Syrian Arab Republic
Information Sharing Protocol

April 2025

Introduction

This Information Sharing Protocol (ISP) is designed to support data responsibility in the Syria. Data responsibility in humanitarian action is the safe, ethical, and effective management of personal and non-personal data for operational response, in accordance with established frameworks for personal data protection.

This ISP establishes a common framework and clear approach, standards, terminology, roles, and responsibilities for responsible granular data and information sharing in relation to operational data management activities in Syria. It applies to all humanitarian actors present in, and supporting response activities in country; it helps increase the HCT's visibility of data sharing throughout the response.

The ISP is developed through a collective exercise which will be led by coordination groups (ISCG/ISG/ICCG) and Information Management Working Group (IMWG) in accordance with the Inter-Agency Standing Committee (IASC) Operational Guidance on Data Responsibility.[1] In addition to this ISP, the Principles for Data Responsibility in Humanitarian Action presented in the Operational Guidance serves as a normative guide for responsible data management in this context.

This ISP serves as the primary document to guide data and information sharing in Syria. It is designed to complement existing policies and guidelines and does not in any way affect or replace obligations contained in applicable legal and regulatory frameworks, sector specific protocols or organization policies.

It will be reviewed and updated every two years, or sooner if needed given the circumstances of the response, through a collaborative process overseen by inter-sector coordination (ICCG) and IMWG and subject to review and endorsement by the HCT; however, this ISP will be revised one more time after completing the transition and before the end of 2025.

Purpose and objectives

The purpose and objectives of responsible information sharing include:

1. Improved inter-agency collaboration and strengthened operational coordination related to data sharing within and beyond the humanitarian community.
2. Ability to provide regular, credible situation analysis, response monitoring and reporting
3. Improved protection and response that promote safety, dignity, and the rights and

[1] IASC Operational Guidance on Data Responsibility in Humanitarian Action April (2023), available here: IASC Operational Guidance on Data Responsibility in Humanitarian Action | IASC

capacities to affected populations, including vulnerable groups such as survivors and individuals at heightened risk.

4. Facilitating joint analysis (e.g., coordinated assessments) and avoiding duplication of data management efforts.
5. Ensuring the implementation of data responsibility principles in Inter-sector coordination.
6. Establish and maintain trust among humanitarian partners by committing to responsible information sharing practices and promoting a transparent protocol.

Application and scope

This ISP applies to all humanitarian actors engaged in the delivery of humanitarian assistance in Syria, including United Nations entities, international organizations, and national non-governmental organizations (NGOs), and other relevant stakeholders.

The ISP applies to information sharing as it relates to all forms of operational data management taking place to support the humanitarian response in country:

- **Information sharing** is defined as the transfer of raw or processed data and/or information products developed from it, either through digital means (e.g., email, file transfer services, or otherwise) or physical means (e.g., passing a laptop, universal serial bus [usb] stick or other storage device). Exposure of information (e.g., showing a screen with information on it, showing a report) is included in this definition and subject to the same restrictions as the actual transfer of data or information.
- **Operational data management** is defined as the design of data management activities and subsequent collection or receipt, storage, processing, analysis, sharing, use, and retention and destruction of data and information by humanitarian actors. Such activities occur as part of humanitarian action throughout the planning and response cycle across sectors and include, but are not limited to, situational analysis, needs assessments, population data management, registration and enrolment, case management and Inter-agency referral mechanism, communicating with affected populations, protection monitoring, and response monitoring and evaluation.[2]

This ISP does not supersede or amend existing internal policies relating to mandatory organizational policies.

The ISP covers all operational data and information generated and used in the country, including both personal and non-personal data. The processing of personal data may be subject to applicable national data protection and privacy legislation – depending on organization's privileges and immunities under international law – as well as organizational data (protection) policies. These laws and policies contain the principles for personal data protection, such as a list of equally valid legal bases for the processing of personal data, including but not limited to consent. Such legislation and policies take precedence over this ISP, and it is strongly

[2] IASC Operational Guidance on Data Responsibility in Humanitarian Action (2023): https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action

recommended to consult organizational legal focal points when processing (including sharing) personal data.

