Med Safety App
Vigilance Hub – Guidance

Date: 2021.06

Version: 2.0

Contents

1. Purpose

This document explains the steps required to use the Med Safety Vigilance Hub. Any updates to the Hub, and any of the processes within the Hub will be reflected in revised versions of this document.

Please email your country Superuser for any questions. Superusers can contact the MHRA team via working group meetings of by emailing WEB-RADR@mhra.gov.uk with any enquiries.

2. Background

2.1. Med Safety App

The Med Safety App was developed through the Innovative Medicines Initiative WEB-RADR: Recognising Adverse Drug Reactions project. The App is a e-Reporting tool which facilitates direct and instant reporting of suspected adverse drug reactions (ADRs) to medicines and vaccines by patients and healthcare professionals. It allows for the two-way communication of up-to-date pharmacovigilance information via news feeds and contains an Adverse Events Following Immunisation (AEFI) form in line with the WHO's 25 core variables for AEFI reporting.

https://www.who.int/vaccine_safety/initiative/tools/AEFI_reporting_form_EN_Jan2016.pdf

The Med Safety App allows suspected ADRs to be reported directly to the national centre and receipt of immediate acknowledgement of the submitted report. As the app uses the ICH E2B(R2) messaging standard, the individual case safety reports (ICSRs) can be transmitted directly to a national database that processes such standard messages, such as VigiFlow – UMC's ICSR management system. VigiFlow is tailored for national centres and has built-in support to share data to the WHO global ICSR database, VigiBase.

The Med Safety App is continuously being improved and enhanced. Such enhancements include the development of multiple tailored reporting forms such as the AEFI form.

The Med Safety App is available as a free download from Android or iOS app store and more information about the Med Safety app can be found here

Download Med Safety App:

- App store (For iOS devices)
- Google Play (For Android devices)

2.2. Vigilance Hub

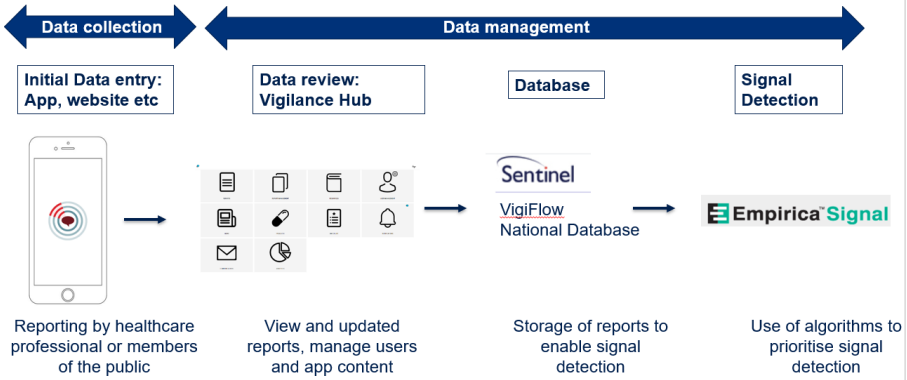
The Vigilance Hub has been created to manage the back-end system (part of the website/app that is not accessible to the user e.g. member of public) of the mobile app. The Vigilance Hub will only be available to staff of regulators (NRA and EPI) who adopt the Med Safety and WEB-RADR mobile apps. The Vigilance Hub can be used to view submitted reports, edit case reports submitted (e.g. with follow-up information) and download report details. It can also be used to configure news items for users of the Med Safety App and create watch lists for products of interest. More information about the Vigilance Hub can be found here

2.2.1 Vigilance Hub training

As part of the African Union Smart Safety Surveillance programme a capacity strengthening training package was created to support countries with their pharmacovigilance activities. This included a live demonstration of the vigilance hub which can be accessed here using the pass code: Ni7ua^5?

2.3. End to end system setup

Initial ADR report data will be entered via the App by healthcare professionals and patients and will then be available to view and update in the vigilance hub. Data will be sent to the national database/VigiFlow as well as the MHRA database, called Sentinel, and will then be available for signal detection activities which will be supported through Empirica.



2.4. High-level functionality

The high-level functionalities for the vigilance hub can be found below. For support on user management, all users should contact the 'superuser' who is the designated member for adding new users.

1. Reporting / Report Management:
   - Ability to create and send ICSRs (XML R2/R3)
   - Export created ICSRs as XML or PDF
   - Upload/post files containing ICSRs (XML R2/3)
   - Receive acknowledgements (XML R2/R3)
   - Track submissions/acknowledgements
   - View and download ICSRs received by the organisation
   - Send updated submissions or follow ups

2. News & Resources:
   - Access to the latest news and guidance materials

3. User Management:
   - Create and manage users of the hub
   - Manage their access rights
   - Disable account access

4. Organisation Management:
   - Manage the branding of their platform
   - Manage how their reports are transmitted
   - Manage their drugs lists and supporting meta data
   - Manage which reporting features they have access

2.5. Vigilance Hub user access levels

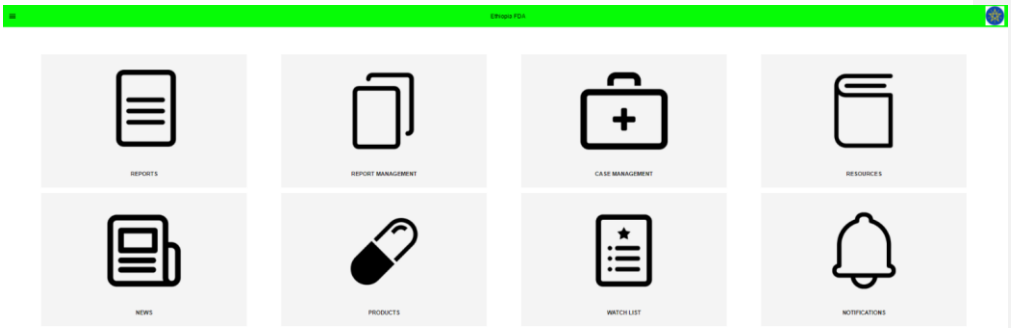
NRA and EPI users of the vigilance hub will be divided into 2 levels of user access privileges (standard user and organisational lead) depending on their role type and required functionalities. User levels will be determined and set by the in country 'superuser' who will assign the access level at the time of set up.

2.5.1. Standard user

A standard user will be the level that most people will have access to and will allow for the following:

- Can update their own password
  - Cannot change their role type
- Can view reports from their organisation
- Can edit and update reports from their organisation
- Can view news articles
- Cannot access 'Configure News' (Organisational lead access)
- Cannot access 'Organisation Management' (Organisational lead access)

When a standard user logs into the vigilance hub you will be presented with a homepage containing the below '**tiles'** which allows access to various functionalities. This includes the tiles for 'Reports' 'Report Management' and 'Case Management' which will be described in more detail within this document. A standard user will be able to view a full list of all products which have been imported for the organisation.

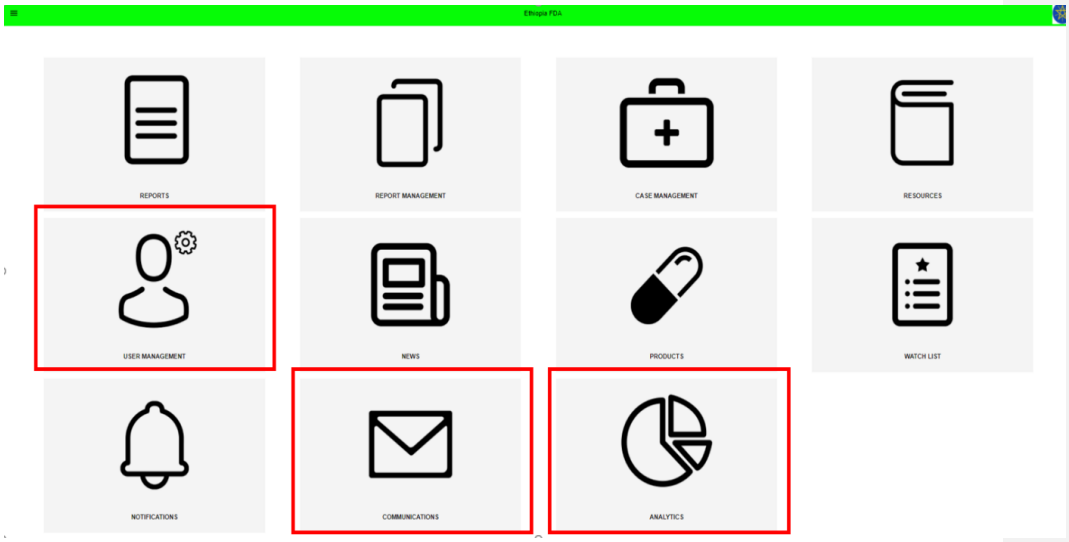


2.5.2. Organisational lead

- Can access 'User Management
  - Can only create Organisation Lead or Standard users and associate them to their organisation(s)
  - Can update their own password but not their role type
- Can only create acknowledgements for reports that their organisation receives

- Can edit organisation details such as the contact details, theme, news configurations, drugs list/meta, professions list and translations
- Can view reports from their organisation
- Can edit and update reports from their organisation
- Can access ‘Configure News’
- Have access to ‘Report Management’

When an organisational lead logs into the vigilance hub you will be presented with a homepage containing the below ‘**tiles’** which allows access to various functionalities. This includes the tiles that are available to a standard user as well as three additional tiles for ‘User Management’, ‘Communications’ and ‘Analytics’.



