorisation holder. However, certain requirements must be met that are laid out in the securPharm Coding Rules entitled "Coding Rules for Medicines requiring Verification for the German Market". The document can be viewed or downloaded from the securPharm website at https://www.securpharm.de/codierung/.

5.2: How do the software systems of wholesalers, pharmacies and hospitals know that a pharmaceutical is subject to mandatory verification?

During the market launch, the marketing authorisation holder must report the fact that a product is subject to mandatory verification to Informationsstelle für Arzneispezialitäten GmbH (IFA). To do so, the regulations and editorial deadlines of IFA GmbH must be observed, so that the label will be available on time for transmission to the software information systems (see also 3.1).

5.3: Is the information sequence in the Data Matrix Code mandatory and how can we save space based on a certain arrangement?

The sequence of the data elements is discretionary. Based on the data designators, the interpretation of the data string is unambiguous. If a data element with variable length is placed last in the data string, no separator is needed (based on the GS1 specifications, the separator can be omitted anyway after fixed-length data elements).

5.4: What is the difference between the various product number versions?

The PZN, which is required for pharmaceutical packs in Germany, can be enveloped by the NTIN as well as the PPN. Both product number versions can be used without obstruction. What should be noted are the different data designators and differences in syntax (headers, separators). Use of the PPN (IFA GmbH) is generally free of charge. As far as the use of an NTIN is concerned, GS1 Germany should be contacted. (From a technical point of view, an NTIN corresponds to the GTIN.)

5.5: Is it required to print the PZN barcode (Code 39) in addition to the Data Matrix Code?

Since 9 February 2019, it has been allowed to represent the PZN exclusively in machine-readable form in the Data Matrix Code (DMC). If Code 39 is omitted, the PZN is to be affixed in clear text with the short designation "PZN".

5.6: Is it possible to have multiple codes on a single package?

The Delegated Regulation allows affixing additional one- or two-dimensional codes to the package, as long as they are not used for verification of the pharmaceutical pack. If multiple codes are affixed to a pack, it is required pursuant to the securPharm Coding Rules Version 2.04a that the PPN emblem be affixed directly next to the Data Matrix Code to be verified.

5.7: Where do I find information about the anti-tampering device?

The anti-tampering device is a protective instrument against manipulation which makes it apparent when a package has been initially opened (tamper verification). Information regarding the various options is provided by international standard EN ISO 21g76:2020, which replaces the previous European standard DIN EN 16679:2015-03.

6. Handling of alarms

6.1: What is an alert in the securPharm system?

If the match of a pharmaceutical pack with the dataset stored in the MAH system cannot be confirmed, the securPharm system will issue a so-called alert. For each alert, it must be investigated whether it was a false alarm, e.g. based on handling errors or technical errors, or if a falsification is suspected.

6.2: How can alerts be classified?

Each alert is labelled with an alert ID, which is uniform on a Europe-wide scale and based on which the affected system participants can view the classification status of any given conflict. The alert ID starts with the national code of the country where the alert was generated (e.g.: DE-d83c3187-3107-4de0-bc52-77a0e452574f).

6.3: What alerts are generated?

The fundamental definition of an alert is stipulated in Article 36 lit. b of the Delegated Regulation. Furthermore, the EMVO has classified alerts of various levels. This is defined in the EMVO URS Part IV and can be viewed in the EMVO's "IMT Design Note" for intermarket transactions.

A simplified overview of level 5 alerts (potentially relevant for the authorities) is provided in the following table:

Return code HUB	Description HUB	Return code MAH system	Description MAH system
Pack Identifier			
#A2	Batch not found	LOT_03	Failed to find a batch (or serial number) for the given data
#A3	Pack not found	PC_02	Unknown serial number
#A52	Expiry date mismatch	LOT_12	Expiry date does not match the date held in the NMVS.
#A68	Batch number mismatch	LOT_13	The batch ID does not match the serial number in the NMVS.
Pack State			
#A7	Pack already in requested state	PCK_19	Property is already set on pack.
#A24	Status change could not be performed	PCK_06, PCK_22, PCK_27	PCK_06: Actual pack status doesn't match the undo transaction (set and undo status must be equivalent). PCK_22: Pack is already inactive. PCK_27: Status change could not be performed.