- **Personal data**: any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an image, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Non-personal data**: any information that does not relate to a data subject. Non-personal data can be categorized in terms of its original nature: data that has never related to a data subject (i.e., that has always been non-personal data), such as data about the context in which a response is taking place and data about humanitarian organization and their activities; or data that was initially personal data but later rendered anonymous, such as data about the people affected by the humanitarian situation and their needs, the threats and vulnerabilities they face, and their capacities. Non-personal data includes Demographically Identifiable Information (DII), i.e., data that enables the identification of groups of individuals by demographically defining factors, such as ethnicity, gender, age, occupation, religion, or location.

For the purposes of this ISP, raw data and the information products (e.g. infographics, charts and maps, situation reports, etc.) developed from it are referred to as 'information', which includes the following:

- Data about the context in which a response is taking place (e.g., legal frameworks, political, social and economic conditions, infrastructure, access, etc.) and the humanitarian situation of focus (e.g., security incidents, protection risks, drivers and underlying causes/factors of the situation or crisis).

- Data (including personal data) about the people affected by the situation and their needs, the threats and vulnerabilities they face, and their capacities.

- Data about humanitarian response actors and their activities (e.g., as reported in 3W/4W/5W).

This ISP does not cover 'corporate' data, such as data related to internal financial upon management, human resources & personnel, supply chain management and logistics, and other administrative functions in humanitarian organizations. The management of such data should be governed by relevant organizational policies. This ISP does not supersede or amend existing internal policies relating to mandatory organizational policies. It is recommended that any data shared on financial aspects related directly to the humanitarian response can be shared voluntarily with the sector lead for operational purposes only.

Data and information sensitivity

The Data and Information Sensitivity Classification indicates the level of sensitivity of different types of data and information for a given context. Data sensitivity is based on the likelihood and severity of potential harm that may materialize if data is exposed in a particular context.[3] If disclosed or accessed without proper authorization, sensitive data and information are likely to cause harm, a negative impact on the capacity to carry out humanitarian activities or an erosion of trust.

- **Data about the context** in which a response is taking place (e.g., legal frameworks, political, social and economic conditions, infrastructure, access, etc.) and the humanitarian situation of focus (e.g., security incidents, protection risks, drivers and underlying causes/factors of the situation or crisis).

- **Data (including personal data) about the people affected by the situation** and their needs, the threats and vulnerabilities they face, and their capacities.

- **Data about humanitarian response actors and their activities** (e.g., as reported in 3W/4W/5W).

Under this ISP, data and information should be shared in-line with the parameters presented in the Data and Information Sensitivity Classification developed and agreed between the humanitarian community.

The Sensitivity Classification was developed through a collective exercise in which different stakeholders aligned on what constitutes sensitive data in Syria. While the table presents the default classification for various data and information types, the classification and associated dissemination method may vary based on the specific circumstances of a given case (e.g. cases in which the identity of a humanitarian actor should not be disclosed, or data relating to particularly vulnerable groups). As the sensitivity of data and information may change over time as the response context evolves, the group and IMWG will review and revise this classification every one year or sooner if needed based on the developments in the context.

[3] IASC Operational Guidance on Data Responsibility in Humanitarian Action (2023).

Data and Information Sensitivity Classification		
All Household (HH)/Key Informant (KI) or beneficiaries' information are severely sensitive and not to be shared. Any datasets/products/maps/assessments that include any personal information/data are severely sensitive and not to be shared.		
Sensitivity Level	**Data and Information Types**	**Classification and Dissemination Methods**
Low or No Sensitivity Information or data that, if disclosed or accessed without proper authorization, are unlikely to cause any harm or negative impacts to affected people and/or humanitarian actors.	- Analysis on population data groups at admin3/admin4 - IDP movement Report - Dataset for PIN and Severity IS and Sector at Admin3 - Partner presence at admin 3&4 - 3W/4W/5W at admin 3&4 - Number of beneficiaries assisted by sector at admin 3 level - Assessment Registry (list of assessments registered either conducted, ongoing or planned by sectors). - Incidents in IDP sites reports. - IDP movement at admin 3 - IDPs in camps population (admin 5) - Humanitarian Needs Overview and underlying data (people in need - PiN and severity at subdistrict level) - HRP Report - HNO Report - Sector or Agencies reports - Administrative lists (admin1 to admin4) and GIS layers - Access severity (subdistrict level) - Number of attacks on health facilities (community level) - Number of attacks to water infrastructures at community level.	**Classification: Public** Data or information may be publicly disclosed. Methods for sharing public data: - Response ReliefWeb - Humanitarian Data Exchange (HDX) - Other response-specific public sites - Sector/cluster portals - Partners portals

