



Surveillance System for Attacks on Healthcare (SSA)

Mobile Application User Guide

ver - 1.0

Table of Contents

Overview	3
Limitations	4
Summary	4
Login	5
Sign Out	9
Forgot PIN	10
Resetting PIN by One Time Password through the registered Mail-ID	11
Resetting PIN by answering the security questions	13
Partner Form	14
Personal Information	14
Attack Description	17
Attack Time and Location	19
Type of Attack	21
Victims of Attack	23
Follow Up Actions	25
Browse Forms	30
All Forms	31
Unsent forms	32
Submitted Form	33
Draft Forms	34
Contact WHO SSA Team	35
For Android	35
For IOS	36
Language	37
Notifications	38
Help	39
Terms & Conditions	40
FAQs	41

Overview

WHO's Surveillance System for Attacks on Health Care (SSA) is a global, standardized monitoring system to collect primary data of attacks on health care.

The SSA Mobile Application is designed to allow SSA contributors, including reporting partners, to easily report attacks on health care. Users will be able to save or submit attack reports offline and synchronize when data connection becomes available. All users are required to log in in the SSA Mobile App prior to reporting data.

The SSA Mobile Application is available on both Android and iOS Operating Systems. The App can be downloaded from the Google Play Store and App Store under the name "WHO SSA". The icon below is the App's logo.

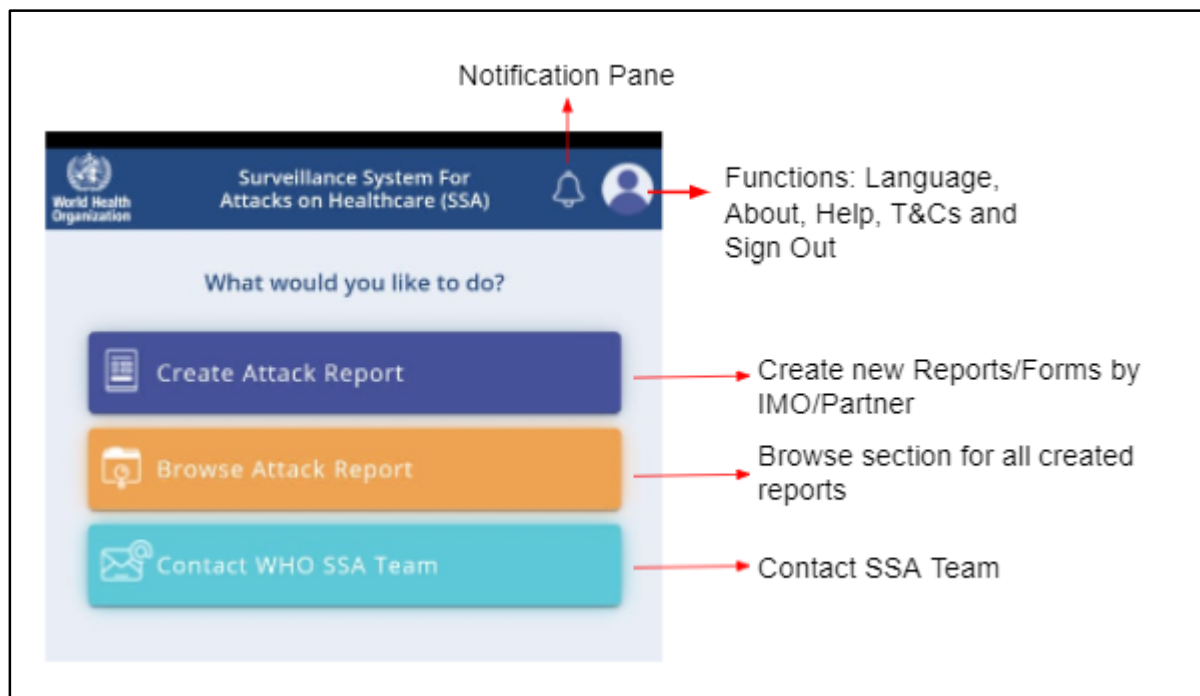


Limitations

1. Telephone should have a locking mechanism
2. Telephone shouldn't be jailbroken

Summary

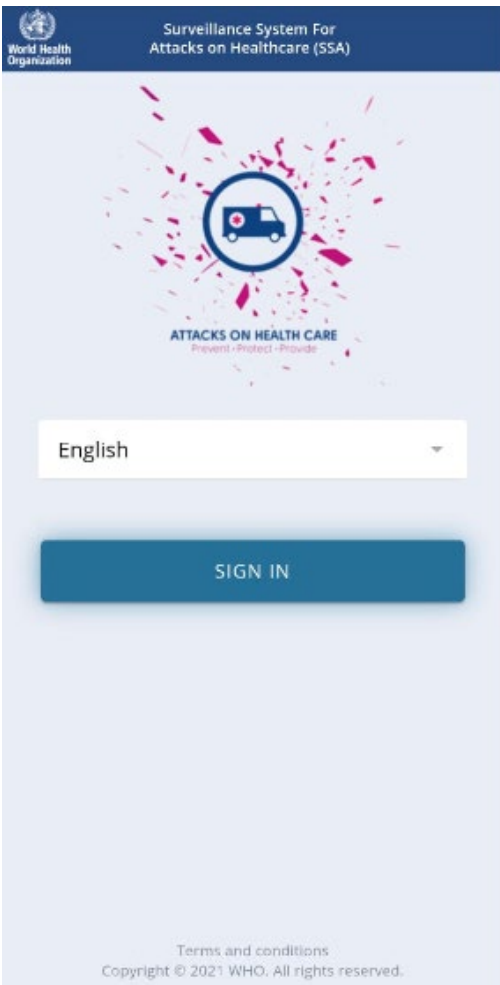
The SSA Mobile Application's home page contains various tabs and buttons which allow quick access to the different features of the Application. A summary of the different tabs and buttons of the home page can be found below.



*T&C: Terms and Conditions

*****Before using the SSA Mobile App, please make sure that your mobile device is secured with a PIN/Pattern/Password or biometric/fingerprint lock.***

Login

 <p>The screenshot shows the login interface of the Surveillance System For Attacks on Healthcare (SSA) mobile application. At the top, a dark blue header contains the World Health Organization logo and the text 'Surveillance System For Attacks on Healthcare (SSA)'. Below the header is a large graphic featuring a blue circle with a white ambulance icon, surrounded by a burst of red and pink petals. Underneath the graphic, the text 'ATTACKS ON HEALTH CARE' is displayed in blue, with the tagline 'Prevent - Protect - Provide' in smaller red text. A white dropdown menu is set to 'English'. Below this is a large blue button labeled 'SIGN IN'. At the bottom, there is a link for 'Terms and conditions' and a copyright notice: 'Copyright © 2021 WHO. All rights reserved.'</p>	<ul style="list-style-type: none">■ The login page has an option to Sign and change the SSA Mobile Application Language.■ Currently, only English/French are supported.■ English language is selected by default.■ After selecting the preferred language of your choice, click the SIGN IN button to Login.■ You would be required to enter the Email-ID and password in the screen that follows later on.■ After successful 'Sign In' users will be redirected to the 'Create PIN' Page.
--	---

World Health Organization

Surveillance System For Attacks on Healthcare (SSA)

Create PIN

Create a 4 digit PIN to secure your SSA account!

1 2 3

4 5 6

7 8 9

0 X

CREATE

- On the first login, you need to create the application PIN.
- This application PIN is the Personal Identification Number of 4 digits, which would be then further used in order to unlock the application.
- Once an application PIN is created, it would remain the same for all users of the application on the same mobile device.
- Please use the back “X” button in order to erase any entered number.
- Only numeric characters (0-9) are allowed as valid characters to set the application PIN.
- Once the PIN is finalized please use the CREATE button to move forward to the confirm PIN Page.



- Once a PIN is created, you need to re-enter the same PIN for confirmation. Please use the same process as creating a PIN page to enter the confirmation PIN.
- If for some reason you need to go back and want to set a new PIN please use the back button from the top left corner of your screen.
- Once you are done adding the PIN please use the CONFIRM PIN Page to move to the next screen.
- If the PIN from the previous screen and the confirmation PIN does not match, the application would not allow you to move forward, instead would prompt you to match both the PINs.
- Once the PIN and confirm PIN match you would move to the next page, to set security questions.

