



ATTACKS ON HEALTH CARE

Surveillance System for Attacks on Health Care (SSA)

METHODOLOGY
VERSION 1.0



**World Health
Organization**

December 2018
WHO/WHE/EMO/2019.2/BRO

Surveillance system for attacks in health care (SSA): methodology

ISBN 978-92-4-151520-7

© **World Health Organization 2019**

Some rights reserved. This work is available under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 IGO licence (CC BY-NC-SA 3.0 IGO; <https://creativecommons.org/licenses/by-nc-sa/3.0/igo>).

Under the terms of this licence, you may copy, redistribute and adapt the work for non-commercial purposes, provided the work is appropriately cited, as indicated below. In any use of this work, there should be no suggestion that WHO endorses any specific organization, products or services. The use of the WHO logo is not permitted. If you adapt the work, then you must license your work under the same or equivalent Creative Commons licence. If you create a translation of this work, you should add the following disclaimer along with the suggested citation: "This translation was not created by the World Health Organization (WHO). WHO is not responsible for the content or accuracy of this translation. The original English edition shall be the binding and authentic edition".

Any mediation relating to disputes arising under the licence shall be conducted in accordance with the mediation rules of the World Intellectual Property Organization.

Suggested citation. Surveillance system for attacks in health care (SSA): methodology. Geneva: World Health Organization; 2018. Licence: CC BY-NC-SA 3.0 IGO.

Cataloguing-in-Publication (CIP) data. CIP data are available at <http://apps.who.int/iris>.

Sales, rights and licensing. To purchase WHO publications, see <http://apps.who.int/bookorders>. To submit requests for commercial use and queries on rights and licensing, see <http://www.who.int/about/licensing>.

Third-party materials. If you wish to reuse material from this work that is attributed to a third party, such as tables, figures or images, it is your responsibility to determine whether permission is needed for that reuse and to obtain permission from the copyright holder. The risk of claims resulting from infringement of any third-party-owned component in the work rests solely with the user.

General disclaimers. The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of WHO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. Dotted and dashed lines on maps represent approximate border lines for which there may not yet be full agreement.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by WHO in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by WHO to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall WHO be liable for damages arising from its use.

Printed in Switzerland

CONTENTS

Background	3
1. Context	3
2. Rationale	3
3. Purpose	4
4. Objectives	4
5. Guiding principles	5
System Overview	7
1. Definition of attack	7
2. How does the SSA work?	7
2-1. Data notification and collection	7
2-2. Data Entry	8
2-3. Verification Method	8
2-4. Data Clearance	10
2-5. Data access	10
2-6. Data use	11
3. Terminology	12
4. Management and Coordination	12
5. Roles and Responsibilities of WHO	13
6. Roles and Responsibilities of other SSA contributors	17
7. Risks and Risk Management	18
8. Safety and Ethics	18
9. Data validity and bias	19
10. Maintaining objectivity	20
11. Monitoring and Evaluation	20
12. Support	20
Annex 1 Defining an attack	21
Annex 2 Data collection template	22
Annex 3 Information Flow	27
Annex 4 Glossary	29



BACKGROUND

1. Context

Health care, including medical personnel, health facilities, transport, and patients, is under attack in different parts of the world. Such attacks deprive people of urgently needed care, put the lives of health care providers at risk, undermine health systems and long term public health goals, and contribute to the deterioration in the health and well-being of affected populations. These attacks represent a gross violation of human rights for both health care workers and patients, affecting the rights to life, liberty, and health. The right to equitable access of health care outlined in the International Covenant on Economic, Social Cultural Rights has been signed and ratified by 164 countries, and the right to health is enshrined in the WHO constitution. Attacks are not only morally indefensible, but are a distinct breach of this international treaty that member parties are expected to uphold. Data suggests that many attacks take place in fragile states and complex emergencies where populations already face health and security inequities. An analysis of the Surveillance System for Attacks on Health Care (SSA) data in the first three quarters of 2018 found that reported attacks increased in the occupied Palestinian territory and Syrian Arab Republic in specific locations where unrest or conflict intensified, demonstrating that access to health care is at greater risk during periods where it may be needed most by the local population.

In 2015, the World Health Organization established the Attacks on Health Care (AHC) initiative. This initiative is a priority of WHO's Health Emergencies Programme.

The vision of the initiative is that essential life-saving health services must be provided to emergency-affected populations unhindered by any form of violence or obstruction.

The Surveillance System for Attacks on Health Care (SSA) is one of the outputs of this initiative. The body of evidence produced by the surveillance system will help to complement two outputs of the initiative:

support advocacy against attacks on health care and provide evidence on the effectiveness of best practices to minimize attacks and mitigate the consequences of attacks.

2. Rationale

Data on attacks on health care have not been systematically collected in a single repository, or made widely available to relevant stakeholders. To understand the extent and nature of the issue, and its impact on public health, a single, standardized surveillance system is needed. A system that is comprehensive and utilizes the same methodology across countries – with context-specific adaptations, as appropriate – will help to address the incomplete documentation of attacks. Such information can inform national and global advocacy efforts and risk reduction interventions to prevent attacks and mitigate their consequences to public health, particularly among the world's most vulnerable populations—those facing public health crises from a wide range of hazards including infectious diseases, conflict, natural events, and terrorism.

WHO has the mandate to develop a surveillance system to document attacks on health care in emergency settings. In 2012, the World Health Assembly adopted Resolution WHA65.20, which calls on WHO's Director General to "provide leadership at the global level in developing methods for systematic collection and dissemination of data on attacks on health facilities, health workers, health transports, and patients in complex humanitarian emergencies, in coordination with other relevant UN bodies, other relevant actors, and intergovernmental and non-governmental organizations."

Ideally, tracking and reporting on attacks on health care is an established part of health information collection that is undertaken and overseen by local health authorities. Recognizing that many attacks occur in fragile states or places facing complex emergencies, this monitoring may not be a routine

activity. There are likely to be many competing priorities for the relevant governments, and maintaining a highly sensitive system that captures all attacks will not take precedence. Additionally, attacks against health care can be ethnically and politically charged events.

Through the SSA, WHO aims to create a comprehensive, globally inclusive, and independent monitoring mechanism. Due to the multifaceted nature of attacks, an autonomous mechanism is best fit to collect data that is accurate and free of bias. The credibility of data that contains sensitive information is much more robust when collected independently. Where possible and appropriate, local authorities will be invited to submit information about attacks to the WCO, but the SSA is not contingent on governments' participation. The WHO leadership role mandated by Resolution WHA 65.20 ensures that the circumstances surrounding the event do not lead to biased or inaccurate information, and that the intended outcomes defined by the AHC initiative are achieved.