3. Log in

To access the Vigilance Hub users will have to contact their designated ‘Superuser’ who will add them to the Hub as either a ‘Standard User’ or an ‘Organisational Lead’. The ‘Superuser’ will provide the new user with a username (work email address) and password.

1. Log into the vigilance hub using the link:

   https://med-safety.redant.cloud/login

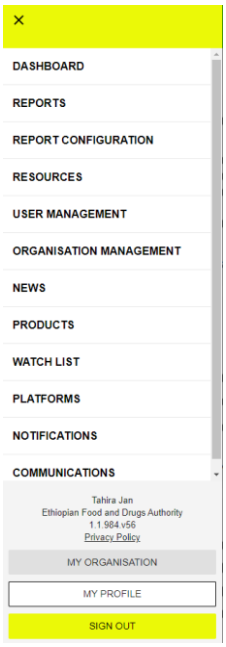
Field Code Changed

1.1 Changing Passwords

Passwords must be kept safe and it is important that these are changed at regular time points, and should be updated as soon as you first access your account. To change a password, follow the below steps:

1. Select the menu option icon from the top left-hand side of the screen 

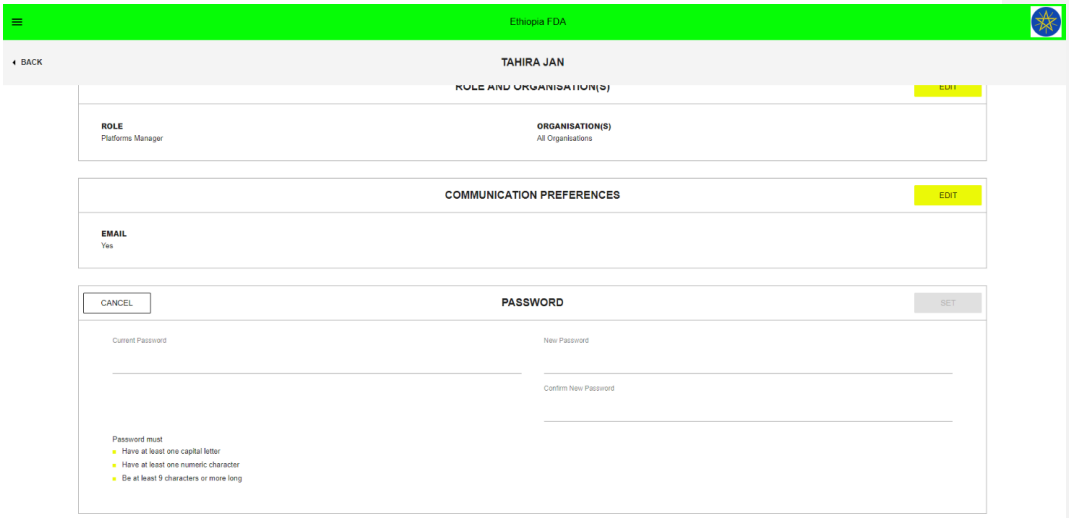
2. Select ‘My Profile’ from the bottom of the dashboard menu. This menu also acts as another way to access the different tiles within the Hub.



3. Scroll to the bottom of ‘My Profile’

4. Select ‘Set now’ in the password section

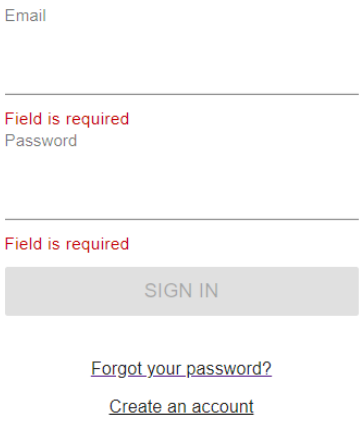
5. Enter your current password and new password (with a repeat confirmation)
   - Password must
     - Have at least one capital letter
     - Have at least one numeric character
     - Be at least 9 characters or more long



6. Select ‘Set’ once you have confirmed a password

1.2 Resetting Passwords

1. If you forget your password, you can reset this by selecting ‘Forgot your password?’ at the login stage



2. Enter your registered email address and select ‘Submit’

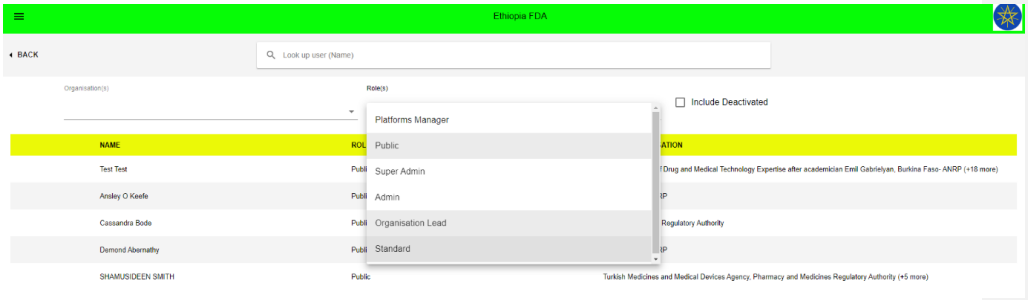
3. You will be sent an email with a secure link and instructions for how to reset your password

1.3 Reactivating accounts

In situations where users are unable to log into their account via the Med Safety App or the Vigilance Hub, there may be a need to reactivate the account which has been locked.

1. Select the ‘User Management’ tile 

2. Select the required role type from the drop-down menu

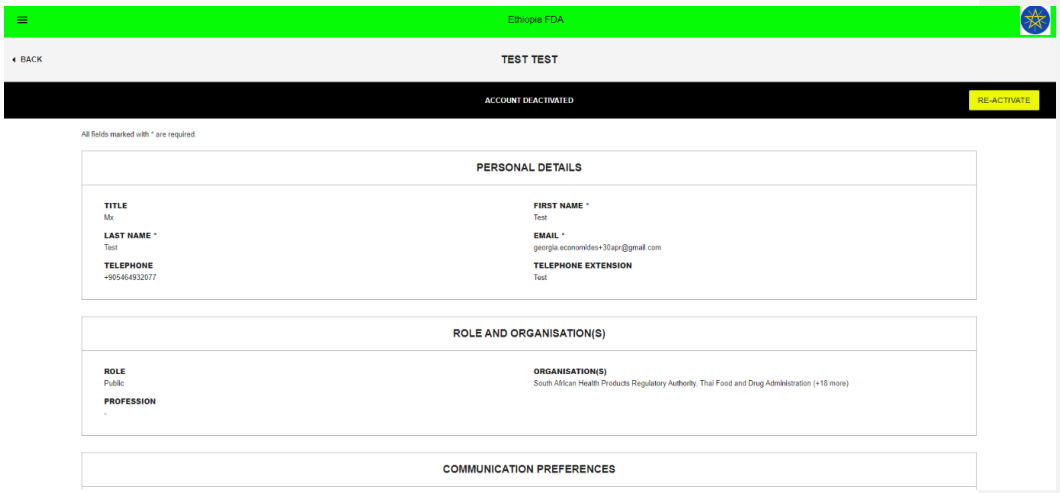


3. Select the check box for ‘Include Deactivated’

4. Locate the username from the list – this will be greyed out if deactivated and in black if currently active.

5. Double check the users email address

6. Select the ‘Re-activate’ button on the top right-hand side



4. Report

4.1. Submitting reports

The ‘Reports’ tile presents the user with a way to submit an ADR report without using the Med Safety App. This may be particularly helpful when entering reports onto the system from paper reports or when Healthcare professionals or patients call hotlines to submit reports.