The screenshot shows the 'Security Questions' page of the Surveillance System For Attacks on Healthcare (SSA) mobile application. The header includes the World Health Organization logo and the title 'Surveillance System For Attacks on Healthcare (SSA)'. The page title is 'Security Questions'. Below the title, there is a paragraph: 'Answer security question(s) below. These questions will help us verify your identity in case you forget your PIN.' followed by a 'Please Note' section: 'Please Note : You must REMEMBER any one answer in order to recover your forgot PIN'. There are three questions, each with a text input field and a placeholder example: 'Q1.What is your favorite color?' with 'e.g. Red', 'Q2.Which is your favorite movie?' with 'e.g. Titanic', and 'Q3. What is your mother maiden name?' with 'e.g. Amanda'. At the bottom, there is a large blue 'SAVE' button.

World Health Organization

Surveillance System For Attacks on Healthcare (SSA)

Security Questions

Answer security question(s) below.
These questions will help us verify your identity in case you forget your PIN.

Please Note : You must REMEMBER any one answer in order to recover your forgot PIN

Q1.What is your favorite color?

e.g. Red

Q2.Which is your favorite movie?

e.g. Titanic

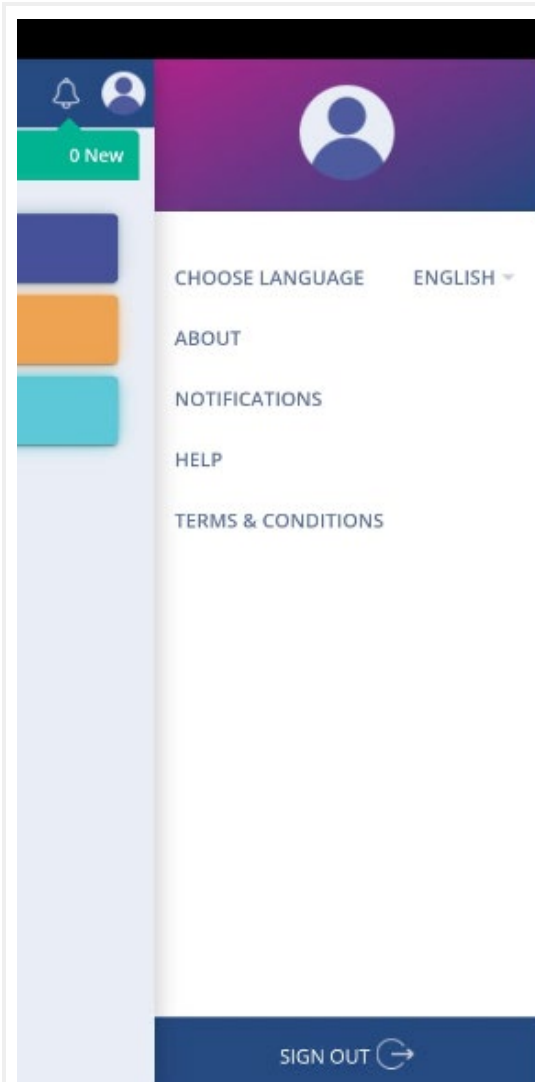
Q3. What is your mother maiden name?

e.g. Amanda

SAVE

- After creating the PIN, you will get a security questions Page.
- These are a set of security questions, which need to be answered in case you forgot your PIN.
- Kindly enter the relevant details for each of the questions, which are easy to remember, and click Save to save the data.
- Please answer all the questions to move to the next page.
- On successful submission of Security questions, you will be logged in to your account.
- After answering the questions, click 'Save' to move to the Home Page.

Sign Out



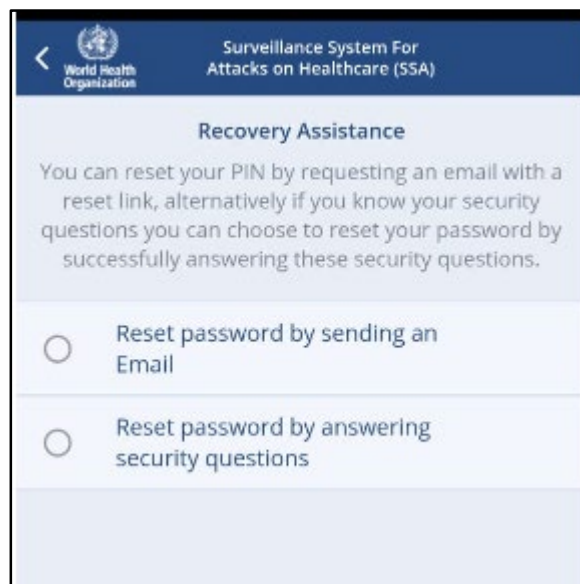
- The Profile section on the right side of the screen has the Sign Out option of logout from the SSA Mobile application.
- You can click on Sign out and will be redirected to the Sign In page.
- After sign-out, stored data will not be cleared.
- If the user logs in again on the same device without clearing the stored data, then they are able to view/edit the submitted contents as well.

Forgot PIN

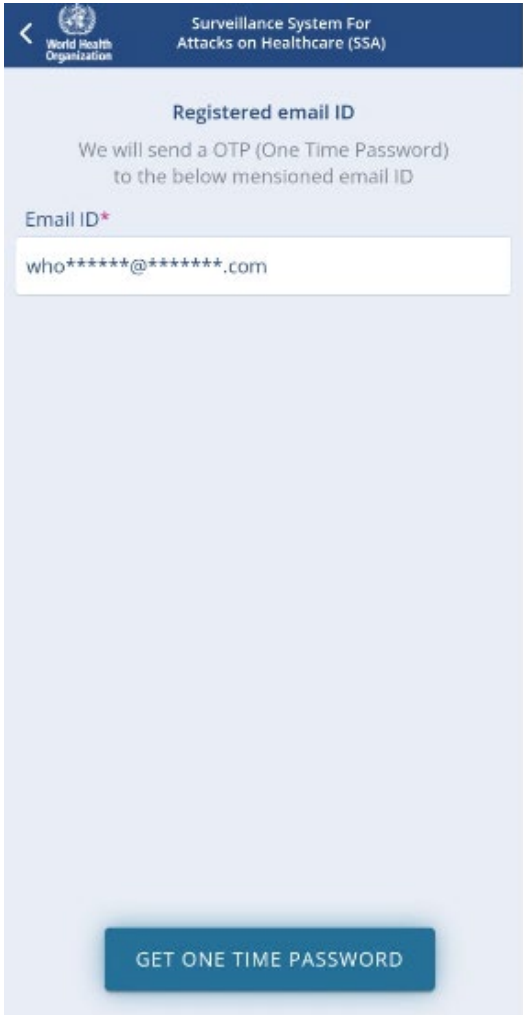
Forgot PIN is the option provided to the user while entering the PIN on the PIN Page. If the user wants to retrieve the existing PIN in order to login into the system, these forgot PIN options can be used.

There are 2 options provided to retrieve the PIN as shown below. You can select any one of them and click Continue to go ahead with that method.