An effective surveillance system depends on close inter-agency work. A surveillance system is only as strong as the number of willing and consistent reporters. WHO works directly with partners on the ground to ensure that there is a wide and inclusive range of reporting contributors, and encourages partner organizations to inform other key actors in the area about the system and how to submit a report. These partnerships support a system that has a high sensitivity of reported attacks that are made publicly available in a timely manner.

On the global level WHO regularly communicates with partner organizations and authorities on the findings and encourages organizations to utilize the SSA as a tool for their own monitoring and advocacy efforts. WHO also relies on inter/agency communication for any reports of attacks faced by partner states to share with relevant country offices to open or bolster an attack report.

This document describes the methodology behind the SSA in detail.

3. Purpose

The purpose of the WHO Surveillance System for Attacks on Health Care (SSA) is to systematically collect and make available data on attacks on health care, and their immediate impact on health care in countries facing emergencies.

4. Objectives

The objectives of the SSA are the following:

- Collect, consolidate, and openly and regularly share reliable data on attacks on health care;
- Better understand the extent and nature of the problem of attacks on health care and the consequences for health care delivery and public health;
- Produce regular reports with consolidated data and trend analysis;
- Provide the evidence base from which to implement advocacy to stop attacks on health care; and
- Identify global and context-specific trends and patterns of violence to inform and implement risk reduction and resilience measures so that health care is protected and health services are available.

5. Guiding principles

The guiding principles of the SSA are the following:

- **High sensitivity:** The SSA contributors, including WHO and partner staff, are encouraged to share information about any and all attacks on health care for inclusion in the database;
- **Accuracy of data:** Data entered in the database and available for public viewing will be associated with a level of certainty, according to the SSA's verification method;
- **Transparency:** The SSA's purpose, objectives, definitions, and use will be stated openly and publicly;
- **Standardization:** The data that are collected and the process of verification within the SSA are standardized, since standardization allows for comparability of data across countries, and simplifies implementation in new settings;
- **Data sharing:** The SSA will follow WHO's mandate to inform and promote the field of health through the collection, analysis, publication and dissemination of attacks on health care data;
- **Timeliness:** Data collection and making data publicly available should occur as soon as possible after the notification of an attack;
- **Reliability:** A standardized data collection template and verification method have been built into the system to maintain data reliability;
- **Safety:** The personal information of sources and victims will be protected through publishing guidelines and data encryption processes;
- **Lawful and fair collection:** Personal identifying information will not be collected about victims of an attack, and contributors are given the option to report anonymously;
- **Confidentiality:** Confidentiality of personal data of both victims and sources will be respected and applied at all stages of data collection and sharing. Contributor personal information will not be shared publicly;
- **Data Security:** Personal data of sources will be kept secure and will be protected through appropriate measures against unauthorized modification, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer; and
- **Ownership of personal data:** Raw data sent by contributors is owned by these individuals. WHO assumes ownership of data that is cleaned, consolidated and aggregated.
- **Simplicity:** The online platform and corresponding reporting mechanisms have been developed to be straightforward, clear, and easy to use by contributors and focal points in country offices
- **Flexibility:** Issues that are identified with the workflow or online platform will be addressed and adapted accordingly



SYSTEM OVERVIEW

1. Definition of attack

WHO defines an attack as any act of verbal or physical violence, threat of violence or other psychological violence, or obstruction that interferes with the availability, access and delivery of curative and/or preventive health services. See annex 1 for further clarification.

2. How does the SSA work?

WHO commits to implementing the SSA, and to managing and sharing its findings at all levels. The designation of the AHC Focal Point at each country office is the decision of the WHO Representative. It is expected that the Incident Manager (IM) or Emergency Manager (EM), or in some cases, the Health Cluster Coordinator (HCC), of the country office will be the AHC focal point for a majority of the priority countries.

WHO Country Offices (WCO) reach out to all possible SSA contributors, including those of the health sector coordination group (and the protection and health clusters when activated), for collaboration. WCO staff and other SSA contributors located throughout the country notify the WCO about reported attacks on health care and gather information over time about such attacks.

The WCO enters the data in a public-facing global database that makes information widely available and can be used to generate automated dashboards and ad hoc reports at country, regional and/or global levels.

At the same time, WHO HQ collects daily information on individual attacks that can be found from open sources or that are reported by other routes and shares these with the relevant country immediately, to trigger further data collection / investigation and to provide additional sources and types of evidence. This data is also used to complete the global picture of attacks, taking into consideration countries where data is not reported through the SSA.

The country-specific data can then be used to inform joint advocacy and action for risk reduction and resilience.

The key features of this system are the following:

- 1) A variety of primary and secondary data sources providing information about attacks
- 2) An interactive and iterative process as more information becomes available at the country, regional and global levels
- 3) A single global database
- 4) The assignment of a level of certainty | associated with each reported attack
- 5) Data on the impact of health service delivery associated with each reported attack
- 6) The ability to generate automated dashboards from the available information

See Annex 3 for the information flow.

In the sections below, the information flow is explained further.

2-1. Data notification and collection

The SSA contributors notify WCO that an attack on health care may have happened and provide as much information as possible about the given attack.

The initial notification and any subsequent data are transmitted to the WCO via the widest possible range of transmission options (e.g. via the SSA, phone, email, paper, face-to-face, encrypted mobile application).

Data are collected at country level by partners and WCO staff. These data are triangulated by data gathered at the global level through open source platforms.

There is a web-based data template available to the SSA-designated partners.

The reporting form is the full length data collection template, and is only accessible through an internal dashboard page that requires a log in with a WHO Application Directory Service (ADS) or WIMS account (Annex 1). An ADS account allows users to sign in to any ADS-enabled web site or service designated by WHO, like the SSA that hosts the dashboard and the full length data collection template.

Anyone outside of WHO is capable of creating an ADS account, and logging on to the internal dashboard page. However, only certain ADS accounts defined as partners by WCOs will be able to access the full length reporting form. The internal dashboard page accessed with an ADS account by users that are not defined as partners will be identical to the public dashboard page.

The types of data that are collected are based on the questions in a standard SSA Data Collection template (see Annex 1).

The WCO works with partners to gather the data necessary to fully complete the SSA Data Collection template, as much as possible given the circumstances, access and availability of witnesses.