1. Log into the vigilance hub using the link: https://med-safety.redant.cloud/login

Field Code Changed

2. Select the ‘Reports’ tile from the main dashboard

3. Select ‘New Report’

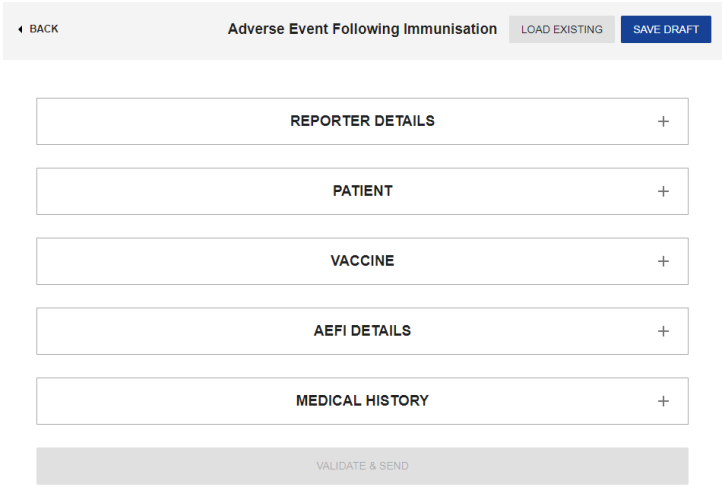
4. Select the report type from the drop-down menu – either ‘Adverse Event Following Immunisation’ for a vaccine report or ‘Report a suspected side effect to a medicine’ for all other medicines. Please note that there will be two options for the AEFI form; one for healthcare professionals and one for members of the public/patients (MOP).
   NB: You may want to consider forming local processes when entering reports via the Vigilance Hub to be able to distinguish between reports submitted via the App and the Hub.

5. Click ‘Select’

6. You will then be presented with a version of the report which looks different to the Med Safety App version of the report but all fields within this report are the same as the App.

7. You can load an existing report (E2B xml compliant report) or save your draft report using the options at the top right-hand side of the page.

8. Select the + sign next to each report block and enter the details as per the headers and questions.



9. When complete, select ‘Validate & Send’ at the bottom of the page.

5. Report Management

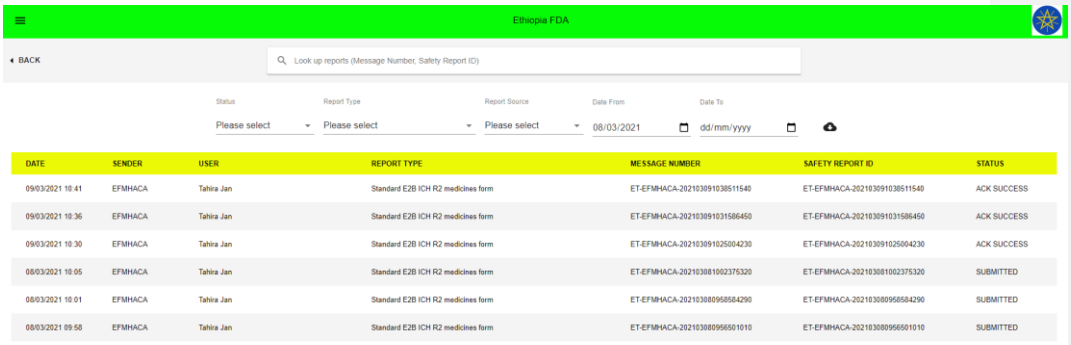
5.1. Case search

1. Log into the vigilance hub using the link: https://med-safety.redant.cloud/login

Field Code Changed

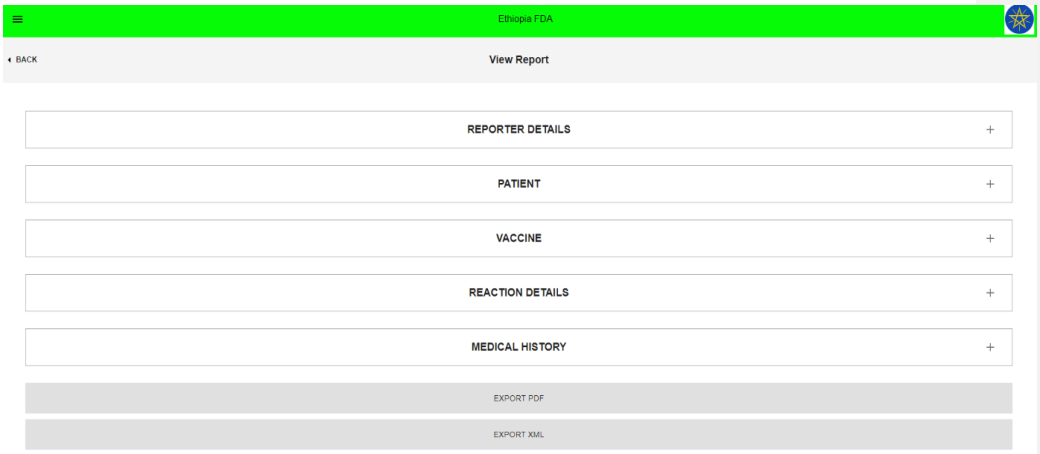
2. Select the 'Report Management' tile from the main dashboard

3. Click on the search bar at the top of the dashboard
4. Enter the Safety Report ID/case reference.
5. You will be able to view the date and time of submission, username, safety report ID and report status.



6. You can also select cases by selecting dates using the 'Date from' and 'Date to' calendar picker.
7. There is also an option to filter reports by 'Status', 'Report type' and 'Report Source' if required. This is less likely to be used for Med Safety App reports.
8. Select the case of interest
9. Select 'Export PDF' or 'View Report' as required

10. When you select ‘View Report’ you will be taken to the Vigilance Hub report form as per the below where you can again export the PDF version of the report



6. Case Management

When accessing the 'Case Management' tile as either a standard user or an organisational lead you will be able to view the reports that have been received by the organisation, download PDF versions of cases and create updates for cases where follow up information has been received.

The 'Case Management' tile is a repository of all the reports with your organisation will have received through the Med Safety App for your particular country. Cases can be viewed on the dashboard within this tile. Some of the functionality is similar to the report management tile – in time there will only be one tile for this functionality.

6.1. View cases

1. Log into the vigilance hub using the link: https://med-safety.redant.cloud/login

Field Code Changed

2. Go to the 'Case Management' tile to be presented with the Case Management dashboard of reports

3. You can use the 'Validation' options to view cases that are valid/not-valid/invalid using the dropdown which would indicate if there were any errors in the data processing.

4. You can view the case 'Receiver Status' to ensure cases are successfully processed. If any cases are flagged as 'unsuccessful' it is important to feedback to your 'Superuser' who will notify the MHRA immediately.

5. Cases can be filtered by date received, by clicking the calendar icon next to 'Date from' and Date To' options and scrolling to select the relevant dates.

6. On the right-hand side you will see the number of reports that appear based on your selected search parameters.

7. To view a case of interest, click on the case number (on the left-hand side of the screen) to restrict the cases to all cases with this Safety report number

6.2. Case search

1. Click on the search bar at the top of the dashboard

2. Enter the Safety Report ID/case reference. All versions (initial case and update cases) of the case will appear in the dashboard.

3. Select the 3 dots to the right-hand side of the case

4. Click 'Report Summary' for options to see further case information

5. You can export case details by selecting 'Export PDF' to view a PDF version of the case which has been received. This is a version which can be shared with a healthcare professional or a patient if required.

6.3. Follow ups/Case update function

If follow up information is actively sought and collected from the organisation, the 'case management' tile can be used to create an update for the initial case report.

1. Use the search bar to search by entering your Safety Report ID and 'enter'
2. Select the 3 dots to the right-hand side of the case
3. Click 'Report Summary'
4. Select 'Update'

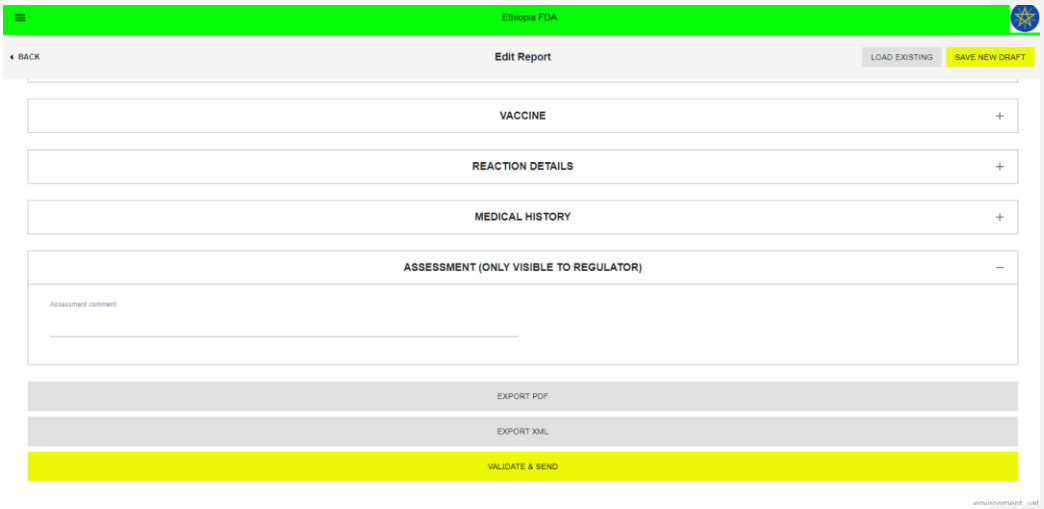
5. You will then be presented with a read-only version of the report which looks different to the Med Safety App version, however all fields within this report are the same as the App.
6. Click 'Update' from the top right-hand corner of the page.
7. Add additional/follow up information using the report form that is available by selecting the + sign next to the relevant report fields (See 'Reports' section for more information).
8. You can open repeatable blocks by selecting the 'pen' icon to the right-hand side.
9. If information needs to be removed, you can select the 'bin' icon on the right-hand side to delete previously entered information. You should only delete information if it is found to be incorrect e.g. if a drug has been stopped then a stop date should be added whilst the entry is kept.
10. Once follow up has been completed, click 'Validate & Send' at the bottom of the page. Note, you can save a draft at any stage of completing follow up.
11. You will see a successful submission status.
12. A new report row will be available, earlier case will become inactive to prevent version control issues. You will be able to view the date and time stamps for all reports.