1. Reset PIN by Email
2. Reset PIN by answering security questions



a. Resetting PIN by One Time Password through the registered Mail-ID



Registered email ID

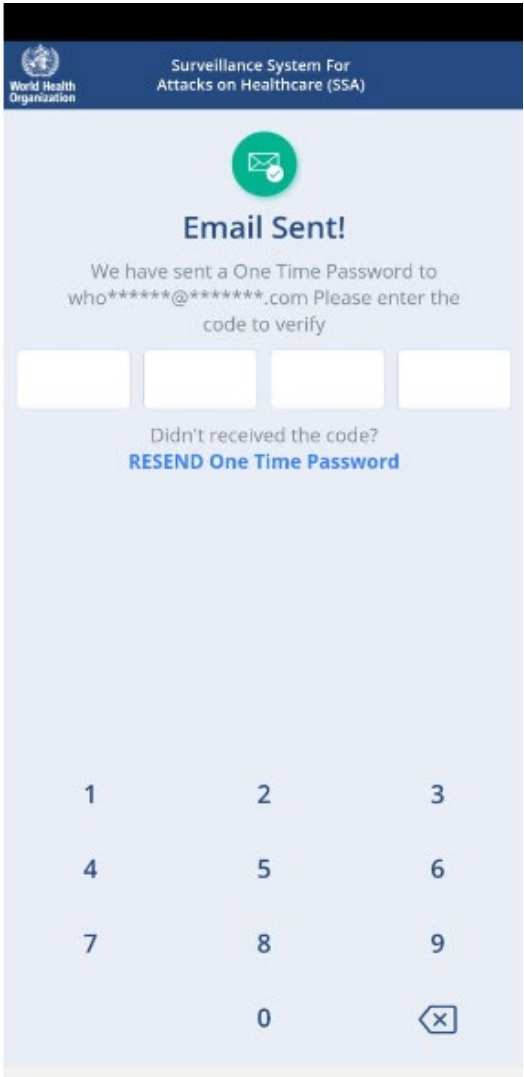
We will send a OTP (One Time Password) to the below mentioned email ID

Email ID*

who*****@*****.com

GET ONE TIME PASSWORD

- If you choose resetting your PIN via Email ID, you will be redirected to the confirm email page.
- You need to verify your Email ID on which you will receive one time password (OTP).
- You can click on Get one time password to get OTP on registered Email ID.
- If your Email ID is not correct you can click back and choose another method for resetting the PIN.



The screenshot displays the 'Email Sent!' screen of the Surveillance System For Attacks on Healthcare (SSA) mobile application. At the top, the WHO logo and the app title are visible. A green circular icon with a white envelope and a checkmark is centered above the heading 'Email Sent!'. Below this, a message states: 'We have sent a One Time Password to who*****@*****.com Please enter the code to verify'. There are four empty white boxes for entering the code. Below the boxes, a link 'RESEND One Time Password' is provided for users who did not receive the code. At the bottom, a numeric keypad is shown with digits 1-9, 0, and a backspace icon.

- You will be redirected to verify the OTP sent on your registered Email ID.
- You can enter the code received on your Email.
- If you did not receive the code by any chance, you can click on RESEND OTP to receive it again.
- Once you enter the correct OTP, you will be asked to reset the PIN.
- The Internet will be required to perform reset of PIN by internet verification.

b. Resetting PIN by answering the security questions



Surveillance System For Attacks on Healthcare (SSA)

Security Questions

Answer security question(s) below. These questions will help us verify your identity in case you forget your PIN.

Please Note : You can answer any one of the question correctly in order to recover your forgot PIN

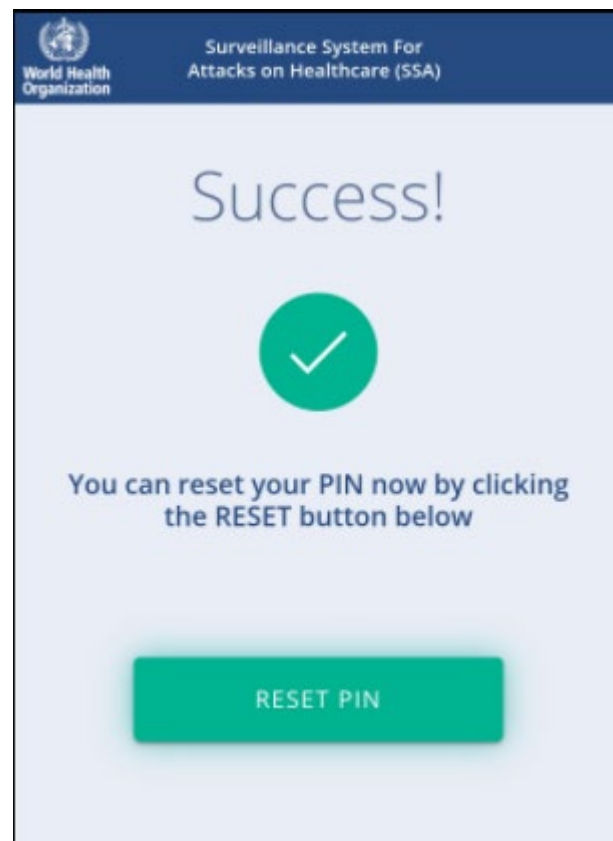
Q1.What is your favorite color?
e.g. Red

Q2.Which is your favorite movie?
e.g. Titanic

Q3. What is your mother maiden name?
e.g. Amanda

VERIFY

- If you choose resetting your PIN by answering security questions, you will be redirected to the verify security questions page.
- You need to answer any one of the 3 questions correctly and click verify.
- On successful verification of the answer, you will be asked to reset your PIN as shown below



Surveillance System For Attacks on Healthcare (SSA)

Success!



You can reset your PIN now by clicking the RESET button below

RESET PIN

Partner Form

The Partner Form can be used by reporting partners to report attacks on health care. The Mobile App forms collect the same data as the web-based SSA partner forms.



- Status: Not Submitted, Not uploaded: This gives the status of the current form with the number DRFT000001. As the form is neither submitted nor uploaded, it will be reflected in all the screens of the partner form. Here DRFT prefix refers to draft forms and 000001 is the number of the form which will be incremented for every draft form created. Similarly prefix will vary depending on type of form like UNSNT (for unsent form), FRM etc.
- The  sign is used to close the current form. On clicking it, it will ask to discard, save as a draft or close the current form.
-  is used to go back to the previous page.
- Step 4 of 6 indicates the step number/screen of the partner form.
- By clicking on the SSA, there will be a popup to close the form, discard or save it as a draft.

Note: If the form is discarded on Step 1 it will be discarded completely; If it is discarded at Step 2, it will be saved until Step 1.

a. Personal Information

World Health Organization

Surveillance System For Attacks on Healthcare (SSA)

DRFT000003

Status : Not submitted, Not uploaded

Step 1 of 6

PERSONAL INFORMATION

☐ I wish to remain anonymous

Full Name *

Full Name

Phone Number *

Phone Number

Email *

Email

Affiliation/Organisation

Affiliation

I am

Please select..

☐ Other

☐ I agree to be contacted for confirmation and/or further details

BACK NEXT

SAVE

- Personal information page refers to the information of the Partner who is reporting the attack.
- There is a checkbox provided if the partner wants to keep his/her identity anonymous. If this not checked, then Fullname, Email, and Phonenumber will become mandatory
- You can enter your Full Name, Email, and Phone number as a part of personal information. (You cannot enter anything else other than numbers in Phone number box)
- You can enter the details of the Affiliation/Organization that you work.
- After that you can provide details as to which category of partner do you belong to like Eyewitness, Victim, etc.

I am

☐ An eyewitness

☐ A Victim

☐ An eyewitness told me about the attack

☐ An eyewitness told someone, who then told me about the attack

CANCEL OK

- If your category does not match the dropdown, you can click on Other checkbox and enter the relevant details of your category.

Note: If you do not check the Other box, values will not be saved even if entered.

- The last checkbox is to get contacted from SSA with respect to the details you have provided. In case you check this, you will have to provide Mobile Number and Email.

	<ul style="list-style-type: none">■ Click Next to move to the Next Page of Partner form.■ Click Save to save the form. <p>Note: Even if you have checked “I want to be anonymous” but you wish to be contacted then you have to provide a Mobile number and Email as mandatory.</p>
--	---

b. Attack Description

World Health Organization

Surveillance System For Attacks on Healthcare (SSA)

Step 2 of 6

DRFT000001

Status : Not submitted, Not uploaded

ATTACK DESCRIPTION

Description *

Description about the attack

Immediate Impact

Description about the impact

Affected Health Resources

Health care Facilities

Please select..

Health care Transport

Please select..

Health care Personnels

Please select..

Health care Supplies / Assets

Please select..

- Attack description is the page required to fill the details of the attack that is being reported. There are various parameters of the attack defined in this page which can be filled based on the details available to the partner. It is a mandatory field and if it is not filled, the Next button would be disabled.
- Description - This is a mandatory field required to explain the description of the attack that is being reported by the Partner.
- Immediate Impact - You can enter the details of the immediate impact created due to the attack.
- Affected health resources - There are various health resources that may be affected by the attack are given in this section. You can select your relevant answer from the dropdown of each resource.
- Health Care Facilities: Based on Health care facilities affected or not, you can select YES, NO, or Unknown from the dropdown.
- Health Care Transport: Based on Health care transport affected or not, you can select YES, NO, or Unknown from the dropdown.
- Health Care Personnels: Based on Health care personnels affected or not, you can select YES, NO, or Unknown from the dropdown.
- Health Care Supplies/Assets: Based on Health care Supplies/Assets affected or not, you can select YES, NO, or Unknown from the dropdown.