6.4: Where can the marketing authorisation holder note the result of his alert investigation so this information is available to the verifying entity?

In the alert management system of the MAH system, e.g. in the alert detail view of the alert in question.

6.5: How can a marketing authorisation holder use the alert management system of ACS?

In order to use the alert management system, the administrator designated in the MAH system must assign a certain role with privileges to the user. For additional information on using the tool, please consult the manual for the MAH system. Use of the alert management system is not obligatory for the marketing authorisation holder.

6.6: How is an alert generated?

Alerts can be triggered by all user groups. This example of how an alert is generated is about an alert triggered by a verifying entity in Germany.

1. The pharmaceutical pack is scanned by the pharmacy (or another verifying entity) and the query (e.g. verification or inactivation) is routed to the pharmacy system (PH system).

2. The PH system routes the query to the MAH system in anonymised format.

3. The MAH system conducts the verification of the query.

4. If a conspicuity occurs, the MAH system generates a distinct alert ID and routes it back to the PH system together with the scan result. The associated alert is simultaneously routed to the EU Hub and stored in the MAH system.

5. The PH system returns the scan result to the verifying entity (including the alert ID, if applicable).

If the verification result is positive, the verifying entity is informed of the positive result (scan result).

6.7: Who clarifies if the alert is a false alarm or a suspected falsification?

The affected marketing authorisation holder must clarify if it is a false alarm or a suspected falsification, if he is able to do so. He can note the result of the investigation in the alert management system, e.g. in the detail view of the alerts in question.

6.8: What false alarms can be clarified by the marketing authorisation holder?

The marketing authorisation holder can clarify the following:

- Printing errors (e.g. print quality, coding)

- Errors during the data upload

In the best-case scenario, he will include this verification in his quality assurance process before circulating a pharmaceutical.

6.9: What can the marketing authorisation holder do in the alert management system after an alert occurred? How is an alert processed?

If the MAH system identifies a conspicuous event, the alert ID of the alert generated is transmitted to the PH system as well as the EU Hub.

If the marketing authorisation holder does not use the alert management system, the alert is immediately and automatically routed to the authorities portal.

However, if he uses this additional function of ACS, the following steps are possible:

1) The alerts can be assessed within seven calendar days. For this purpose, the marketing authorisation holder can view information in the alert management system.

2) If an alert is unfounded (e.g. technical error), the alert can be de-escalated by the marketing authorisation holder in the MAH system (after the technical error is resolved). Otherwise, the alert can be escalated by the marketing authorisation holder in the MAH system.

Note: If an alert is not processed within seven days, it is escalated automatically.

Regardless of this fact, the usual legal reporting obligations for marketing authorisation holders apply.

6.10: What is expected of the marketing authorisation holder as part of alert processing?

As a rule, the marketing authorisation holder can only check whether an alert was caused by internal errors (e.g. missing batch upload, incorrect expiry date uploaded, incorrectly printed packaging, etc.). If this is the case, the alert can be de-escalated by the marketing authorisation holder via the alert management system of ACS (please see 6.5 for usage of the tool). As long as this error is not resolved (if it is possible), the pack remains not dispensable for the verifying entity. As a result, any correction (e.g. subsequent data upload) should be made as quickly as possible but at least within seven calendar days (see 6.9).

In the case of alert type "A68 - NMVS_FE_LOT_13" (The batch ID does not match the serial number in the NMVS), the marketing authorisation holder can de-escalate the alert, if the error in the batch number occurred e.g. due to incorrect uppercase or lowercase spelling. For this alert type, the unique identifier (product code (GTIN/NTIN/PPN) and serial number) is correct. However, if the batch is unknown to the marketing authorisation holder, it is recommended that this alert be escalated.

If the marketing authorisation holder decides to use the alert management system for manual processing of the alerts, it is requested that a comment with meaningful information be entered. The comment is an important component in the communication with other system participants (e.g. terminals). This comment can be viewed independent of the status manually set by the marketing authorisation holder ("escalated" or "de-escalated") and may help the triggering entity during error analysis.

6.11: Can the market participant where the alert occurred see the result of the marketing authorisation holder's classification?

The market participant can view the result of a classification via a graphical user interface provided by the NGDA (NGDA-GUI) at https://securpharm-gui.ngda.de/. If the alert is classified as a false alarm by the marketing authorisation holder, it will not be subject to mandatory reporting.