The data to be collected as per the SSA Data Collection template are the following:

- Description of the attack
- Description of immediate consequences to health service delivery
- Date of attack
- Location (e.g. name of town, facility, GPS coordinates)
- Identity and/ or type of source of data
- Health resources involved (e.g. health facility, ambulance, health worker, patient)
- Type of attack (e.g. abduction, shooting, threat of violence)
- Total deaths and injuries (by sex, age group and type)
- Description of immediate actions for re-establishing health services and follow-up for victims

2-2. Data Entry

As data are made available to the WCO, it is entered into the web-enabled secure global database by a designated WCO staff member, usually the designated AHC Health Information Manager (HIM) or Information Management Officer (IMO).

The data are then cleaned by the AHC HIM or IMO to standardize spelling and formatting and to eliminate duplicate reports. Multiple sources of information of the same attack from the SSA partners are grouped into a single attack report.

2-3. Verification Method

Once data are entered, each reported attack is assigned a level of certainty by the AHC HIM/IMO which conveys a level of confidence that the reported attack has occurred. The level of certainty applies to whether the attack occurred, but does NOT apply to the detailed data about the attack.

This level of confidence, reflecting the level of certainty that the event happened, is assigned based on the application of the SSA verification method.

There are four levels of confidence: "rumour", "possible", "probable", and "confirmed".

The SSA verification method uses standard criteria, based on the types and sources of information received about an attack.

Table 1: Criteria for determining the level of certainty of an attack on health care

Source of Information	Certainty level
<ul style="list-style-type: none"> • Social media post (Twitter or Facebook) OR • Hearsay OR • Form submission from anonymous source 	Rumour
<ul style="list-style-type: none"> • Media report from local or international news source OR • Communication from an organization not defined in the partner group that an attack has been made against them 	Possible
<ul style="list-style-type: none"> • One eyewitness accounts of the attack as told to one or more SSA partner OR • Two secondary accounts (not eyewitnesses) of the attack as told to one or more SSA partner(s) 	Probable
<ul style="list-style-type: none"> • Communication from an SSA partner that an attack has been made against them OR • One eyewitness account by someone from the SSA partner group OR • Two eyewitness accounts of the attack as told to one or more SSA partner(s) OR • Types and sources of information that would be graded as 'Probable' PLUS-A photo, video or satellite image of the attack or its aftermath, or an international media or police report that provides clear evidence of the attack 	Confirmed

The standard criteria for determining a level of certainty that an attack occurred can be found in Table 1.

As noted, the level of certainty does NOT apply to the detailed data about the attack. It is likely that different accounts from different sources or from different moments in time may capture different quantitative and qualitative data about the attack. These data, along with the source of the data, will be included in the database as associated sub-entries under the attack header.

The level of confidence associated with an attack does not change based on accumulating more of one type of source or evidence beyond that detailed in Table 1. For instance, many eyewitness or secondary accounts may exist, but only the numbers of eyewitness accounts and secondary accounts of the attack detailed in Table 1 are necessary for the level of certainty. Data from sources beyond those required for determining level of certainty are included in the data base as associated sub-entries.

For any other evidence that is not captured in this table, the report will be labelled by the Information Manager as a “rumour” until further information is collected.

For any reported attack, the WCO will work to maximize the amount and quality of data and sources to increase the associated level of certainty. Efforts to reach higher levels of confidence include regular communication with partner organizations working in the area and if possible, with local authorities. The role of the focal point in the country offices is not to be an investigative force, but to utilize inter-agency partnerships for gathering information and attaining higher levels of certainty.

2-4. Data Clearance

The WCO AHC focal point in-country, as well as the WHO Representative, review and clear the entry on a new attack, and its assigned level of certainty, before it becomes public on the database.

2-5. Data access

Once the data about an attack are entered, assigned a level of certainty, and cleared, the data are made available in a web-enabled, publicly-available secure global database.

Not all information from an attack report will be published to minimize the risk of disclosure of personal information of victims and data sources. Certain data points are always published and others are always suppressed in the public database. Furthermore, data can be withdrawn from the public database at any point if later deemed unsafe by WCOs.

Safeguarding the confidentiality of victims and contributors who share information about an attack is the main priority with data made available on a public database. Personal identification information about victims will never be collected. Personal data about partners is collected,

as it is integral for the accuracy assessment, but will never be shared publicly. To ensure that the other guiding principles of the SSA are met, particularly high sensitivity and accuracy, the continued confidentiality of sources is imperative, so that partners feel safe to report an attack without fear of identification. Data security and storage measures outlined in the ‘Risk Management’ section will be followed to guarantee protection of source information.

Additionally, there are characteristics of data that make it easier for a public user to attempt to identify an individual, either a victim or a source. These key characteristics are small sets of data, detailed statistics, and sensitive data. To ensure that the data is anonymous and protected from these characteristics, two categories with defined published and suppressed fields have been established.

Data in category B (not made public) can be used for analyses of attack trends and reports internally by WHO.

While discussions about attack reports will be made with local authorities whenever possible, the publication of data will be made without the consent of the government. This decision is based on several factors that outweigh a mandated agreement from governments. It is not the role and responsibility of Member States to provide data for this surveillance system, unlike other data collection mechanisms undertaken by WHO. In many cases, the independent nature of the monitoring system could benefit authorities to objectively demonstrate the trend and nature of attacks in their countries

Category A:

Category B:

Data that is made public	Data that is NOT made public
<ul style="list-style-type: none"> Country of attack location Date and time of attack Health resources affected by attack Type of attack Type of facility impacted Aggregate level data of death, injuries, and removal of personnel Level of Certainty 	<ul style="list-style-type: none"> Province and City/town of attack location Identities of source information Type of source data (eyewitness or not) GPS coordinates of reported attack Name of health facility and affiliation Description of attack, circumstances, and impact on health services Disaggregated data by sex, age and person type Follow-up actions taken

2-6. Data use

The data can be used to inform advocacy and programmatic priorities and interventions at national, regional, and global levels by WHO, collaborating partners, and other stakeholders. The data can also be used for further investigation and research.

In Article 2 of the WHO Constitution, the outlined functions require WHO to, “establish and maintain such administrative and technical services as may be required, including epidemiological and statistical services; to promote (...) research in the field of health; and to provide information (...) in the field of health.” The creation of a publicly accessible database is a step in the right direction towards raising awareness and minimizing attacks. Limiting the access and use of data to only a few organizations will lead to limited collaboration and ineffective actions. Attacks on health care are a problem that span a wide range of fields beyond public health, such as development, human rights, legal issues, and economic growth. For example, the achievement of the Sustainable Development Goals will be hindered if attacks continue unabated. The utilization of this data

by actors outside the health field is encouraged, and any attempt to limit the access and use of published data by WHO will shut out potential allies in the work towards ending these attacks.