Health care Warehouse / Storage

Please select..

Health care Patients

Please select..

☐ Other

Number of health transport affected

Number of facilities affected

Number of warehouse affected

BACK NEXT

SAVE

- **Health Care Warehouse/Storage:** Based on Health care Warehouse/Storages affected or not, you can select YES, NO, or Unknown from the dropdown.
- **Health care Patients:** Based on Health care patients affected or not, you can select YES, NO, or Unknown from the dropdown.
- If there is any other Health Resource affected apart from the ones provided, you can check on 'Other' and provide details of it.
- **Number of health transport affected:** You can enter the number of health transports affected by the attack.
- **Number of facilities affected:** You can enter the number of facilities affected by the attack.
- **Number of warehouse affected:** You can enter the number of warehouses affected by the attack.
- Click Back to move to the previous page of the partner form.
- Click Next to move to the Next Page of the Partner form.
- Click Save to save the form.

c. Attack Time and Location

DRFT000001
Status : Not submitted, Not uploaded

Step 3 of 6

ATTACK TIME AND LOCATION

Attack Date *

30/03/21

Attack Time

11:23 AM

Approximate time

Select

☐ Time Unknown

Country/Territory *

Afghanistan

Governorate / Province

Governorate / Province

Community / City / Town

Community / City / Town

GPS coordinate

GPS coordinate

Targeted health facility

Targeted health facility

■ Attack time and location is the page required to fill the time and location details of the attack that is being reported. There are various parameters of the attack related to time and location in this page which can be filled based on the details available to the partner.

■ Attack Date - This is a mandatory field required to mention the date of the attack that is being reported by the Partner.

■ Attack time - You can enter the exact Attack time by selecting the appropriate time from the given dropdown.

■ Approximate Time: If the exact time of the attack is not known, you can select the range of time the attack is suspected to have happened.

■ Time Unknown: If the time of the attack is not known, you can select this checkbox. If this checkbox is selected, you will not be allowed to enter details in the Attack time and Approximate time fields, and vice-versa.


■ Country/ Territory: This is a predefined value based on the country of the Partner.

Note: Partner will not be able to update the value in the forms.

■ Governorate/Province: You can enter the name of the Governorate/Province where the attack has occurred in this field.

■ Community/City/Town: You can enter the name of the community/city/town where the attack has occurred.

■ GPS coordinate: If you have the details of the GPS where the attack has occurred, you can enter the details here.

	<ul style="list-style-type: none"> ■ Targeted Health facility: You can provide the details of the Targeted health facility where the attack has occurred.
	<ul style="list-style-type: none"> ■ Affiliation: Affiliation is the type of supporting organization for which the facility, transport or persons are attacked. You can select any/multiple from the Government, NGO, Private, UN, Red Cross of which the attack has occurred. If there is any other organization not present in the list, you can check on Other and enter the details of the affiliation. ■ Type of Facility: You can select the type of facility provided by the affiliated organization from the dropdown. If there is any other facility not provided in the list, you can check on Other and enter the details of the facility. <div data-bbox="755 1096 1091 1564"> <p>Type of facility</p> <ul style="list-style-type: none"> <input type="radio"/> Primary <input type="radio"/> Secondary <input type="radio"/> Tertiary <input type="radio"/> Mobile Clinic <input type="radio"/> Pharmacy <p>CANCEL OK</p> </div> <ul style="list-style-type: none"> ● Click Next to move to Next Page of Partner form. ● Click Save to save the form.

d. Type of Attack

World Health Organization

Surveillance System For Attacks on Healthcare (SSA)

Step 4 of 6

DRFT000001

Status : Not submitted, Not uploaded

TYPE OF ATTACK

Attack Types

☐ Abduction/Arrest/Detention of health personnel or patients

Health Workers

Abduction Arrest Detention

Patients

Abductions Arrest Detention

☐ Removal of health care assets (e.g. transport, supplies, materials)

☐ Assault (without weapons)

Violence with individual weapons (knives, bricks, clubs, guns, grenades and improvised explosive devices (IED))

Violence with heavy weapons (requires more than one person to use such as firearms, tanks, missiles, bombs, mortars)

☐ Setting fire

- Type of Attack is the page required to get the details on the different types of attacks that could have happened. There are different types of attack categories listed in this section. You can select any/multiple based on your report.
- Abduction/Arrest/Detention of health personnel or patients - You can select this if any health worker or patient is abducted/arrested/detained. Upon selection, you can also enter the number of Health workers/Patients that are Abducted/Arrested/Detained in respective boxes.
- Removal of healthcare assets - You can select this attack if any of the health care assets have been removed like transport, supplies, materials, etc.
- Assault: You can select this attack if there is any assault involved in the attack without weapons.
- Violence with individual weapons: You can select this attack if there has been violence with weapons like knives, bricks, guns, grenades, or IED.
- Violence with heavy weapons: You can select this attack if there has been violence with heavy weapons that requires more than one person to use such as firearms, tanks, missiles, bombs, mortars, etc.
- Setting fire: You can select this attack if the fire has been set in the attack.

Step 4 of 6

☐ Setting fire

☐ Chemical agent

☐ Militarization of a health care asset

☐ Armed or violent search of health care personnel, facility or transport

☐ Obstruction to health care delivery (e.g. physical, administrative, legal etc)

☐ Psychological violence/threat of violence/intimidation

☐ Sexual assault

☐ Unknown

☐ Criminalization of health care

☐ Other

BACK NEXT

SAVE

- **Chemical Agent:** You can select this attack if there is any chemical agent used in the attack.
- **Militarization of health care assets:** You can select this attack if there has been the militarization of any healthcare asset.
- **Armed or violent search of healthcare personnel, facility or transport:** You can select this attack if there has been armed or violent search of healthcare personnel, facility, or transport.
- **Obstruction of healthcare delivery:** You can select this attack if there has been obstruction of any health care delivery such as physical, legal, etc.
- **Psychological violence/threat of violence/intimidation:** You can select this if the type of attack belongs to any of these categories.
- **Sexual Assault:** You can select this attack if there is any sexual assault involved in the attack
- **Unknown:** You can select this attack if the type of attack is unknown.
- **Criminalization of healthcare:** You can select this attack if there has been the criminalization of healthcare in the attack.
- You can check on 'Other' and enter different types of attacks if your attack does not belong to the above-mentioned type of the attack.
- Click Next to move to the Next Page of Partner form.
- Click Save to save the form.

e. Victims of Attack

World Health Organization

Surveillance System For Attacks on Healthcare (SSA)

Step 5 of 6

DRFT000003

Status : Not submitted, Not uploaded

VICTIMS OF ATTACK

Total Deaths

Health Care Providers

Auxiliary Health Staff

Patients

Others

Males

Females

Age <18

Age ≥ 18

- Victims of Attack is the page required to get the details about the victims that have been affected by the attack. Victims of the attack are classified based on death and injuries that could have happened during the attack.
- Total Deaths: You can mention the number of deaths that have occurred in the attack.
- Further, these numbers of total deaths can be divided into deaths of Healthcare providers, Auxiliary Health staff, Patients, and others.

Note: Total deaths cannot be less than the sum of Healthcare providers, Auxiliary health staff, Patients, and others.

- Males/Females and Age Group - You can enter the number of deaths based on the Gender in respective Columns of Males and Females. Also, the number of deaths in the age group of less than or greater than 18 can be entered in respective boxes.

Note: Total deaths cannot be less than the sum of Males and Females. Also, Total deaths cannot be less than the sum of Age<18 and Age>=18.