6.4 Assessment Comments (for regulator use only)

When regulatory assessment comments need to be associated within the case for easy access between the NRA and EPI these can be added via the Vigilance Hub. - Only those with Organisation lead and Standard user access will be able to view and edit comments. Assessment comments are not visible for front end public users.

1. Locate the report for which you would like to add an assessment comment by using the search bar and entering the Safety Report ID and 'enter'
2. Select the 3 dots to the right-hand side of the case
3. Click 'Report Summary'
4. Select 'Update'

5. You will then be presented with a read-only version of the report
6. Click 'Update' from the top right-hand corner of the page.
7. Scroll to the bottom of the page to the report block titled 'Assessment (only visible to regulator)
8. You can open repeatable blocks by selecting the '+' symbol on the right-hand side of the block.
9. Enter the regulatory comment in the 'Assessment comment' field
10. Once completed, click 'Validate & Send' at the bottom of the page. Note, you can save a draft at any stage.



11. You will see a successful submission status.

12. A new report row will be available, earlier cases will become inactive to prevent version control issues. You will be able to view the date and time stamps for all reports.

NB: All updated vaccine cases are automatically sent to both Sentinel and Vigiflow.

7. News

To view news a standard user can click on the 'News' tile to access a read-only version of news which has been created for the organisation.

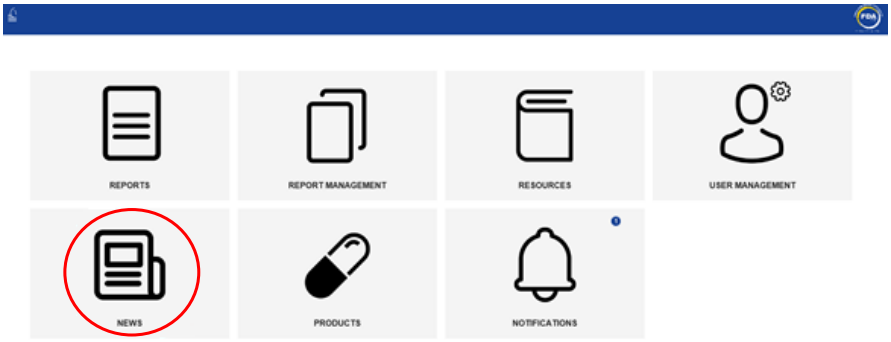
An organisational lead will be able to create customised news articles in 2 different ways as below.

7.1. Creating news articles

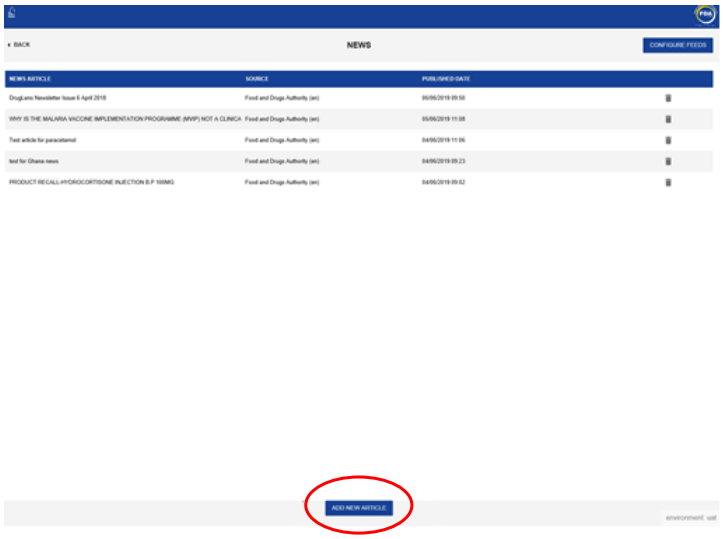
1. Log into the vigilance hub using the link: https://med-safety.redant.cloud/login

Field Code Changed

2. Select the **News** tile



3. Select 'add new article' from the bottom of the page



4. Add title – maximum limit of 255 characters
5. Add a summary (a brief description of the article) - maximum limit of 255 characters
6. Add content – no character limit

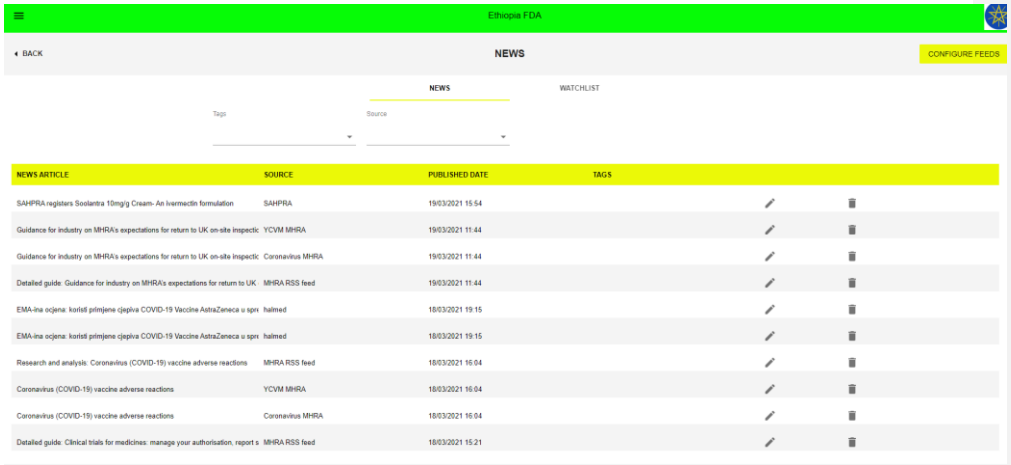
7. Attach documents if desired
8. Select language – note if your app uses multiple languages, you will need to create an article separately for each language.

9. Date and time – if you wish for a future publication date or time, amend the date and time (this will allow you to publish a news article at a specified date and time)

10. Select ‘submit’ to make the article live to all users

11. News article will appear in the app after approximately 10 minutes (or specified future date and time).

The second way to add a news article is to configure a news feed.



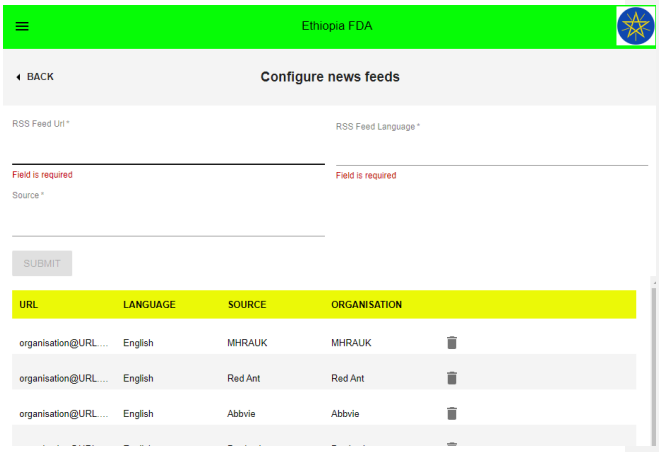
7.2. RSS feed news articles

1. Select ‘Configure News’ from the top right-hand side of the page

2. Embed a link within the app by adding the RSS feed URL

3. Add the RSS feed language and source and then click ‘ Select’.

4. Please note it can take 24 hours for your RSS feed to show in the App.



8. Products

The ‘Products’ tile will contain all of the products that you have listed within the Med Safety App. These will be listed to the WHO/UMC drug list and needs to be maintained regularly to ensure that all products are available for selection from the user.

