The National Verification System

For End Users in Belgium and Luxembourg

ACCESS REQUEST FORM Instructions

Main steps for submitting the Access Request Form

The **On Line form** is strongly advised for cases where only one End User (or a few End Users of a group) needs to request access, eg. individual pharmacies.

ON LINE FORM	
1.	Download the Instructions
2.	Download the Terms&Conditions and the Privacy Policy
3.	Read carefully the instructions provided hereafter
4.	Fill in the form according the instructions
5.	On the last page of the form read carefully the NMVS Access Policy (NAP)
6.	Accept the NAP by clicking "SUBMIT"

The **Off Line form** is strongly advised if an organisation needs to request access for a longer list of End Users, eg a pharmacy chain, a wholesaler with different warehouses, a hospital with different pharmacies at different locations.

OFF LINE FORM		
1.	Download the Instructions	
2.	Download the Terms&Conditions and the Privacy Policy	
3.	Read carefully the instructions provided hereafter	
4.	Download the Excel file and the NMVS Access Policy (NAP)	
5.	Fill in the Excel file according the instructions and save the file in the following format: **XXX_organisationname_YYYYMMDD** with XXX: PHA for pharmacies, HOSP for Hospitals and WHS for wholesalers and YYYYMMDD the date (for example 20181231)	
6.	Fill in and sign the NAP	
7.	Scan the NAP and send the NAP together with the Excel file to BeMVO by email, with email subject: "FMD USER ACCESS REQUEST" at following email address	
	for Pharmacies	pha@bemvo.be
	for Hospitals	hosp@bemvo.be
	for (Other) Wholesalers	whs@bemvo.be

Instructions to the Access Request Form

The Access Request Form is composed of 4 sections

1) Information on the End User organisation
2) The actual End User location
3) The End User system and IT information
4) Acceptance of the NMVS Access Policy

In the On Line form, the mandatory fields are marked with a "*".
In the Off Line form, the column titles in bold indicate the mandatory fields.

1) End User Organisation

This section requests information on the organisation that is legally responsible for the End User.
In case you are a site of **a hospital** or you are a warehouse of **a wholesaler**, this can be the hospital or wholesaler.
In case you are **a pharmacy** this can be the organisation that owns or exploits the pharmacy.

This section requests also to enter the **Responsible person**. This is the person who will accept the NMVS Access Policy (NAP).
Typically this would be the person representing the organisation.
For pharmacies it is agreed by the different stakeholders that the head-pharmacists (pharmacien titulaire, apotheker titularis) also can accept the NAP. In that case the pharmacist can enter his contact details in this section.

Organisation name	The name of the organisation or company who is legally responsible for the End User.
Organisation type	Referring to the section on "who are the End Users", the possible options are: Pharmacy, Hospital, Wholesaler, Other Wholesaler (i.e. a company having a wholesaling license)
Address information	The full address information of the responsible organisation
KBO-BCE / RCS	The official registration number of the organisation
Responsible person	Name of the person who will accept the NMVS Access Policy
Contact details	The contact details of the responsible person

2) End User Location identification

This section requests information on the actual End User.
An End User is defined by his physical location. Referring to the section "What is an End User" this means that different warehouses of a wholesaler are different End Users, different pharmacies in different sites are different End Users, al pharmacies of a pharmacy chain are different End Users.

This section requires also the contact details of the main contact person. This is the person at the Location that should be contacted for any communication, such as information on system availability, handling of alert messages, …
The section requires also the registration ID of the Location:

- For (Other) Wholesalers: the Authorisation Number from the EUDRA GMDP WDA list
- For Pharmacies (hospital and public): the Registration number provided by FAGG/AFMPS

- For LUXEMBOURG users: enter the ZIP code

Name of the location	The name of the End User location. - in case of a pharmacy this is the name of the pharmacy; - in case of a hospital pharmacy, this could be the hospital site where the hospital pharmacy is located; - in case of a wholesaler, this could be the name of the wholesaler warehouse
Address information	The full address information of the End User location
Registration ID	The code, in general allocated by an authority, that allows a unique identification of the End User location (For Luxembourg users: enter the ZIP code)
Main contact person	Name of the person at the End User location who can be contacted in case a communication with the End User is needed; Because communication will mainly happen through mail, it is advised to provide a stable (generic) email address
Contact details	The contact details of the main contact person

3) IT System details

This section requests information on the End User's IT system being used for access to the Verification System and contains 4 parts:

- The software used for the connection to the Verification system
- (a) Details on the Internal IT department and/or (b) contact details of the External IT partner; at least one of both needs to be provided (both are also possible)
- Indicate if the User Access Credentials can be sent to the External IT partner.
  If this is not allowed by the User, then the User is expected to implement the connection himself.

(1) Primary information required is the **Software System and Version** used by the End User to access the Verification system.

Depending on
(1) the type of solution that will be used to connect to the Verification system and
(2) the integration or not of such solution with an existing software/ERP system,
then the Software Name and Version to mention is:

Dedicated ERP system (own development or external)		
1	Acquired stand-alone FMD software package and used separate from ERP	Name & version of the stand-alone FMD software package
2	Acquired FMD software package (module) that is linked (or integrated) to the ERP system	Name & version of the integrated FMD software package
3	FMD module developed within the ERP system	Name and version of the ERP system
Standard external software system		
1	Acquired stand-alone FMD software package and used separate from the standard software	Name & version of the stand-alone FMD software package

2	FMD module integrated in the standard software system	Name & version of the software system

(2) Internal IT details

The contact details of the internal IT contact.
In case no external partner is mentioned, then this information is mandatory.

(3) External IT details

The contact details of the external IT contact.
In case no internal IT department is mentioned, then this information is mandatory.

(4) End-User Credentials

In case an external IT partner is mentioned, the standard procedure is that the User Credentials will also be provided to that external IT partner. Eg., in the case of a pharmacy, the user credentials will be provided to his Software Supplier to allow that supplier to implement the connection for the User.
IF YOU OBJECT to the User Credentials being provided to that external IT partner, then check this box in the form. Selecting this option then also implies that the User will manage (with or without his external IT partner) the implementation himself.

Software name	The name of the software package that will be used to connect to the Verification System (see decision table above)
Software version	The version of the software referred to in previous item
Internal IT department	Contact information of the person at the End User's premises or organisation that can be contacted in case of technical questions; if the used solution is fully integrated in a software package provided by an external software supplier and no local IT responsible is available, this section can be left blank
External IT provider	Company and contact information of the external software supplier who provides the software module (stand alone or integrated in a software package) for access to the Verification System; in case of a pure internal development, this part can be left blank.
End User Credentials	The end user credentials will be sent to the relevant persons from the end user's organisation or location. In case of an external IT provider, the standard is that the end user credentials will also be sent to that IT provider to facilitate the implementation by that IT provider. In case you object to this procedure, check this box.

4) Acceptance of the NMVS Access Policy
The legally responsible person (mentioned in section 1) End User Organisation) accepts the NMVS Access Policy (containing both the T&C and the DPP) by clicking "Submit".
The acceptance of the NMVS Access Policy should only be done after review of the related documents (T&C and the DPP) by the responsible person of the organisation.