Step 5 of 6

Age <18	Age ≥ 18
<input type="text"/>	<input type="text"/>

Total Injuries
<input type="text"/>

Health Care Providers	Auxiliary Health Staff
<input type="text"/>	<input type="text"/>

Patients	Others
<input type="text"/>	<input type="text"/>

Males	Females
<input type="text"/>	<input type="text"/>

Age <18	Age ≥ 18
<input type="text"/>	<input type="text"/>

BACK

NEXT

SAVE

- **Total Injuries:** You can mention the number of injuries that have occurred in the attack.
- Further, these numbers of total injuries can be divided into injuries of Healthcare providers, Auxiliary Health staff, Patients, and others.

Note: Total Injuries cannot be less than the sum of Healthcare providers, Auxiliary health staff, Patients, and others.

- **Males/Females and Age Group -** You can enter the number of injuries based on the Gender in respective Columns of Males and Females. Also, the number of injuries in the age group of less than or greater than 18 can be entered in respective boxes.

Note: Total Injuries cannot be less than the sum of Males and Females. Also, Total deaths cannot be less than the sum of Age<18 and Age>=18.

- Click Next to move to the Next Page of Partner form.
- Click Save to save the form.

f. Follow Up Actions

Surveillance System For Attacks on Healthcare (SSA)

DRFT000001

Status : Not submitted, Not uploaded

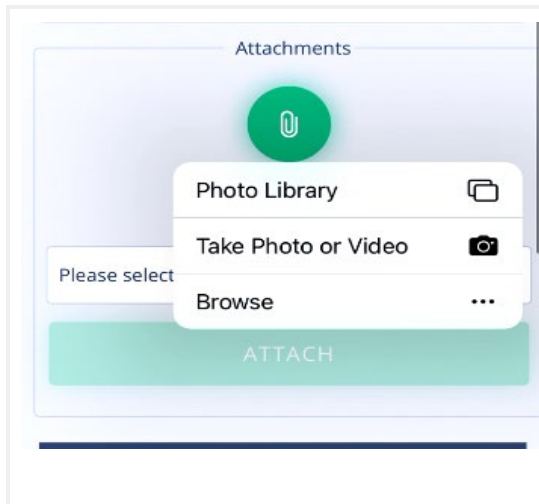
DESCRIBE ANY FOLLOW UP ACTIONS TAKEN

Follow up Actions

Description about the attack








- Follow-up actions are the page where the partner can describe or attach the actions taken by him/her after the attack.
- Follow up Actions: You can write the details of the actions taken as a part of the follow-up for the attack.
- Attachments: You can attach any file as a part of proof for the follow-up action.

iOS Attachments



- For iOS, you can add pictures/videos from the 'Photo Library' .
- You can directly take a photo or video by using 'Take Photo or Video'. After taking the photo or video, 'Use Photo' / 'Use Video' option to include it in the attachment.
- You can browse photos/videos from different sections by using the 'Browse' option.

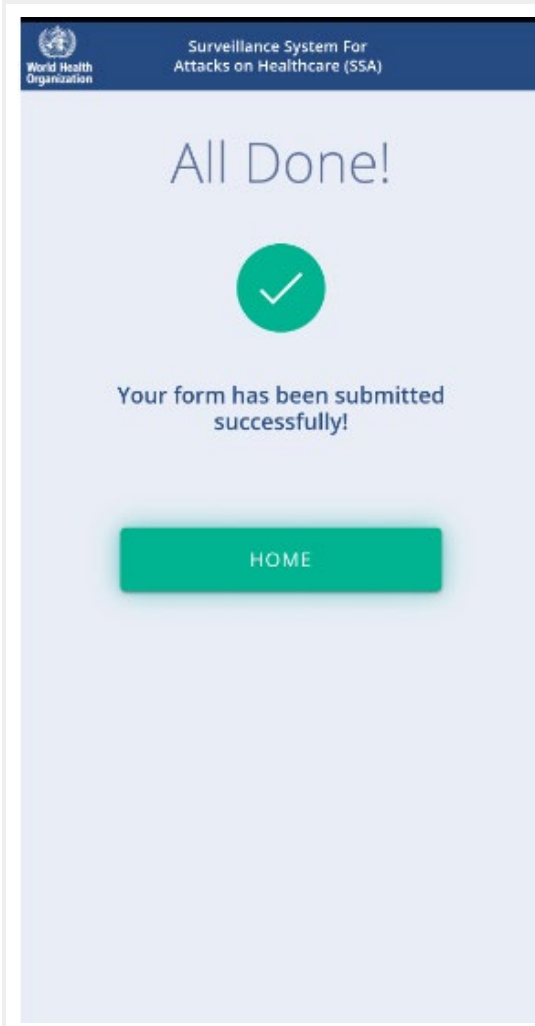
Android Attachments

<p>BROWSE FILES IN OTHER APPS</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  Bug reports </div> <div style="text-align: center;">  Drive </div> <div style="text-align: center;">  Drive </div> <div style="text-align: center;">  Drive </div> </div> <p>RECENT FILES ON PHONE</p> <div style="display: flex; justify-content: flex-end; align-items: center; margin-bottom: 10px;">  </div> <div style="margin-bottom: 10px;">  <div> <p>Screenshot_2021-05-24-11-56-20-62...</p> <p>11:56 am 348 kB JPG image</p> </div> </div> <div>  <div> <p>Screenshot_2021-05-24-11-56-18-99...</p> </div> </div>	<ul style="list-style-type: none"> ■ For android, on click of attachments you will be redirected to a page from which the user can browse the folder to select the attachment.
---	---

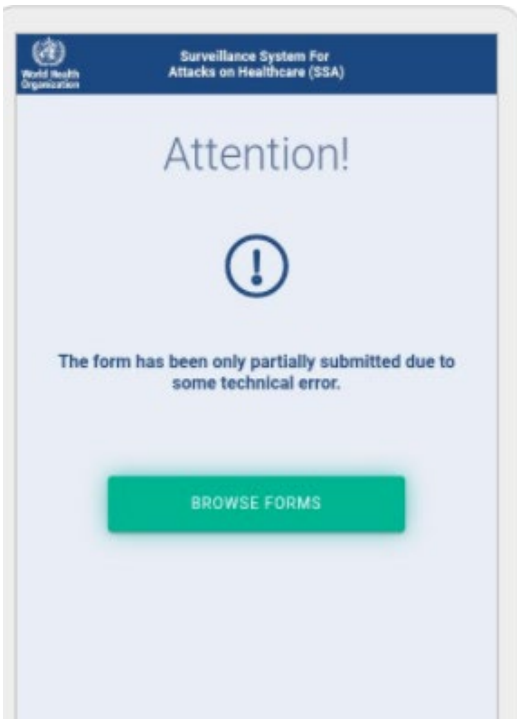
<p>Choose file type</p> <hr/> <div style="margin-bottom: 10px;"> <input checked="" type="radio"/> Please select.. </div> <div style="margin-bottom: 10px;"> <input type="radio"/> Photos </div> <div style="margin-bottom: 10px;"> <input type="radio"/> Video </div> <div style="margin-bottom: 10px;"> <input type="radio"/> Satellite image </div> <div style="margin-bottom: 10px;"> <input type="radio"/> International media report </div> <div style="margin-bottom: 10px;"> <input type="radio"/> Police report </div> <div style="margin-bottom: 10px;"> <input type="radio"/> Partner Information/Report </div> <div style="margin-bottom: 10px;"> <input type="radio"/> Local/National Media Source </div> <div style="margin-bottom: 10px;"> <input type="radio"/> Other </div> <hr/> <div style="display: flex; justify-content: flex-end; gap: 20px;"> CANCEL OK </div>	<ul style="list-style-type: none"> ■ After selecting attachment you need to select any file type from the dropdown and attach it. ■ If your file type is not present in the dropdown, you can select Other and add the attachment. <p>Note: You can add only one attachment as the type 'Other'.</p>
--	---

The screenshot shows the 'Step 6 of 6' screen of the 'Surveillance System For Attacks on Healthcare (SSA)' mobile application. The header includes the World Health Organization logo and a close button (X). The form displays the identifier 'DRFT000013' and the status 'Status : Not submitted, Not uploaded'. A section titled 'DESCRIBE ANY FOLLOW UP ACTIONS TAKEN' contains a 'Follow up Actions' label and a text input field with the placeholder 'Description about the attack'. Below this is an 'Attachments' section with a warning: 'PLEASE PAY ATTENTION TO THE ATTACHMENT SIZE AS THIS MAY TAKE SOME DATA USAGE'. It features a green circular icon with a paperclip, the text 'No file chosen', a dropdown menu with 'Please select..', and a green 'ATTACH' button. A 'FILE' section shows a list of attachments, including 'Screenshot_2021-05-24-11-56-26-71.jpg' with a red 'X' icon for removal. At the bottom, there are three buttons: 'BACK' (blue), 'SAVE AS DRAFT' (green), and 'SUBMIT' (dark blue).