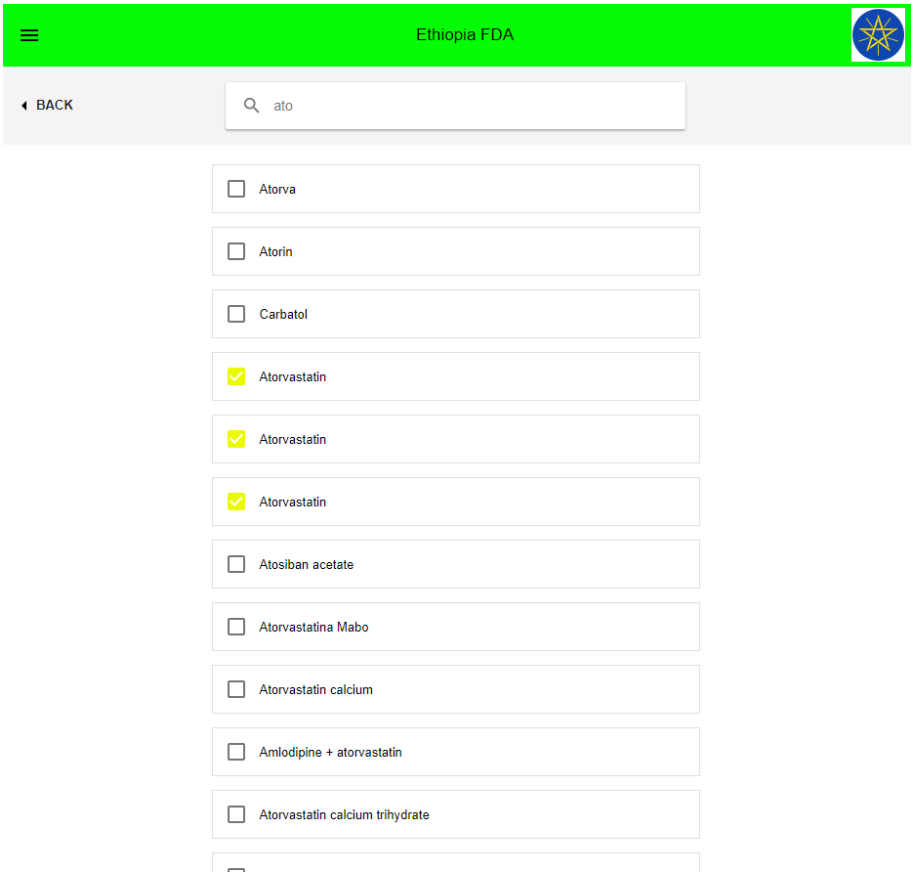
8.1. Creating product watchlists

Within the Med Safety App you can create a watch list where you can flag products of interest and then see any news articles associated with this products. This functionality is mainly intended for App users but it is visible in the Vigilance Hub.

1. Log into the vigilance hub using the link: https://med-safety.redant.cloud/login

Field Code Changed

2. Go to the ‘Products tile to be presented with a list of all products 
3. To search for a product, you can start typing in the search field
4. To add a product to the watch list, select the check box next to the product name.



5. Select the product of interest (in this case Atorvastatin) to see the summary of ADR data submitted to the MHRA for the associated active ingredient. All of the data provided here is linked to the UMC's Vigibase and any empty fields means no data is held.

6. Group information using the drop down to see data of interest by: reactions, gender, age, continents, year

7. You can view related news, report a side effect for this product or remove it from the watch list using the buttons at the bottom of the page

9. Communications

The ‘communications’ tile allows the user to tailor the acknowledgements and follow up emails that get sent to reporters. When a report is submitted via the Med Safety App, an acknowledgement is sent to the users thanking them for reporting a case and providing a copy of the report reference number. Acknowledgements can be tailored differently for different kinds of reports such as medicines and vaccines, to provide very specific information about the vaccination programme. Tailored acknowledgements can also be used to point reporters towards further information or towards specific websites.

9.1. Edit communications

1. Log into the vigilance hub using the link: https://med-safety.redant.cloud/login

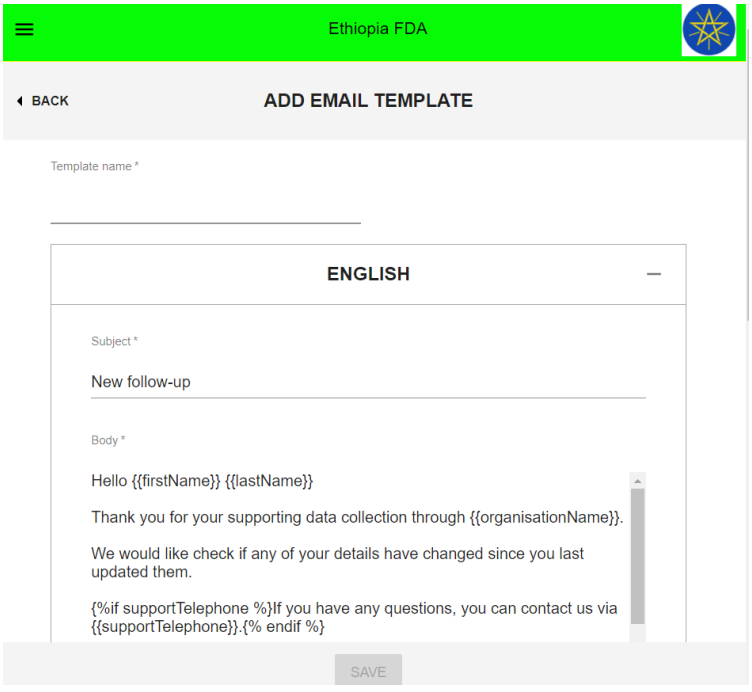
Field Code Changed

2. Go to the ‘Communications’ tile to view customised acknowledgements and follow up templates

3. To edit the content within the acknowledgement/follow up, this can be done in real time by selecting the ‘pen’ icon next to the acknowledgement template.

4. Edit the subject or body of the template

5. Click ‘save’ once completed.



9.2. Add new communications

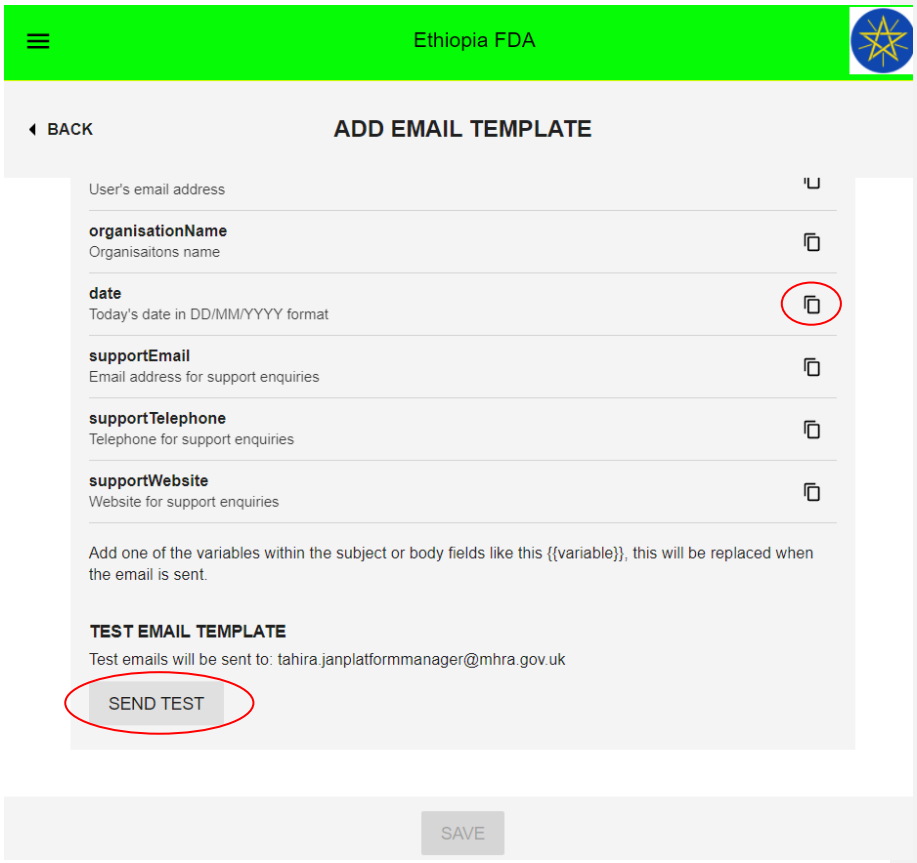
1. Select ‘Add template’

2. Enter template name, edit subject and body

3. To add a standard variable (pre-set fields with look up logic) such as date to the template select the ‘copy’ icon to the right-hand side of the variable and paste into the template body.