Over the long-term, documentation, publication and international discourse of attack data are critical. Affected populations and local governments can use this data in rebuilding efforts, identifying health services gaps and prioritizing needs. Similarly, WHO will utilize this data for operational research on the impact of attacks on health service delivery and public health. Partner organizations will be able to use the trend data in discussions with both state and non-state actors about the protections they deserve in order to effectively serve relevant populations. Outside of health care delivery, other organizations with relevant mandates can use this data for accountability mechanisms.

Partner organizations and other advocacy actors, such as human rights, legal and local grassroots groups, can use the shared data for their own advocacy efforts and to add to their

respective monitoring systems. Furthermore, this information can inform organizations, including WHO, about the current climate and health system situation in different countries, which can affect programming and security decisions.

3. Terminology

The SSA uses standard terminology to facilitate the gathering, reporting, entry and aggregation of data.

The SSA terminology has been aligned as much as possible with the terminology used by similar data collection and reporting mechanisms.

See Annex 4 for the Glossary.

4. Management and Coordination

WHO leads and manages the implementation of the SSA, providing coordination and support to contributors. In settings in which the Health Cluster is activated, WHO will actively engage with cluster partners to contribute and benefit from the data collection process. WHO will also provide the management and security of the database and the collected data. The WCOs are encouraged, when possible, to include governments, civil society and organizations outside of the health sector to collect and share data on attacks on health care, as well as access and use data in the global database.

Individuals who submit an attack report are the owners of that raw data. WHO assumes ownership of all data once the reports are cleaned, consolidated, and aggregated into a single attack record.

5. Roles and Responsibilities of WHO

The SSA operates across the three levels of WHO: country level, regional level and headquarters. The overall roles and responsibilities at each level are described below.

WHO country office

The WHO Head of Country Office (HWCO) / WHO Representative (WR) is responsible for the following activities:

- Ensure country-level implementation of the system
- Designate the AHC Focal Point and the AHC HIM/IMO for the project
- Inform national MOH about the SSA and its guiding principles, and encourage MOH involvement
- Promote the SSA among health partners at the most senior level and encourage their involvement
- Ensure that the WCO and all WHO sub-offices uphold the SSA's guiding principles
- Review and approve data for public view in the global database
- Be aware of changes or updates to data on attacks that are already published
- Advocate for the protection of health care and the delivery of health services, citing available data

The Attacks on Health Care (AHC) focal point — generally either an Incident Manager (IM) (in acute emergencies) or Emergency Manager (EM) (in protracted emergencies) — is responsible for the following activities:

- Supervise the AHC Health Information Manager (HIM)/ Information Management Officer (IMO) involved in the implementation and operation of the SSA
- Ensure that partners are engaged in the SSA as contributors; work closely with the Health Cluster Coordinator in this regard
- Review and clear data on attacks for public view in the global database
- Make final decision on certainty level grading of the report
- Be aware of changes or updates to data on attacks that are already published
- Perform preliminary analysis of country-level data and interpret data for situation reports and other attacks-specific reports
- Reach out to regional and headquarters levels for advice on system implementation
- Together with the partners, use data to inform advocacy and risk reduction interventions
- Advise HWO/WR on advocacy and risk reduction interventions

WHO country office

The Attacks on Health Care (AHC) Health Information Manager (HIM)/ Information Management Officer (IMO) is responsible for the following activities:

- Make all possible efforts to collect details of each attack on health care from all possible sources, including WCO staff, partner organizations, and WHO HQ for triangulation
- Ensure that HIM/IMO in all WHO sub-offices collect and transmit any available data
- Monitor local and national media on attacks on health care
- Enter data in the global database, considering data coming from WHO HQ, and combining available information into a single data entry
- Assign a level of certainty to each attack
- Clean/de-duplicate and review completeness of entered data
- Submit data about attacks via the global database to the Incident Manager/ Emergency Manager and WR for review and clearance
- Perform preliminary analysis of country-level data
- Generate and disseminate information for situation reports, infographics and periodic country-level dashboards and ad hoc reports

The Health Cluster Coordinator (HCC) is responsible for the following activities:

- Promote the SSA among health partners and encourage their involvement
- Serve as liaison between partners and the SSA HIM/IMO as required
- Receive notifications of attacks on health care from system contributors and transmit them to the SSA HIM/IMO
- Contribute to interpretation of data
- Work closely with IM/EM and partners to use the data to inform health cluster advocacy and risk reduction interventions

Note: In some countries, the HCC will also act in the AHC focal point role where there is no Incident Manager or Emergency Manager.

WHO regional office

The AHC regional focal point is responsible for the following activities:

- Promote the SSA among health partners at the most senior level
- Review system application and data in the global database from WCOs in the region to standardize and harmonize use and provide related guidance to relevant WCO staff
- Conduct country missions to provide technical support and guidance
- Generate and disseminate periodic regional-level dashboards and reports
- Perform ad hoc data analysis to answer specific questions about regional characteristics of attacks on health care and produce reports based on this information
- Use available regional data to inform regional advocacy and risk reduction interventions

The Regional Programme Area Manager for Emergency Operations (PAM/EMO), the Regional Emergency Director (RED), and the Regional Director (RD) are responsible for the following activities:

- Promote the SSA among health partners and encourage their involvement
- Ensure country level implementation of the SSA
- Use available regional data to inform regional advocacy and risk reduction interventions

WHO Headquarters (HQ)

The AHC HQ focal point, the Technical Officer for Attacks on Health Care Initiative is responsible for the following activities:

- Manage the implementation of the AHC initiative including the management of the SSA implementation
- Manage the AHC HQ team, and liaise with AHC regional and country focal points
- Support country and regional offices in the implementation and management of the SSA
- Promote the SSA among health partners through the Global Health Cluster and other networks
- Promote the SSA among advocacy organizations and media
- Advocate for the protection of health care and the delivery of health services, citing available data
- Maintain the SSA global database
- Review system application and data in the global database from WCOs to standardize and harmonize use and provide related advice to relevant regional and country office staff
- Provide ongoing improvements to standardization and function of the system and database
- Generate and disseminate periodic, publicly-available dashboards with globally-aggregated data
- Create an annual report on the global scope of attacks on health care including analysis of global and regional characteristics of attacks on health care
- Establish and maintain a generic email address to trouble shoot, and to receive information on unresolved country-level issues or complaints.
- Maintain a tracking sheet that documents questions, issues and unclear areas about reporting attacks to ensure consistent decision-making and clarity around use of the system
- Send triggers to WCOs with information about attacks that are acquired through open sources and other means
- Use available global data to inform global-level advocacy, risk reduction strategies, and the research agenda of the AHC initiative