- By clicking X on the attached file you can remove the attached file.
- Once these details are filled you can Save this partner form as a draft for future modifications. By clicking Save as draft, the form will be saved as draft and will be redirected to draft forms in the “Browse Forms” section.
- You can submit the form to the server if you have entered all the details from your side.
- If you are on a cellular network while submitting the form, the system would ask for a confirmation before submitting the form to the server.
- If we do not accept the submission, the form will move to the Unsent form section and will not be submitted.



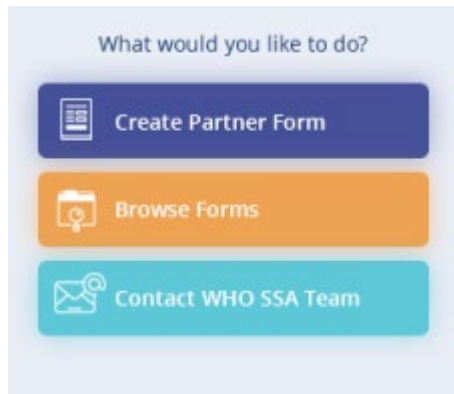
- Once the form is submitted, you will be shown a Success message on the Screen
- You can click on Home to return to the home screen of SSA Application.



- In case of failure of form submission, the below screen will appear stating that form has been partially submitted due to technical errors.
- You can click on Browse forms to go to the Browse forms page and check the status.
- In the browse form section you can be able to browse the form in the unsent section and try to resubmit the form.

Browse Forms

Once the Partner Form has been “submitted”, “discarded” or “saved as draft”, the form will be available in the “Browse Forms” section.






In this section, you will be able to find all the forms created by the partner. You can also see the unsent forms which have not been submitted due to any connection error.

Note: As per the status of the form i.e. submitted, draft or unsent, Form number with prefixes <FRM.....>, <DRFT.....> and <UNST.....> will be saved in Browse forms.

a. All Forms

The screenshot shows the 'Surveillance System For Attacks on Healthcare (SSA)' mobile application. At the top, there is a header with the WHO logo and the title 'Surveillance System For Attacks on Healthcare (SSA)'. Below the header, there are four tabs: 'All', 'Unsent', 'Submitted', and 'Drafts'. The 'All' tab is selected, and the screen displays a list of forms under the heading 'ALL FORMS'.

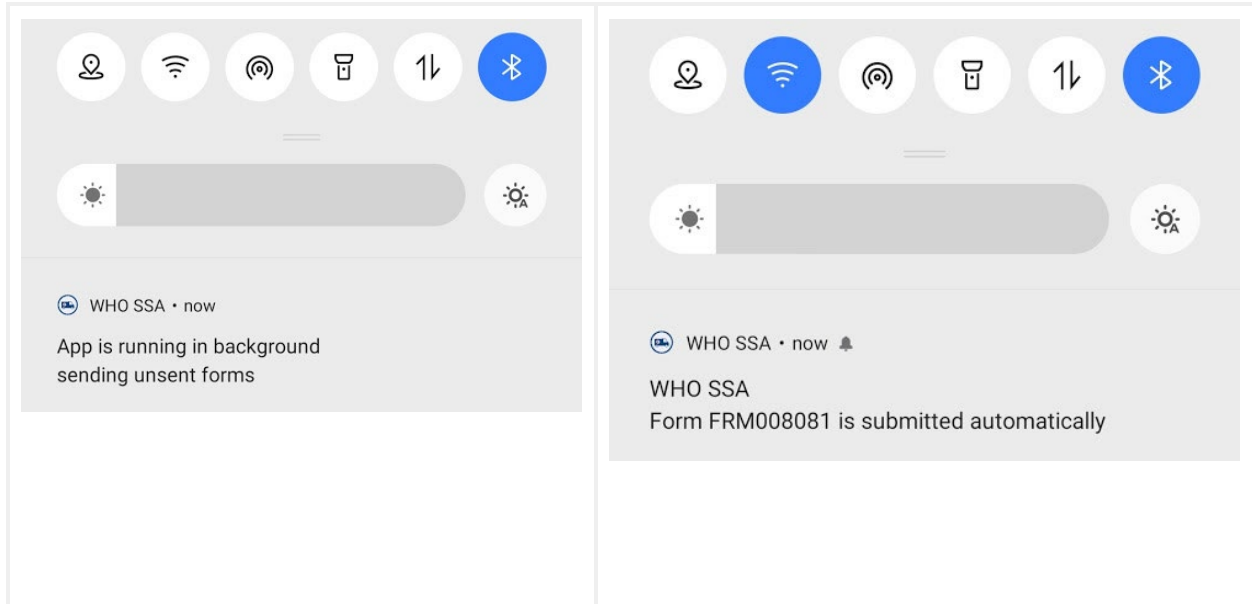
Form ID	Attack Date	Report Date	Status
DRFT000009	30/03/21	30/03/21	Unsent
DRFT000007	30/03/21	30/03/21	Unsent
DRFT000006	30/03/21	30/03/21	Unsent
FRM007898	30/03/21	30/03/21	Submitted
FRM007894	30/03/21	30/03/21	Submitted
FRM007891	30/03/21	30/03/21	Submitted

- This section of the forms contains a list of all the forms which are created by the partner.
 - In total these forms are categorized into 3 different types
 - Unsent forms
 - Submitted forms
 - Draft forms
 - You can click on the form number to open the respective forms.
 - Attack Date and Report Date shown in the screenshot indicates when the attack happened and at which date it was reported.
 - The PINK symbol indicates the current status of the form i.e. draft, unsent or submitted.
-  indicates the unsent form. Unsent forms are ones that are not uploaded to the server
-  indicates the submitted form. You can click on the form to view the submitted data.
-  indicates the forms which are in draft. You can click on this form to make changes and submit the form.
- On clicking the back arrow, you will be redirected to Home Screen.

b. Unsent forms



- This section of browse forms contains a list of the unsent forms which have been created but not submitted due to connection/network issues.
- There is an option to Upload the form directly by clicking on the green upload button. If the Internet is made available the application would try to upload the form to the server. Here the logic is that the user does not need to go through the form submission process by clicking on the form. Instead the form can be directly submitted from the upload button.
- Attack Date and Report Date is shown in the screenshot indicating when the attack happened and at which date it was reported.
- On clicking the back arrow, you will be redirected to Home Screen.
- If you have tried to Submit the form without the internet it will get saved in the Unsent section. When the internet is available, if the application is running in the background, it will Submit the unsent form and send the notification on the screen.
- If any forms are unsent and the app is killed, you will get a notification after 24 hours that the form is unsent.



c. Submitted Form

The screenshot shows the 'Submitted Forms' section of the mobile application. At the top, there is a header with the World Health Organization logo and the text 'Surveillance System For Attacks on Healthcare (SSA)'. Below the header, there are four tabs: 'All', 'Unsent', 'Submitted' (which is highlighted), and 'Drafts'. The main content area is titled 'SUBMITTED FORMS' and lists five forms: FRM007926, FRM007925, FRM007898, FRM007894, and FRM007891. Each form entry displays the form ID, the Attack Date, and the Report Date, all of which are 30/03/21. To the right of each form entry, there are three icons: a document, a magnifying glass, and a trash can.