4. Click ‘Send test’ to view a test copy of the new acknowledgement or follow up template.

5. Select ‘Save’



10. Analytics

The ‘analytics’ tile is a high-level overview of the aggregated information that an organisation receives and will provide the number of reports that have been received over a given time period as well as how many registered users you have. The ‘analytics’ tile also allows the user to export excel spreadsheets of the data/reports contained within the vigilance hub for the organisation.

10.1. View high level data

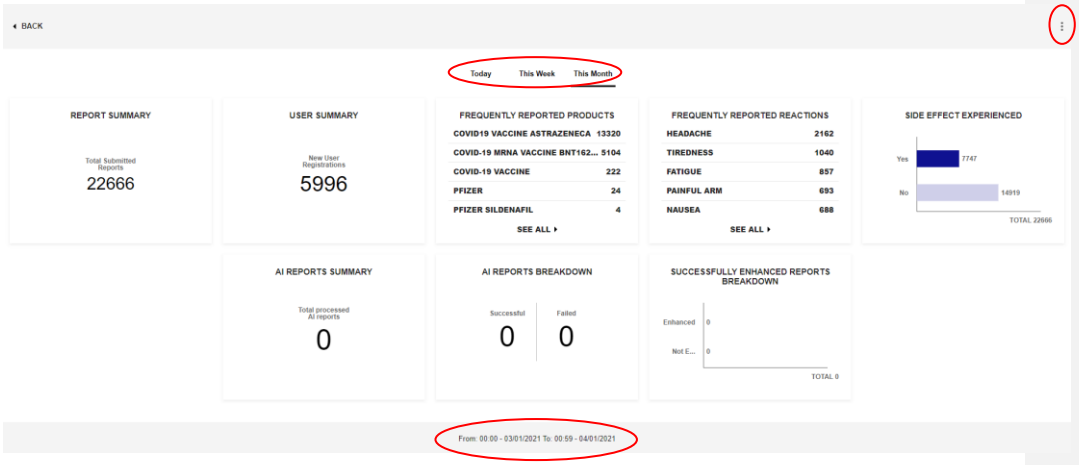
1. Log into the vigilance hub using the link: https://med-safety.redant.cloud/login

Field Code Changed

2. Go to the ‘Analytics’ tile to be presented with the analytics dashboard of data

3. A snapshot of the high-level data can be viewed in the analytics dashboard by:
   - Day
   - Week
   - Month

4. The specific date that the data is referring to can be seen at the bottom of the page



10.2. Exporting data

1. Click on the 3 dots in the top right-hand side of the page

2. Filter the data by time period by selecting the date required ‘start date’ and ‘end date’

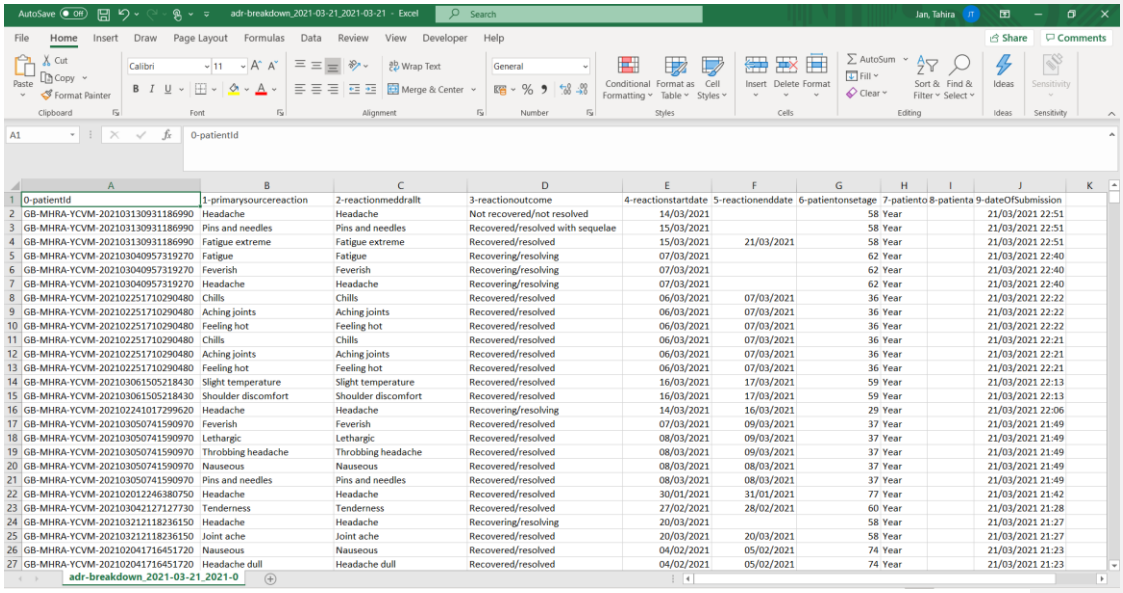
3. The data is available in CSV outputs which will look similar to an excel spreadsheet

4. Select which data set you require from
   - Patient information (contains patient demographics)
   - Medicine/vaccine breakdown (product information)
   - Adverse drug reaction breakdown
   - Narrative details

5. Select ‘export’

6. The document will download and can be opened (‘open file’) from the bottom left-hand side of the page

7. The excel sheet can be filtered to show data using different field values if required



0-patientId	1-primarysourcereaction	2-reactionmeddrallt	3-reactionoutcome	4-reactionstartdate	5-reactionenddate	6-patientonsetage	7-patiento	8-patienta	9-dateOfSubmission
GB-MHRA-YCVM-20210313093118699O	Headache	Headache	Not recovered/not resolved	14/03/2021		58	Year		21/03/2021 22:51
GB-MHRA-YCVM-20210313093118699O	Pins and needles	Pins and needles	Recovered/resolved with sequelae	15/03/2021		58	Year		21/03/2021 22:51
GB-MHRA-YCVM-20210313093118699O	Fatigue extreme	Fatigue extreme	Recovered/resolved	15/03/2021	21/03/2021	58	Year		21/03/2021 22:51
GB-MHRA-YCVM-20210304095731927O	Fatigue	Fatigue	Recovering/resolving	07/03/2021		62	Year		21/03/2021 22:40
GB-MHRA-YCVM-20210304095731927O	Feverish	Feverish	Recovering/resolving	07/03/2021		62	Year		21/03/2021 22:40
GB-MHRA-YCVM-20210304095731927O	Headache	Headache	Recovering/resolving	07/03/2021		62	Year		21/03/2021 22:40
GB-MHRA-YCVM-20210225171029048O	Chills	Chills	Recovered/resolved	06/03/2021	07/03/2021	36	Year		21/03/2021 22:22
GB-MHRA-YCVM-20210225171029048O	Aching joints	Aching joints	Recovered/resolved	06/03/2021	07/03/2021	36	Year		21/03/2021 22:22
GB-MHRA-YCVM-20210225171029048O	Feeling hot	Feeling hot	Recovered/resolved	06/03/2021	07/03/2021	36	Year		21/03/2021 22:22
GB-MHRA-YCVM-20210225171029048O	Chills	Chills	Recovered/resolved	06/03/2021	07/03/2021	36	Year		21/03/2021 22:21
GB-MHRA-YCVM-20210225171029048O	Aching joints	Aching joints	Recovered/resolved	06/03/2021	07/03/2021	36	Year		21/03/2021 22:21
GB-MHRA-YCVM-20210225171029048O	Feeling hot	Feeling hot	Recovered/resolved	06/03/2021	07/03/2021	36	Year		21/03/2021 22:21
GB-MHRA-YCVM-20210306150521843O	Slight temperature	Slight temperature	Recovered/resolved	16/03/2021	17/03/2021	59	Year		21/03/2021 22:13
GB-MHRA-YCVM-20210306150521843O	Shoulder discomfort	Shoulder discomfort	Recovered/resolved	16/03/2021	17/03/2021	59	Year		21/03/2021 22:13
GB-MHRA-YCVM-20210224101729962O	Headache	Headache	Recovering/resolving	14/03/2021	16/03/2021	29	Year		21/03/2021 22:06
GB-MHRA-YCVM-20210305074159097O	Feverish	Feverish	Recovered/resolved	07/03/2021	09/03/2021	37	Year		21/03/2021 21:49
GB-MHRA-YCVM-20210305074159097O	Lethargic	Lethargic	Recovered/resolved	08/03/2021	09/03/2021	37	Year		21/03/2021 21:49
GB-MHRA-YCVM-20210305074159097O	Throbbing headache	Throbbing headache	Recovered/resolved	08/03/2021	09/03/2021	37	Year		21/03/2021 21:49
GB-MHRA-YCVM-20210305074159097O	Nauseous	Nauseous	Recovered/resolved	08/03/2021	08/03/2021	37	Year		21/03/2021 21:49
GB-MHRA-YCVM-20210305074159097O	Pins and needles	Pins and needles	Recovered/resolved	08/03/2021	08/03/2021	37	Year		21/03/2021 21:49
GB-MHRA-YCVM-20210201224638075O	Headache	Headache	Recovered/resolved	30/01/2021	31/01/2021	77	Year		21/03/2021 21:42
GB-MHRA-YCVM-20210304212717273O	Tenderness	Tenderness	Recovered/resolved	27/02/2021	28/02/2021	60	Year		21/03/2021 21:28
GB-MHRA-YCVM-20210321121823615O	Headache	Headache	Recovering/resolving	20/03/2021		58	Year		21/03/2021 21:27
GB-MHRA-YCVM-20210321121823615O	Joint ache	Joint ache	Recovered/resolved	20/03/2021	20/03/2021	58	Year		21/03/2021 21:27
GB-MHRA-YCVM-20210204171645172O	Nauseous	Nauseous	Recovered/resolved	04/02/2021	05/02/2021	74	Year		21/03/2021 21:23
GB-MHRA-YCVM-20210204171645172O	Headache dull	Headache dull	Recovered/resolved	04/02/2021	05/02/2021	74	Year		21/03/2021 21:23