The HQ Chief of Humanitarian Policy and Guidance is responsible for the following activities:

- Manage the AHC HQ focal point in implementation and management of the SSA
- Promote and advocate for the protection of health care in emergencies at inter-agency fora and global events
- Use available global data to inform global-level advocacy and risk reduction strategies
- Encourage the involvement of WHO Executive Management, including the Director of Emergency Operations, Regional Emergency Directors, the Regional Directors, the Deputy Director General for Emergency Preparedness and Response, and WHO's Director General (DG)
- Advocate for the protection of health care and the delivery of health services
- Provide alternative and independent pathways for reporting of attacks on health care should national or regional barriers arise to their reporting or publication in the global database

6. Roles and Responsibilities of other SSA contributors

Global, regional and country level partners are encouraged to contribute to the SSA in the following ways:

- Promote the SSA internally among staff
- Contribute to the SSA by notifying the WCO of reported attacks on health care and collecting and providing related data to the WCO;
- Uphold the guiding principles of the SSA.

Obligations and Rights of the SSA contributors: 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. All partners have a right to refuse participation when contacted by the WCO about any known information related to an attack. Additionally, partners are under no obligation to carry out further investigations relating to an attack if they do not wish to do so. 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 publically.

Roles and Responsibilities of Ministries of Health, where involvement is possible:

Health authorities will be invited and encouraged to contribute to the SSA in the following ways:

- Promote the SSA internally among Ministry of Health staff
- Contribute to the SSA by notifying the WCO of reported attacks on health care and collecting and providing related data to the WCO;
- Use the publicly-available data to inform their own, complementary surveillance systems, advocacy, and programmatic interventions to protect health care, reduce the risk of attacks, and increase resilience; and
- Uphold the guiding principles of the SSA.

7. Risks and Risk Management

The risks of the system are the following: (1) lack of standardized application, (2) lack of will, access, security or capacities to collect and enter data (3) disclosure of personal information of sources and victims, (4) potential endangerment of sources due to the sensitive subject matter, and (5) potential hacking attempts into private database.

WHO will manage these risks by (1) maintaining dedicated staffing as required, (2) promoting the system and seeking funding for staff and activities, (3) sensitizing government and partners about the system, (4) conducting initial and ongoing trainings and technical assistance for WCO staff as well as all system contributors, (5) applying the SSA in a standardized manner, (6) taking all measures to discuss and agree upon risks and benefits and ensuring all contributors participate solely on a voluntary basis, (7) following defined processes for protecting personal data, (8) applying several layers of IT security and (9) reassessing risks on a regular basis.

The IT measures include site security and data encryption. Only designated focal points of country offices will be made authorized users and given log in access to the private database. These focal points will only be able to view form submissions and reports for attacks in their own country. All the data submitted to the database will be encrypted, so even if the system is hacked and a copy of the database is made, the data will be unreadable.

8. Safety and Ethics

WHO will uphold and promote safe and ethical practices for its staff and all the SSA partners and users, in accordance with WHO Research Ethics Review Committee and guidance. WHO will aim to minimize any adverse consequences of involvement in the SSA by sensitizing partner organizations to the possible risks and benefits of participation prior to the SSA implementation.

WHO will ensure that the identity of the source of data will be a priori suppressed in the publicly-facing database and marked as “anonymous” within the internally-facing database if preferred by the source. Security measures discussed in the risk management section explain how the identity of partners will not be compromised even if the system is hacked. Furthermore, only publishing certain data points minimizes the risk of disclosing personal information.

WHO and partners will continually weigh the risks and benefits of participation to their personnel and to other contributors within the changing security context.

WHO will inform all the SSA partners of the use and viewership of the data they provide, and of the risks and benefits of participating. The top of each reporting form will include text reiterating the voluntary nature of the SSA and the option to exclude personal information and remain anonymous. Thereafter, their participation in the system will imply informed consent.

To protect the victims of an attack, no personal identifying information will be collected. The only detailed data collected, when possible, will be the number of victims in the following categories: sex, age group and personnel type (for health workers). This disaggregated data, along with other detailed statistics, will not be published in the public database to protect the identities of victims. This data will be used for larger analyses of attack trends and reports.

The publishing guidelines for data access on a public database were created to safeguard the personal information of sources and

9. Data validity and bias

victims. Additionally, at any time data can be withdrawn or further suppressed in the database if the risk level changes.

The decision on which data points to publish and which data points not to make public was decided in consideration of the safety and ethics of data use by public users. The guiding principle of data sharing is balanced with the safety and confidentiality of sources and victims. The data can be used to generate reports that can be exported to Excel. The data that is shared includes sufficient information for users to view trends, conduct analyses and contribute to their respective advocacy and monitoring efforts. At the same time, users will not be able to identify personal information about sources and victims because detailed statistics and information about an attack will not be published. Even though these detailed data points will not be publicly shared, they are necessary to collect because they will be used for analyses and reports about larger trends, and will inform operational research about the impacts on health delivery systems described in the third output of the AHC initiative.

The system has been reviewed and approved by the WHO Research Ethics Review Committee.

The agreed means of data transmission to the WCO should take into consideration the context, including the impact on the likelihood of participation of contributors and security concerns. Security concerns of the handling and disposal of shared data should be agreed in advance with contributors, depending on the local context.

The WCO AHC/HIM/IMO, and his/her back-up, will be the sole persons with the ability to enter new data. Data entry by the AHC HIM/IMO is done directly into a web-enabled secure online database. Data will be sent to the AHC focal point and then the HWO/WR for read-only review and clearance. Entry into the database is done using a personal token. The database is secure with additional encryption for sensitive data points which is discussed in risk management section.

The use of a highly inclusive and timely surveillance system like the SSA to capture data on attacks on health care is essential to maintain the high sensitivity of the system, in effect preferring the presence of false positives in the system (i.e. the SSA receives notification about an attack that did not in fact occur) over false negatives (i.e. an attack happens but the SSA does not report it). The inclusivity and timeliness of such a system could be expected to drive down accuracy of reported data. To maintain accuracy of WHO-reported data, the system has increasing levels of certainty that are associated with a reported attack, based on the amount of data that is available and the supporting evidence. Additionally, a standardized data collection template and verification method has been built into the system to maintain data reliability.