If the alert is classified as a suspected falsification by the marketing authorisation holder, it will be subject to mandatory reporting by the marketing authorisation holder to the supervisory authority in charge. A rating as a suspected falsification also results in the legal reporting obligation of the verifying entity. If the investigation result is available after e.g. only three days, there is no need to wait for the deadline of seven calendar days to make a report.

However, if there are other indications of a suspected falsification in addition to the negative verification through the securPharm system, there is an immediate reporting obligation to the supervisory authority in charge.

6.12: What is the allowed duration for classifying an alert?

Only a marketing authorisation holder who uses the alert management system has seven calendar days for classifying an alert as a false alarm or as a suspected falsification. If a marketing authorisation holder does not use the alert management system, an alert is immediately and automatically escalated.

6.13: What happens if the marketing authorisation holder does not classify the alert?

For companies that do not use the alert management system, the alerts are escalated immediately and automatically.

For companies that do use the alert management system, the alert is only automatically classified as a suspected falsification after the deadline of seven calendar days has passed. In these cases, the securPharm system reports to the Federal Institute for Drugs and Medical Devices. The reporting obligations of the market participants remain unaffected.

6.14: Do the same regulations apply to parallel importers?

Yes.

6.15: What is the meaning of the status report "Pack inactive" at the verifying entity?

Pursuant to the Delegated Regulation, it is possible to verify the status of a deactivated pack. This function helps the pharmacist to check the status of a pack, e.g. if he wants to verify whether he has already dispensed the pack/removed the pack from the system. The specific representation of the result varies based on the software used. Since such a verification does not trigger an alert, you will find no alert ID in the alert management system and therefore no "Pack History" for this process.

6.16: Since 1 December 2020, the securPharm GUI for verifying entities has been expanded by additional tools. Which ones?

NGDA has added an alert monitoring tool to the securPharm GUI. Verifying entities (wholesalers, pharmacies) can obtain information regarding the details and processing status of an alert by the marketing authorisation holder. If the marketing authorisation holder has already processed the alert, the verifying entity can view the status and any comment entered by the marketing authorisation holder there. Furthermore, it is planned that the verifying entity itself will be able to post comments regarding the alert for the marketing authorisation holder. In the medium term, this step is to provide a dialog option between the participants.

7. Returns

7.1: What needs to be considered when handling returns?

According to the Delegated Regulation, a higher falsification risk is assumed for pharmaceuticals that are returned by end users. Therefore, pack verification across the entire supply chain is legally mandated. Returns may occur for various reasons, e.g. delivery damage or an exceeded expiry date (see Question 9.1.). Accordingly, there may be packs with the status "Active" or "Inactive". In the case of returns, it is therefore recommended to verify the pack in terms of its status before an "active" pack is inactivated e.g. as "destroyed".

8. Batch recalls

8.1: What needs to be considered during a batch recall?

If a batch needs to be recalled, this can also be done via "Batch Recall" in the system via access to the EU Hub (see Article 40 lit. a of the Delegated Regulation (EU) 2016/161). By setting the "Recall" status for a batch in the system, all packages of this batch are set to "recalled" in addition to the existing status. This status results in a deactivation of the pack, which is reported back to a dispensing entity during decommissioning, and this prevents the pack from being dispensed to the patient. In this respect, the marketing authorisation holder must ensure that the status change performed in the system is conducted before the recall is published in the trade press, so that the entire supply chain is automatically informed of the new pack status when verification or decommissioning is attempted.

9. Status changes

9.1: A pack subject to mandatory verification in accordance with the Falsified Medicine Directive reaches its expiry date. What do I need to do?

As soon as a pack reaches its expiry date, the unique identifier of that pack is automatically deactivated in the securPharm system. Therefore, it is important that market participants do not attempt to additionally deactivate the unique identifiers of expired packs (e.g. by setting them to "Destroyed"). No additional status changes in the securPharm system are necessary. Potential other duties (e.g. documentation of disposal) remain unaffected.

However, a verification of the authenticity of the unique identifier of the pack will still be possible: In that case, the securPharm system will respond with the information that the expiry date has been exceeded and the pack must not be dispensed. The pack must be handled in accordance with the existing requirements.