	- Number of attacks on schools at community level. - Locations with EO/UXO/ERW contamination - Number of trucks and storage capacities data provided from LOGs sector	

Moderate Sensitivity Information or data that, if disclosed or accessed without proper authorization, are are likely to cause minor harm or negative impacts and/or be disadvantageous for affected people and/or humanitarian actors	- Population figures at admin 3 & 4 (including SADD/population groups) - IDPs movements: Datasets at admin4 (with SADD) - Population and IDP data at community level - Inter-sector assessment at admin 3 &4 datasets (i.e., MSNA) - All types of datasets/survey results (e.g. aggregated to the household level and with additional disaggregation based on different indicators) - Infrastructure lists without GPS coordinates (i.e. number of schools, water stations, bakeries at community level) - protection sector service mapping[4] - Public health facility information at community level, excluding GIS coordinates.	**Classification:** Restricted Data or information can be shared within a wider humanitarian community, based on a clearly specified purpose and related standards for data protection. Methods for sharing restricted data: - ICCG/IMWG - Hub-level or Field Offices mailing lists (sub-national offices) Intra-sector mailing lists - HDX [via HDX Connect]

[4] Protection and AoR services might be anonymized in case sharing details is considered sensitive by the Cluster and/or AoR

High Sensitivity Information or data that, if disclosed or accessed without proper authorization, are likely to cause serious harm or negative impacts to affected people and/or humanitarian actors and/or damage to a response.	- Number of beneficiaries assisted, and services provided (community level) - Number of humanitarian workers (community-level) - Aggregated analysis on access incidents reported by communities and organizations - All related data of datasets (Areas of control/influence). Location information on all humanitarian facilities (schools, health facilities, water infrastructures etc.)	**Classification: Confidential** Data or information can be disclosed within an organization or small community of organizations directly involved in delivering humanitarian assistance, based on a clearly specified purpose and related standards for data protection. Methods for sharing confidential data: - Internal intra-sector sharing only. - Inter-sector sharing on a case-by-case basis
Severe Sensitivity Information or data that, if disclosed or accessed without proper authorization, are likely to cause severe harm or negative impacts and/or damage to affected people and/or humanitarian actors and/or impede the conduct of the work of a response.	- Complaints and feedback mechanism dashboard - 3W/4W/5W raw partner such as partner personnel names and locations and any other personal information. - Aggregated analysis on access incidents reported by communities and organizations - Names and locations of humanitarian workers - Warehouse locations - All information on personal data of beneficiaries (i.e., beneficiary lists, patient records, etc.)[5] - GIS coordinates for public health facilities and schools - Sensitive protection facilities including GBV shelters Full Raw data on MSNA - Location and names of professional staff in the humanitarian field (Teachers, health workers etc)	**Classification: Strictly Confidential** Highly limited, bilateral disclosure only. Determined and approved on a case-by- case basis, with assurance of upholding the highest standards of data protection. Method for sharing strictly confidential data: Bilateral disclosure between organizations based on formal requests and, in some cases, bilateral data sharing agreements

[5] Personal data should be managed in accordance with established frameworks for personal data protection. This means that any data management activities that include the management of personal data must be guided by national and regional data protection laws or organizational data protection policies. Generally, any sharing of personal data with third parties must be based on data subjects' informed consent to the sharing of their data.

	· All information on personal data of children, including lists, locations of Children Associated with Armed Forces and Armed Groups (CAAFAG) · All information on personal data of GBV survivors · All related data of location of incidents, airstrikes and impacted areas reporting · Raw incident data on GBV/PSEA · Raw data from complaints and feedback mechanisms · Aggregated analysis on PSEA anonymized analysis	

Whenever possible, ISG and IMWG members, cluster lead/co-lead agencies and members, and individual organizations should strive to share data in a timely manner through the appropriate channels in-line with the classification and recommended dissemination methods in the table above.