11. User Management

The ‘User Management’ tile allows the user to see other users within the organisation and allows the user (organisation lead) to add a new user. In the first instance all organisation leads should be added by contacting the in country ‘Superuser’ who may then give permission for other members to add new users.

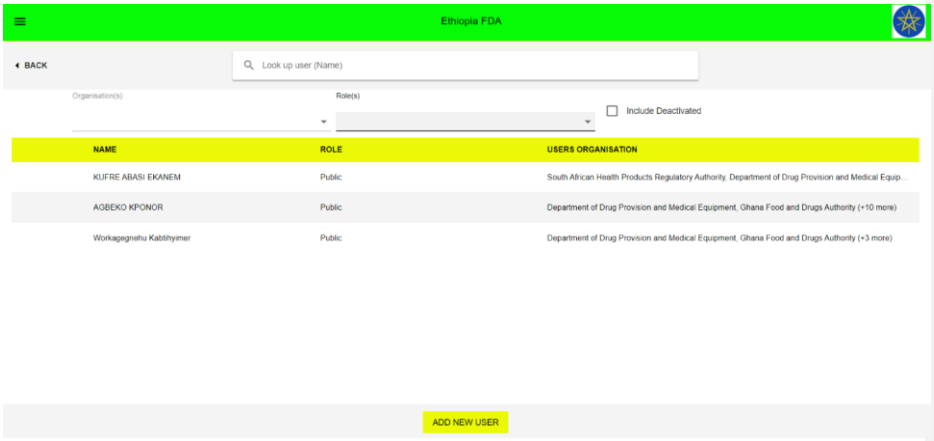
11.1. Adding a new user

1. Log into the vigilance hub using the link: https://med-safety.redant.cloud/login

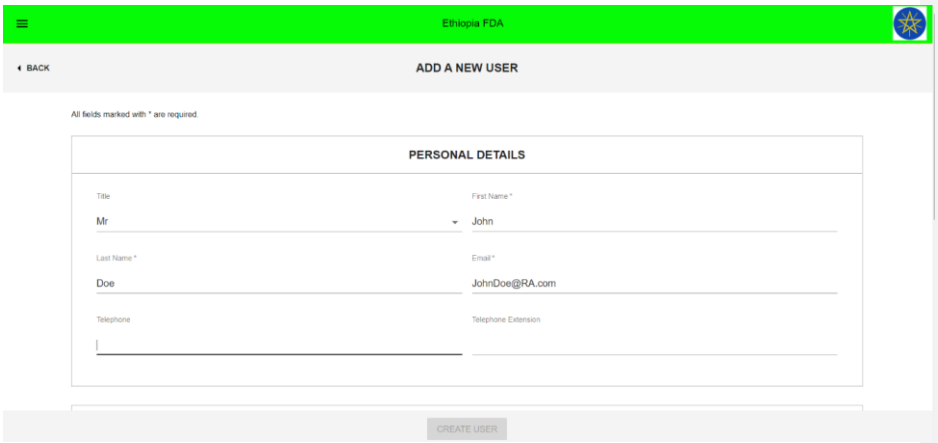
Field Code Changed

2. Select the ‘User Management’ tile

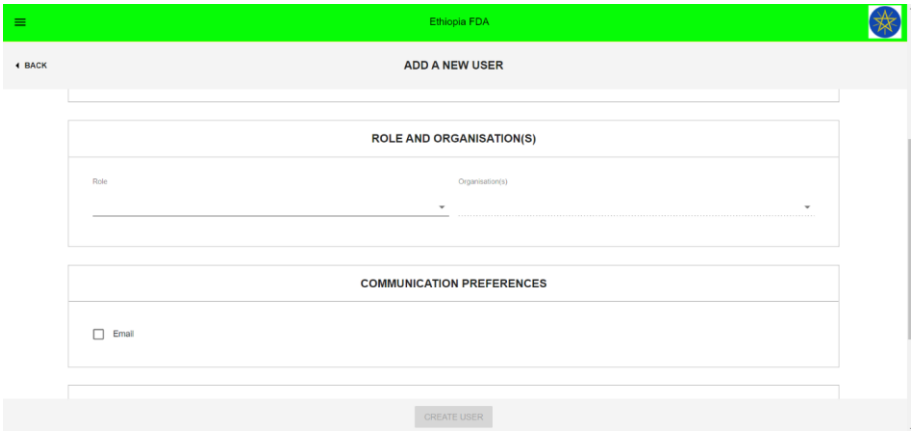
3. Select ‘Add new user’ from the bottom of the screen



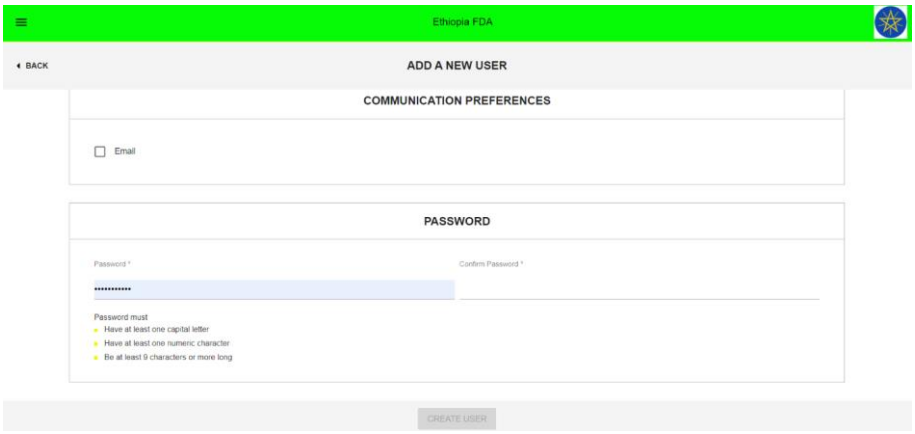
4. Enter details under the ‘Personal details’ header for the user ensuring all fields with an asterix (*) are complete.



5. Under ‘Role’ select either **standard user** or **organisational lead** depending on the level of access that is required for the user. Then add the relevant organisation and select ‘Communication preference’ as **email** if required.



6. Under the ‘Password’ header enter a unique password which should only be shared with the user. The password must meet the following criteria
    - Have at least one capital letter
    - Have at least one numeric character
    - Be at least 9 characters or more long



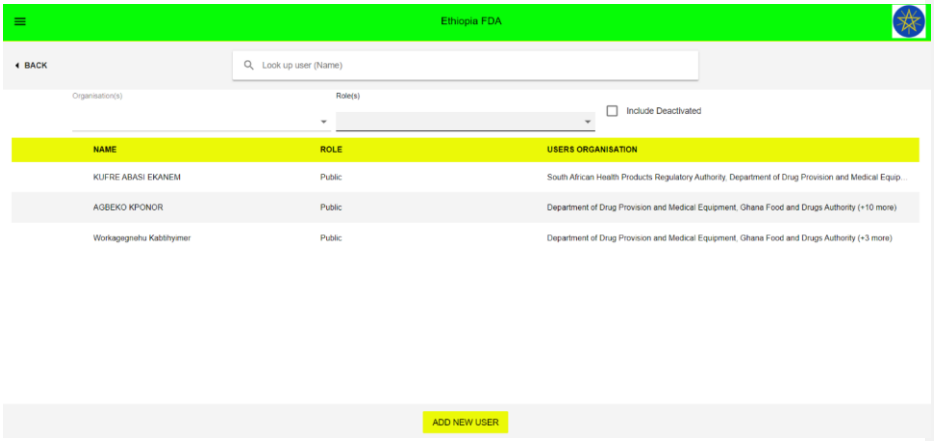
7. Select **create user** from the bottom of the screen

11.2 User Permissions – Report Type

To limit the types of reports that a standard user can access (for example, EPI programme standard users), an organisation lead can set their permissions to vaccine only reports.