Despite the purpose of the SSA to consistently apply standardized methods to collect and share information on reported attacks on health care of which the WCO are notified, collecting and reporting data on attacks on health care introduces the possibility of bias in the number or types of attacks of which WHO is notified. Fearing retaliation, system contributors may, for instance, be less likely to notify WCO staff of attacks done by certain groups. The WCO may not be notified of attacks occurring in rural or insecure areas because of a lack of system contributors in the area. Prevention of bias in the notification of attacks will require ongoing discussion and training about types of attacks that should be reported, and encouragement among contributors to notify WCO of any attack, not only those that are well-publicized. Another measure in place to prevent bias and to capture a high proportion of incidents is routine review and triangulation of secondary-sources. The AHC team at HQ will send daily triggers to WCOs with any reported incidents available from open-sources. Additionally, periodic reviews or sensitivity analyses of the SSA will be conducted to assure no type of attack is systematically excluded from the system.

10. Maintaining objectivity

WHO's leadership in implementation of the SSA is required for the integrity and independence of the data. Nonetheless, WHO and all other contributors should be engaged in ongoing sensitization and dialogue to review the data collection and transmission procedures within a country.

To overcome any perceived subjectivity or undue influence, WHO and/or partner contributors will have access to a generic email address at WHO HQ to signal unresolved issues or to voice complaints. This email address will provide an alternative and independent pathway for reporting of attacks on health care should national or regional barriers arise to their reporting or publication in the global database.

11. Monitoring and Evaluation

WHO HQ and ROs, together with partners, will lead monitoring and periodic evaluations of the implementation of the system and will make recommendations and oversee the implementation of remedial measures to improve the functionality of the system. Periodic reviews of sensitivity analysis will be conducted to assure no type of attack and geographic area is systematically excluded from the system.

An evaluation at the end of the project cycle will examine if the way the system was implemented at each country office explains the observed outcomes, and if the system overall achieved its intended objectives.

12. Support

Support for WCOs in implementing the SSA will be available before the launch of the tool and consistently throughout the utilization. Pre-implementation training will be developed by the AHC HQ Focal Point and delivered through webinar trainings, regional in-person trainings, and select country trainings. Any changes to appointed staff working on the SSA will receive training.

Regular support will be available to all country offices for any issues or questions faced. A dedicated email will be created to provide continued support.

ANNEX 1 DEFINING AN ATTACK


WHO's definition of attacks on health care considers two main aspects, the effect of the incident on the delivery of health care, and whether there was an incident that targeted health care delivery mechanisms. The following matrix looks at the interaction between these two aspects:

TARGETED ATTACK ON HEALTH CARE DELIVERY		
TYPE OF IMPACT ON HEALTH SERVICE DELIVERY	TARGETED	NOT TARGETED
	DIRECT	INDIRECT
	<p>ATTACK</p> <p>Incidents that directly target an aspect of the health care system, but have an indirect impact on health service delivery, availability, and accessibility.</p> <p>E.g. A discriminate bombing of an actively used hospital or a forced closure of a primary health centre by an armed group.</p>	<p>ATTACK</p> <p>Incidents that are not specific violence or targeted towards an aspect of the health care system, but have a direct impact on health service delivery, availability, and accessibility.</p> <p>E.g. A paediatrician is killed while in a market place, unrelated to their role as health personnel, but this loss of life has direct implications to the health system.</p>
	<p>ATTACK</p> <p>Incidents that directly target an aspect of the health care system, but have an indirect impact on health service delivery, availability, and accessibility.</p> <p>E.g. A health worker is detained because of their role, but are released after a short amount of time.</p>	<p>TO BE DECIDED WITHIN CONTEXT</p> <p>Incidents that are not specific violence or targeted towards an aspect of the health care system, and do not have a direct impact on health service delivery, availability, and accessibility. These type events fall under the "grey area" and need to be considered on a case-by-case basis.</p> <p>E.g. A health worker has to wait at a checkpoint for 2 hours en route to work. (The questions then would be: was the health worker delayed specifically because of their role as health personnel? And, did their delay have an impact on health care delivery? If the answer is yes to either of these questions, then the incident moves out of this area into one of the other boxes.</p>

**The examples given in this 2x2 table are arbitrary and could be considered to fall under different categories based on the context of the situation.*

Any type of event that either has a direct impact or direct targeting of health care is considered to be an attack. Events that fall under the category of indirect impact and indirect targeting to health are considered on a case by case basis by the WCO.

ANNEX 2 DATA COLLECTION TEMPLATE


World Health Organization

Report an attack

SURVEILLANCE SYSTEM FOR ATTACKS ON HEALTH CARE (SSA) Administrator's Dashboard

- Only fill out if safe and secure to do so (names, locations or other sensitive information will be kept confidential and secure)
- Please fill out the form as completely as possible.

Personal Information

☐ I wish to remain anonymous

*Full Name

Full Name

*Phone Number

Phone number

*Email

Email

Affiliation/Organization

Affiliation

I am

Please select...

☐ Other

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

Attack Description

* Description

Describe the attack and its circumstances

Immediate Impact

e.g. extent of physical damage, services or facilities compromised or stopped and to what extent, size of the catchment population deprived of services, number of consultations per day stopped

Affected health resources

Health care Facilities

Please select...

Health care Transport

Please select...

Health care Personnel

Please select...

Health care Supplies/Assets

Please select...

Health care Warehouse/Storage

Please select...

Health care Patients

Please select...

☐ Other

e.g. ministry, academic institutions

Attack Time and Location

*Attack Date	<input type="text" value="2019-02-05"/>	Attack Time	<input type="text" value="10:40:45"/>
*Country	<input type="text" value="Please sele..."/>	Governorate / Province	<input type="text" value="Governorate / Prc"/>
Community / city / town	<input type="text" value="Community / city /"/>	GPS Coordinates	<input type="text" value="Latitude & Longtit"/>
Targeted Health Facility	<input type="text" value="If the attack happened at a health facility, provide the name of the"/>		
Affiliation	<div><div><input type="checkbox"/> Government</div><div><input type="checkbox"/> NGO</div><div><input type="checkbox"/> Private</div><div><input type="checkbox"/> UN</div><div><input type="checkbox"/> Red Cross</div></div> <div><i>Affiliation/supporting organization of facility, transport or persons attacked</i></div>		
	<div><input type="checkbox"/> Other <input type="text"/></div>		
Type of Facility	<input type="text" value="Please select..."/>		
	<div><input type="checkbox"/> Other <input type="text"/></div>		

[How to get location?](#)