- This section of the forms contains a list of the Submitted forms that are already saved and submitted to the server.
- You can click on the form to view the details of the attack.
- The submitted forms cannot be edited. They can be only viewed.
- Attack Date and Report Date shown in the screenshot indicates when the attack happened and at which date it was reported.
- On clicking the back arrow, you will be redirected to Home Screen.

d. Draft Forms



DRAFTS	
DRFT000009	<div>Attack Date: 30/03/21</div> <div>Report Date: 30/03/21</div>
DRFT000007	<div>Attack Date: 30/03/21</div> <div>Report Date: 30/03/21</div>
DRFT000006	<div>Attack Date: 30/03/21</div> <div>Report Date: 30/03/21</div>
DRFT000002	<div>Attack Date: 30/03/21</div> <div>Report Date: 30/03/21</div>
DRFT000001	<div>Attack Date: 28/02/21</div> <div>Report Date: 30/03/21</div>

- This section of browse forms contains a list of the Draft forms that are saved in the App but not submitted.
- You can click on the form to edit the details of the attack.
- Once the editing is completed you can save the form as a draft or submit the form.
- Attack Date and Report Date shown in the screenshot indicate when the attack happened and at which date it was reported.
- On clicking the back arrow, you will be redirected to Home Screen.

Contact WHO SSA Team

For Android

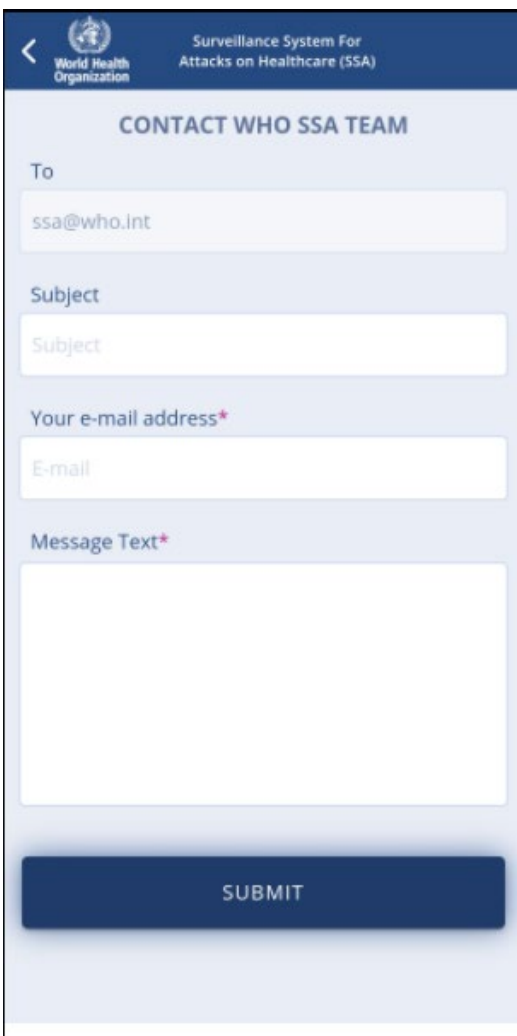
The screenshot shows the 'CONTACT WHO SSA TEAM' screen. At the top, there is a blue header with the WHO logo and the text 'Surveillance System For Attacks on Healthcare (SSA)'. Below the header, the title 'CONTACT WHO SSA TEAM' is displayed. The form contains the following fields:

- To:** ssa@who.int
- Subject:** Subject
- Your e-mail address*:** E-mail
- Message Text*:** (A large text area for the message)

A blue 'SUBMIT' button is located at the bottom of the form.

- The Home page of the app has the option to Contact the WHO SSA Team.
- On clicking that tab, you will be redirected to the page as shown.
- You can enter the details in the sections of Subject, Email and Message Text according to your reason for contacting.
- You can click on Submit to Submit your feedback/query/reason for contacting WHO SSA Team.
- To move back to the HOME page click the back button.

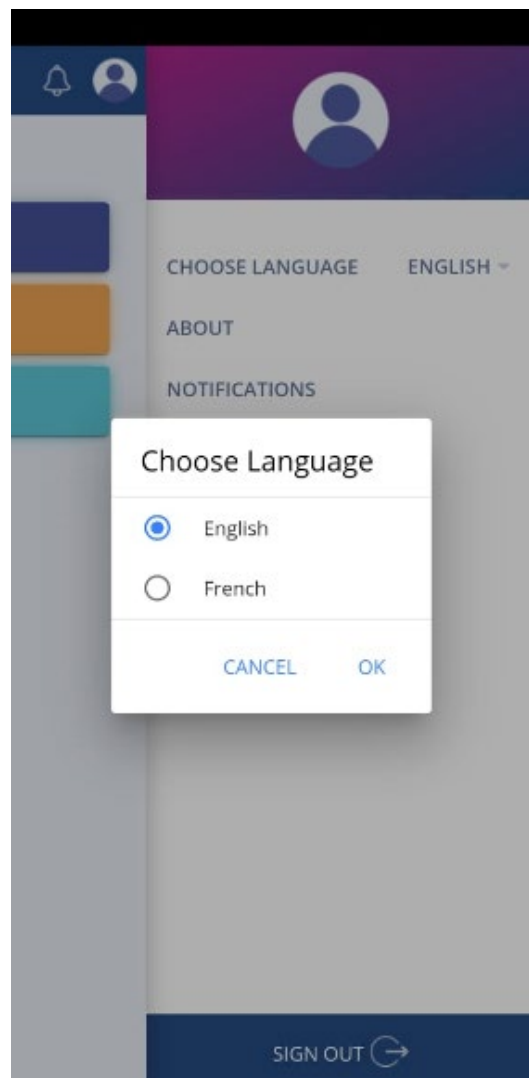
For IOS



The screenshot shows a mobile application interface for the 'Surveillance System For Attacks on Healthcare (SSA)' by the World Health Organization. The title bar is dark blue with a back arrow, the WHO logo, and the text 'World Health Organization' and 'Surveillance System For Attacks on Healthcare (SSA)'. Below the title bar, the section is titled 'CONTACT WHO SSA TEAM'. The form contains four input fields: 'To' (pre-filled with 'ssa@who.int'), 'Subject' (pre-filled with 'Subject'), 'Your e-mail address*' (pre-filled with 'E-mail'), and 'Message Text*' (a large empty text area). At the bottom of the form is a dark blue button labeled 'SUBMIT'.

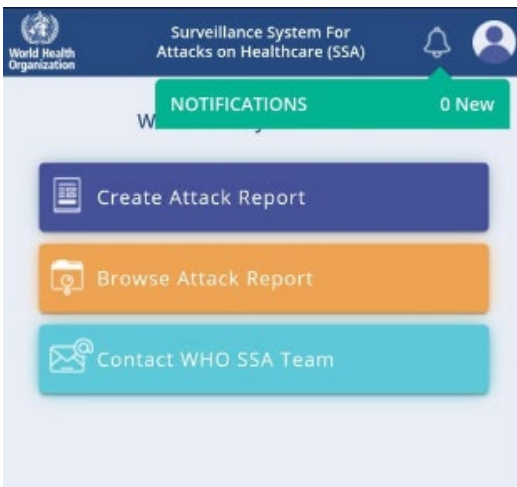
- The Home page of the app has the option to Contact the WHO SSA Team.
- On clicking that tab, you will be redirected to the page as shown.
- You can enter the details in the sections of Subject, Email and Message Text according to your reason for contacting.
- You can click on Submit to Submit your feedback/query/reason for contacting WHO SSA Team.
- To move back to the HOME page click the back button.

Language



- The Profile section on the right side of the screen has the option to change the language of the SSA application.
- You can click on the Choose Language option in the profile section and select your preferred language.
- There are 2 options currently between English and French.

Notifications





In-App Notification

- The Profile section on the right side of the screen has the option to check the In app notifications.
- You can click on the notification and you will be redirected on the Bell icon of the home screen.
- It will display the number of unseen notifications like App updates, form not sent etc.

System Notifications

- These are system notifications which will display in your device every 24 hours and 48 hours.
- These notifications include forms not submitted due to internet connectivity issues, app is running in the background and submission is processed and reports/forms submitted offline.

Help

< 
Surveillance System For
Attacks on Healthcare (SSA)


HELP

Contact support at ssa@who.int if you experience any issues with the SSA Mobile App. To find out more about the Attacks on Health Care initiative or the SSA, visit [WHO's website](#).

What data will be publically available once an attack is reported on the SSA?

The SSA publishes data that is collected and verified by WHO on the affected health resources, types of attacks and number of affected personnel. Information such as the date of an attack, the country in which it occurred and its associated certainty level is also publically available.