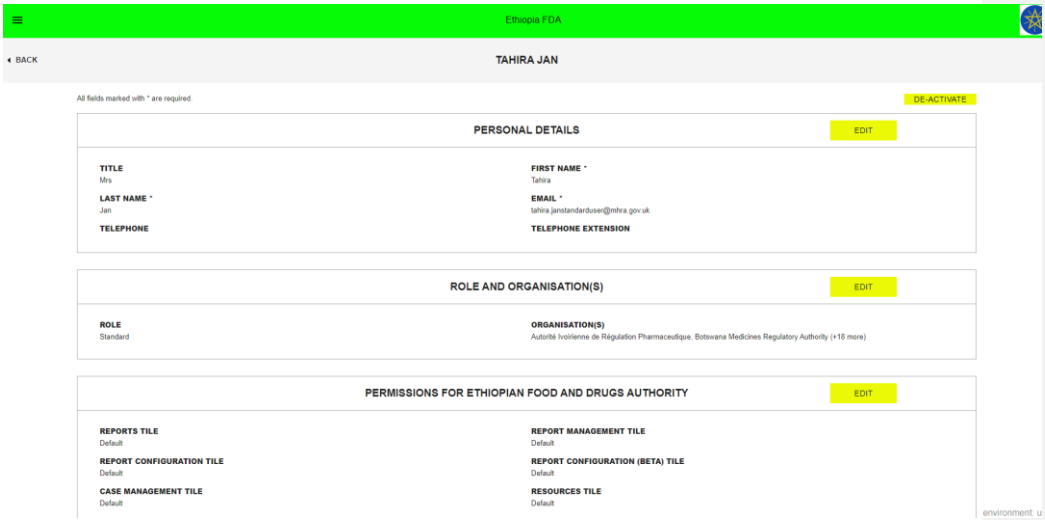
1. Select the ‘User Management’ tile 

2. Select ‘Standard User’ from the Role(s) drop-down menu



3. Select the User from the list

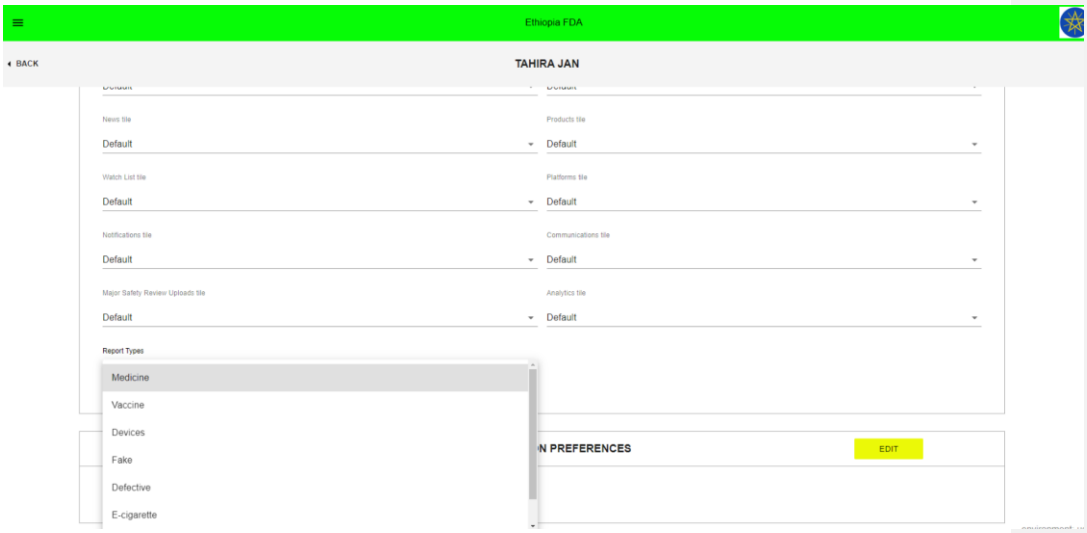
4. Select ‘Edit’ to the right-hand side of the Permissions block



5. Scroll down to the field for ‘Report Type’ and select ‘Vaccine’ (or required report types) from the drop-down list

6. Select ‘save’. The user will now only have access to cases for the report type for which permissions have been set. If the report type is set to ‘default’ the user will have access to all report types.

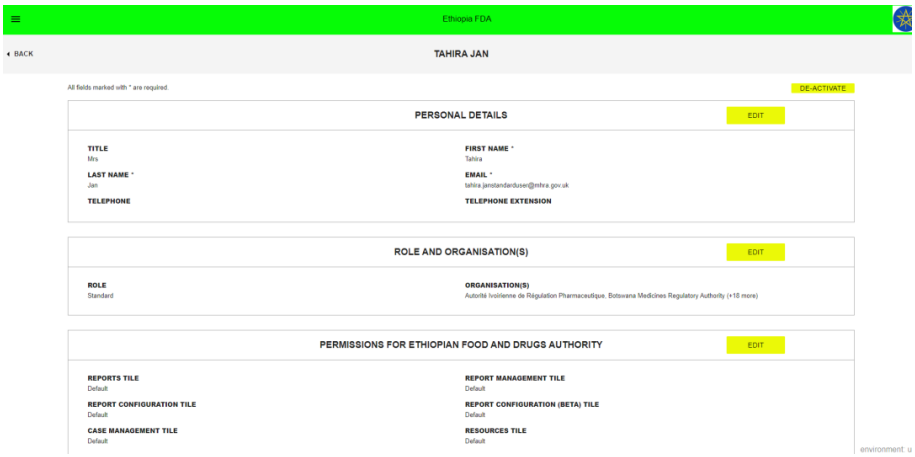
NB: When setting up new users you will not have access to the permissions block. This will only be available once the new users’ details have been set up and saved.



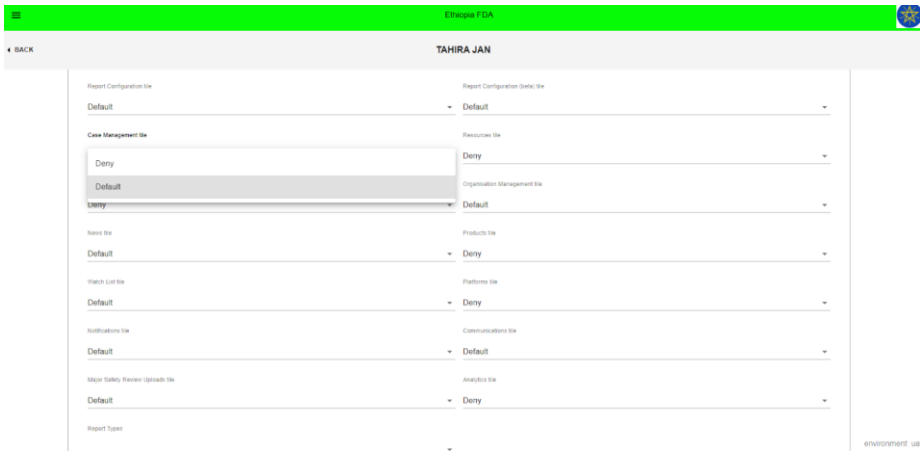
11.3 User Permissions – Specific Hub access (tile restriction)

To limit Vigilance Hub access for particular users (for example users from the communications team who may not need access to report details), organisation leads can restrict access to the tiles they can view when they log into the Vigilance Hub.

1. Select the ‘User Management’ tile 
2. Select the role type for the user from the drop-down menu
3. Select the User from the list
4. Select ‘Edit’ to the right-hand side of the Permissions block



5. For each tile that the user should not have access to, change the drop-down option from ‘Default’ to ‘Deny’. Only tiles that the user should have access should be set to ‘Default’



6. Click save

12. Revision history

Version Number	Date	Update made by
Final 1.0	2021.03	Tahira Jan
Updated Final 2.0	2021.06	Tahira Jan

13. Acronyms

Acronym	**Meaning**
ADR(s)	Adverse drug reaction(s)
Med Safety App	Med Safety mobile application
Mobile App	Mobile application
UMC	WHO Collaborating Centre for International Drug Monitoring, the Uppsala Monitoring Centre
WEB-RADR	WEB - Recognising Adverse Drug Reactions project
WHO	World Health Organization
AEFI	Adverse Events Following Immunisation
ICSRs	Individual case safety reports
NRA	National Regulatory Agency
EPI	Expanded Programme for Immunisation