Type of Attack

Attack Types

☐ Removal of healthcare personnel or patients

Health Workers

Abduction

0

Arrest

0

Detention

0

Patients

Abduction

0

Arrest

0

Detention

0

- ☐ Violence with heavy weapons (requires more than one person to use such as firearms, tanks, missiles, bombs, mortars)
- ☐ Violence with individual weapons (knives, bricks, clubs, guns, grenades and improvised explosive devices (IED))
- ☐ Assault (without weapons)
- ☐ Removal of health care assets (e.g. transport, supplies, materials)
- ☐ Setting fire
- ☐ Chemical agent
- ☐ Militarization of civilian health facility
- ☐ Armed or violent search of health care personnel, facility or transport
- ☐ Obstruction to health care delivery (e.g. administrative or legal)
- ☐ Psychological violence/threat of violence/intimidation
- ☐ Sexual assault

☐ Other

Victims of the Attack

Total Deaths	<input type="text" value="0"/>	Health Care Providers	<input type="text" value="0"/>	Auxiliary Health Staff	<input type="text" value="0"/>
		Patients	<input type="text" value="0"/>	Others	<input type="text" value="0"/>
		Males	<input type="text" value="0"/>	Females	<input type="text" value="0"/>
		Age < 15 years	<input type="text" value="0"/>	Age ≥ 15 years	<input type="text" value="0"/>
Total Injuries	<input type="text" value="0"/>	Health Care Providers	<input type="text" value="0"/>	Auxiliary Health Staff	<input type="text" value="0"/>
		Patients	<input type="text" value="0"/>	Others	<input type="text" value="0"/>
		Males	<input type="text" value="0"/>	Females	<input type="text" value="0"/>
		Age < 15 years	<input type="text" value="0"/>	Age ≥ 15 years	<input type="text" value="0"/>

Describe any Follow up Actions Taken

Follow up Actions	<div>e.g. follow-up for victims, re-establishment of health services or any other information that you would like to be included regarding the aftermath of an attack</div>
-------------------	---

Attachments

Attach a file	<input type="button" value="Browse..."/> No file selected. <input type="button" value="Choose a file type"/> <input type="button" value="Please select..."/> <input type="button" value="Upload"/>		
ID	File	File Type	Click to Remove

Sources

Sources entered

- ☐ Social media post (Twitter or Facebook)
- ☐ Hearsay
- ☐ Form submission (regardless if eyewitness or not) from an anonymous source
- ☐ Secondary accounts (not eyewitnesses) as told to a SSA contributor
- ☐ Eyewitness account as told to a SSA contributor
- ☐ Eyewitness account by a SSA contributor
- ☐ Photo
- ☐ Video
- ☐ Satellite image
- ☐ International media report
- ☐ Local media report
- ☐ Police report

☐ Other

Certainty level

Certainty Level

Please sel... ▼

Comments

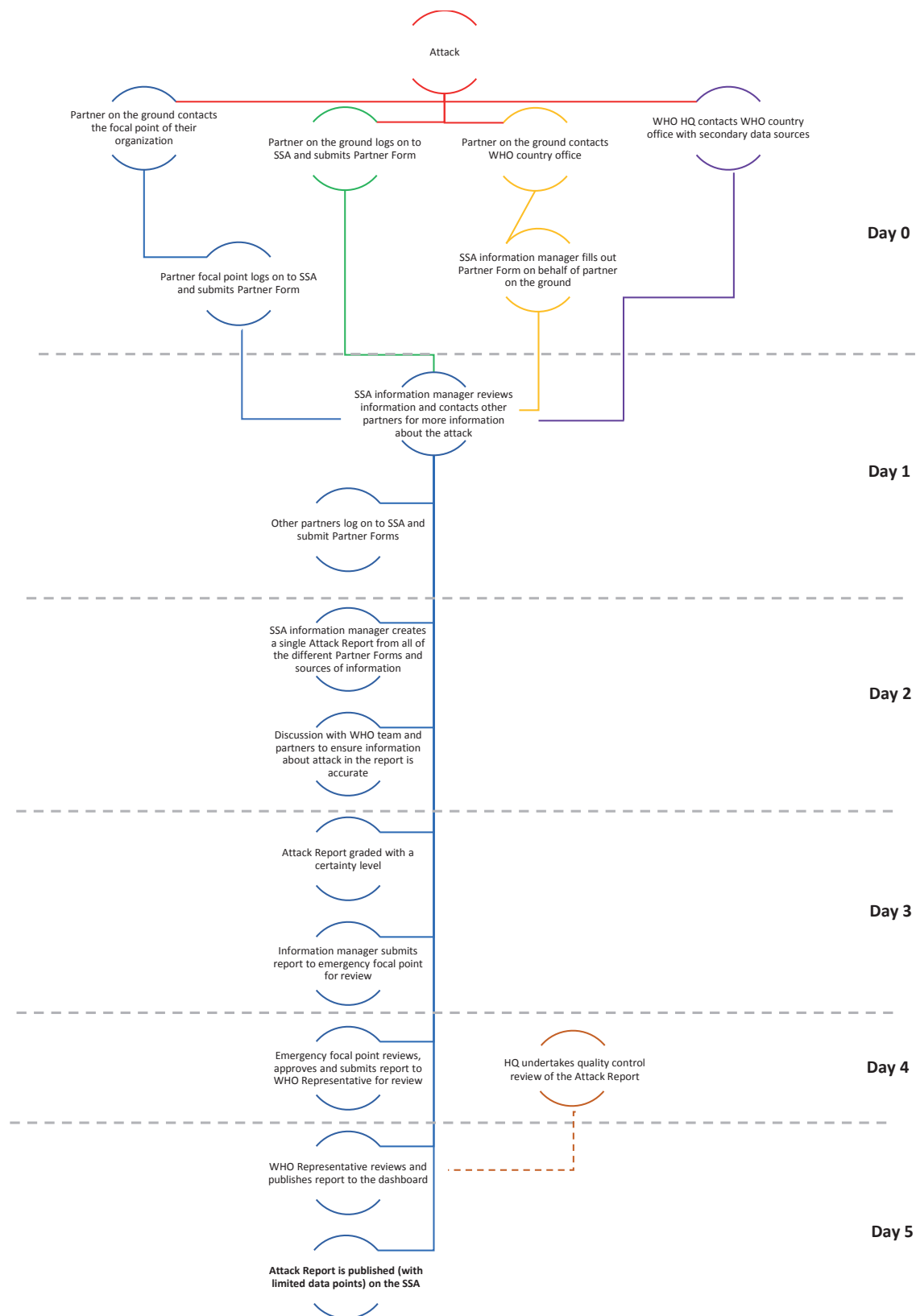
Comment

Cancel

Create

Please note: on the Partner Form, there will be no 'Sources Entered' or 'Certainty Level' section, these are only for the WCO to fill out. Furthermore, on the Attack Report there will be no 'Personal Information' section, but instead a section summarizing the linked Partner Forms.