Under WHO's definition, what are attacks on health care?

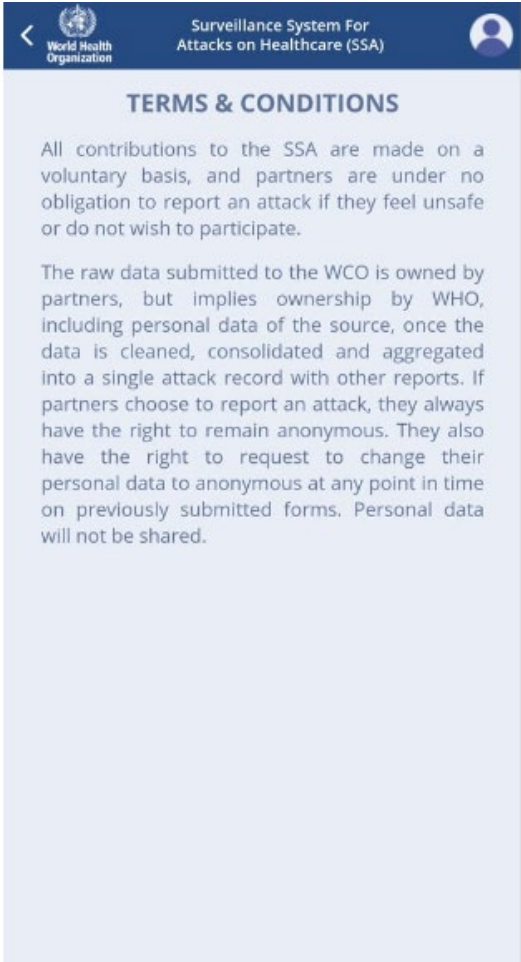
WHO defines an attack on health care as any act of verbal or physical violence or obstruction or threat of violence that interferes with the availability, access and delivery of curative and/or preventive health services during emergencies. The nature and types of attacks vary across contexts and can range from violence with heavy weapons to psychological threats and intimidation.

Who can report attacks on health care via the SSA?

SSA contributors include the health sector

- The Profile section on the right side of the screen has the help section for the SSA Mobile Application
- You can click on the help to get some FAQs with respect to the Application.
- The Help section gives you an insight on what kind of attacks are there on healthcare, who can report such attacks etc.
- You can contact support directly by clicking ssa@who.int and visit WHO website by clicking on WHO's website.
- You can click on back button to go back to the home page

Terms & Conditions

 <p>TERMS & CONDITIONS</p> <p>All contributions to the SSA are made on a voluntary basis, and partners are under no obligation to report an attack if they feel unsafe or do not wish to participate.</p> <p>The raw data submitted to the WCO is owned by partners, but implies ownership by WHO, including personal data of the source, once the data is cleaned, consolidated and aggregated into a single attack record with other reports. If partners choose to report an attack, they always have the right to remain anonymous. They also have the right to request to change their personal data to anonymous at any point in time on previously submitted forms. Personal data will not be shared.</p>	<ul style="list-style-type: none">■ The Profile section on the right side of the screen has the Terms & Conditions section for the SSA Mobile Application■ You can click on the TERMS & CONDITIONS to know the terms of being a partner with respect to the Application.■ These Terms & Conditions describe that the partner cannot be forced to submit or report the attack. Also any Personal data is not shared with anyone.■ You can click on back button to go back to the home page
---	--

FAQs

How do I download the app?

The SSA Mobile Application is available on both Android and iOS Operating Systems. The App can be downloaded from the Google Play Store and App Store under the name "WHO SSA". The icon below is the App's logo,




Click 'Download' to download the app.

How secure is it to report attacks data through the app for the user?

WHO SSA app will be opened only if the device is secured with either Pattern/ Passwords/ Biometric. On opening the app, the user needs to enter a PIN. The data is submitted over a secure HTTPS channel to the server. HTTPS- Hypertext Transfer Protocol Secure the communication protocol is encrypted using transport layer security or, formerly, Secure Sockets Layer (SSL). HTTPS ensures protection from eavesdroppers and man-in-the-middle attacks. In the app, the user name will not be displayed. If the app is not used for more than 15 mins either in the foreground or background then automatically the user will be moved to the 'Enter PIN' page.

The application says "Please enable device security first before using the app" what should I do?

To open the WHO SSA app, the device has to be secured. To enable the device security please follow the below-mentioned steps,

1. Open the **Settings** app 
2. Tap Fingerprint, face & password
3. Based on the convenience select any one type either Pattern/Password/Biometric and add the password
4. After entering the password, close the settings app and open the WHO SSA app.

What do I do if I forget my PIN?

We are able to reset the PIN by either answering the security questions/generating the OTP. To reset the PIN please follow the steps in the **Forgot PIN** section of the document.

How do I change the language?

We are able to change the language while either before 'SIGN-IN' or after 'SIGN-IN'. To change the language please follow the steps in the [Language](#) section of the document.

Actions to be taken when an update is available

When there is an app update, if the user is connected to the internet then an In-app notification will be generated. Go to the Play Store/ App Store and search based on the keyword 'WHO SSA'. The following icon is the app log,



Click on the 'Update' button, the app will be updated and the account details, Submitted, Unsent, Drafts Forms/Reports data will persist after the update.

Will I be able to use the same device for other Partners/IMO?

Yes, we can able to use the same device for other Partners/IMO, but please note the below-mentioned points,

1. As the security questions are device-based same security answers will be considered
2. As the PINs are also device-based same the user has to use the same 'PIN'
3. On switching between the accounts drafted/submitted forms/reports data will not be removed, based on the logged-in user forms/reports will be displayed
4. Data will not be removed from the device unless the user removes the stored data.

How and When can I close the app?

You can close the app when there isn't any attack report to submit by clicking on the device back button and tap on 'YES' in the confirmation pop-up. In case if there are any unsent forms/reports, then on using the device back button app will be closed and moved to the background and it will not ask for the confirmation popup.

How does the autosave work?

During the click of 'NEXT', while filling the form/report the autosave functionality will save the data of the previous steps.

What will happen to the report if I close the app in between?

On closing the app in between while filling the form/report, it will be moved to the 'Drafts' as we have autosave functionality data will be saved till the previous step.

Are there any restrictions on the type of attachment?

No, there are no restrictions on the type of attachment. If the attachment type is not available on the drop-down please select 'Other' as an option.

Note: There can be multiple attachments for all the types except 'Other'.

How to report a new attack if I don't have the internet?

WHO SSA app allows the user to create a new attack report offline. Users can draft them or submit them. On submitting the report offline, the report will be moved to 'Unsent' tabs under the 'Browse' menu. If the app is running in the background and when the internet is available (Either Mobile Data or Wifi) then automatically the report will be submitted to the server. If the app has been killed or the internet is not available for 24/48 hours when a report is in the 'Unsent' tab then a system notification will be generated. Users can submit the report by clicking on the Upload button in the browse report tab.

How to report a new attack report if I am on Cellular network?

As the data lite users are able to submit the report in the Cellular network as well, if the attachment size is larger, then it will take time to complete the submission. But the user can still submit the report using the Cellular network.

What will happen if I 'kill' the app?

If the app is killed and there is an unsent report in the 'Browse' menu then reports won't be submitted automatically. But system notification for the not submitted reports will be generated. On killing the app while creating a report, the report will be moved to 'Drafts'. Users can edit the report from the draft section and Submit it.

How to save the attack in the draft?

If the report is in drafts then the user is able to edit the report. To draft a report click 'DRAFT' at the last step of the report. Also if the app has been closed in between while filing the report the report will be drafted.

Why is my report unsent and what is the further process?

Report can be in the "Unsent" tab if there is no internet or interrupted connection while

submitting the report. Users are able to submit the report when the internet is available by clicking on the 'Upload' button in the unsent tab or open the application with internet connectivity for automatic submission.

Will I be able to see all my rejected reports?

No, the user will not be able to see all the rejected reports. Only the reports submitted by IMO on a particular mobile device will be seen by the user.

Will I be able to see all the reports after the reinstallation of the app?

No, if the user uninstalls the application then all the stored details including account details will be removed.