ANNEX 3 INFORMATION FLOW





ANNEX 4 GLOSSARY

Health Resources

Health care facility	Any facility, fixed, mobile or temporary, providing curative or preventive health care. This includes hospitals, laboratories, clinics, first-aid posts, blood transfusion centers, health information centers, community health centers, vaccination posts, and the medical and pharmaceutical stores of those facilities.
Health care patient	Any person seeking or in need of health care.
Health care personnel	Any person contributing to the delivery of curative or preventive health care, with or without medical or paramedical training (i.e. both health care providers, those who provide health care directly to patients, and auxiliary staff, those who support these services).
Health care supplies/ assets	Any material or equipment that is used for curative or preventive health care. This includes medicines, vaccines, diagnostic equipment, administration documents and equipment, health care facility equipment. This list is not exhaustive.
Health care transport	Any individual or collective means of transport, which function is to convey the wounded and sick, or to transport drugs, medical material, or health care personnel. This includes ambulances, motorcycles, buses, boats, planes and other transports chartered for medical use.
Health care warehouse/ storage	A facility or storage space that stores health care supplies and assets.

Attack Types

Abduction	The unlawful removal, seizure, capture, apprehension, taking or enforced disappearance of a person either temporarily or permanently
Armed or violent search of health care personnel, facility or transport	Examination of a person's body or property, or of a health care facility or transport through the use of physical violence, weapons, or of other means of coercion.
Arrest	A seizure or forcible restraint; an exercise of the power to deprive a person of his or her liberty.
Assault	Violence inflicted from one person to another person that does not involve individual weapons or heavy weapons.
Chemical agent	A hazardous chemical has been intentionally released and the release has the potential for harming people's health.
Detention	The condition of being held in confinement and deprived of personal liberty.
Militarization of civilian health care facility	Diversion of or interference with the primary use of civilian (i.e., non-military) health care facilities or transport by state military or paramilitary forces or non-state armed groups.
Obstruction to health care delivery (e.g. physical, administrative or legal)	Any act resulting in blocking or preventing access to health care (e.g., an ambulance is prevented from accessing patients, or patients are inhibited from accessing or receiving needed health services).

Attack Types

Psychological violence/ threat of violence/ intimidation	Emotional abuse, such as insults, belittling, humiliation, intimidation, or threats of harm. The explicit declaration of a plan, intention or determination to inflict harm, whether physical or psychological.
Removal of health care assets	This can include looting, robbery or theft of health care assets. Looting refers to stealing of goods, typically during a war or riot. Theft is defined as the unauthorized taking of property of another person, and robbery is the act of stealing property from a person through the offender's use of physical force or threat of physical force.
Removal of health care personnel or patients	The act of abducting, arresting or holding in detention health care personnel or patients.
Setting fire	Arson; the act of malicious burning.
Sexual assault	A sexual act committed against someone without that person's freely given consent.
Violence with heavy weapons	Violence with a weapon that requires more than one person to use such as firearms, tanks, missiles, bombs, mortars.
Violence with individual weapons	Violence with a weapon that does not require more than one person to use, such as knives, bricks, clubs, guns, grenades and improved explosive devices (IED).

Type of people affected in an attack

Auxiliary Health Staff	Any health care personnel who carries out non-medical tasks (e.g., administrators, secretaries, accountancy clerks, and other financial personnel, cleaners, drivers, logisticians, security staff).
Health care personnel	Any person contributing to the delivery of curative or preventive health care, with or without medical or paramedical training (i.e. both health care providers, those who provide health care directly to patients, and auxiliary staff, those who support these services)
Health care provider	Any member of health care personnel with a medical or paramedical training that provides curative or preventive health care to patients. This can include doctors, nurses, nurse attendants, midwives, paramedics, physiotherapists, pharmacists, medical and paramedical students, community health workers, vaccinators and traditional birth attendants.
Patients	Any person seeking or in need of health care.

General SSA

Administrator's Dashboard

This platform for the SSA WCO users includes an interactive dashboard with attacks from all other countries, and is also the site to review submitted contributor forms, compile into a single attack report, approve, and publish attack reports. Users will be able to filter by data points in the report, like country and time of attack.

Application Directory Service (ADS)

An ADS account allows users to sign in to any ADS-enabled web site or service designated by WHO, like the site that will host the dashboard and the full length data collection template. Anyone outside of WHO is capable of creating an ADS account, and logging on to the internal dashboard page. However, only certain ADS accounts defined as partner organizations by WHO country offices (WCOs) will be able to access the full length reporting form. The internal dashboard page accessed with an ADS account by users that are not defined as a member of the partner organization group will be identical to the public dashboard page.

Attack

Any act of verbal or physical violence, threat of violence or other psychological violence, or obstruction that interferes with the availability, access and delivery of curative and/or preventive health services.

Attack Report

This is the full report of an attack that the Health Information Manager/ Information Management Officer will fill out, which will consolidate multiple sources of information, including linked Partner forms. It will be submitted, reviewed, approved, and published by the Incident Manager/Emergency Manager and the Head of Country Office/WHO Representative.

GPS coordinates

Global Positioning System using standard representation of geographic point location by coordinates.

Health services

The provision of curative or preventive health care either inside a health facility or in the community through outreach activities (e.g., home-based care or door-to-door vaccination).

Partner Contributor

Partner contributors are individuals who are staff members of organizations that are considered partners. The determination of partner organizations in each country is made on a case-by-case basis by the WCO. Partner organizations are given a unique ADS log in to access the partner form to report an attack. All WHO staff members are considered partners and can access the full partner form by logging in using their WIMS account.

Partner form

The incident report that a partner completes and submits to the WCO that contains information of an attack. An Attack Report is then created from a Partner Form or several Partner Forms with consolidated information.

Process Diagram

A diagram which will illustrate what stage an Attack Report is in: Draft with the HIM/IMO, Approval process with the IM/EM, Approval and publishing process with the HWCO/WR. There is also a to-do list function on the diagram which informs the user who is assigned to complete the current step in the process diagram.

Violence

The intentional use of physical force or power, whether threatened or actual, against oneself, another person, or against a group or community that results in or has the likelihood to result in injury or death, psychological harm, or deprivation.