Additional data sensitivity considerations for areas under changing control

In humanitarian operations, areas experiencing shifts in control or heightened security risks **may** require additional data protection measures to safeguard humanitarian organizations, personnel, and affected populations. This section outlines additional data sensitivity considerations and protective measures to mitigate potential risks and ensure that critical operational information remains secure.

- Partner visibility on IM platforms and products:
  - Partners at a sub-national level may agree with the relevant Clusters to be anonymized on IM reporting platforms and products that will be shared with other partners within their sector or across different sectors or public entities. However, this information might be requested by the national sector coordinator for purposes of analysis, planning and/or operation.
- Information sharing with authorities:
  - IM personnel at national and sub-national levels must not share information with any authorities unless a clear agreement has been discussed and mutually agreed upon by all relevant partners. Such agreements must be voluntary, free from pressure, and aligned with *Table 1: Data and Information Sensitivity Classification in this document and the method of sharing under each severity*. Consequently, all sectoral data will remain protected and safeguarded from external influence.
- Sub-national IM platforms & coordination
  - Sub-national sector coordination teams may maintain separate IM platforms from the national level based on the specific security situation or operational need in their area in consultation with both sub-national and national coordination teams, following a clear assessment of the necessity and implications of doing so.

Sharing (strictly) confidential data

The sharing of strictly confidential data should be highly limited and approved on a case-by-case basis. It should also be based on a formal, bilateral data sharing agreement between organizations whether with government entities and/or donors. Certain data and information

types, such as personal data, are subject to applicable data protection regulations[6], and/or to applicable organizational policies that establish the terms and conditions of sharing such data. This ISP does not affect or replace obligations contained in these frameworks.

The instructions below for the establishment of a data sharing agreement should complement the relevant obligations and should guide actors where such obligations do not apply to them (e.g., organizations whose status accords them

privileges and immunities) or to the data in question (e.g., non-personal sensitive data). A data sharing agreement establishes the terms and conditions that govern the sharing of strictly confidential data and is essential to upholding legal, policy and normative requirements related to the sharing of sensitive data.

Any data sharing agreement or similar formal document established to govern the sharing of strictly confidential data should be developed in line with the Data Sharing Agreement Template included in Annex B of the IASC Operational Guidance on Data Responsibility in Humanitarian Action[7] and contain the following:

1. **Purpose of data sharing**
    - The data is requested for a defined purpose, which must be legitimate, clear, and explicit.
2. **Scope of agreement**
    - The agreement specifies the data that will be shared.
    - The data requested must be proportionate and necessary to fulfil the specified purpose.
3. **Measures for data protection and data security**
    - The signatories must put in place relevant measures to ensure data protection. The sharing must, at a minimum, fulfil obligations outlined in applicable frameworks for data protection and/or data responsibility.[8]
    - These measures include, among others:
        i. Assigning the roles and responsibilities of signatories.
        ii. Modalities for secure sharing, handling, storage, and destruction of data, including data access restrictions.
        iii. The retention and destruction period.
        iv. Appropriate anonymization and other preparation of data.
        v. Confidentiality requirements.
4. **Guidance on data sharing with third parties, in line with Annex A on third-party data sharing**
    - The signatories must agree on:

[6] Relevant legislation including applicable national data protection framework as well as regional data protection frameworks such as the EU General Data Protection Regulation

[7] See Annex B in the IASC Operational Guidance on Data Responsibility in Humanitarian Action, available here: https://docs.google.com/document/d/1zUroa12xHVXkfHD0-o_3Q-3N6NKH3rCN/edit?usp=sharing&ouid=111223130722283162011&rtpof=true&sd=true.

[8] IASC Operational Guidance on Data Responsibility in Humanitarian Action (2023), available here: https://interagencystandingcommittee.org/operational-response/iasc- operational-guidance-data-responsibility-humanitarian-action.

1. A process for notifying the party sharing data if the recipient receives a third-party request for access to the data.
2. Approvals and modalities required for such data-sharing with third parties.

Data incident management

Data incident management helps reduce the risk of incidents occurring, supports the development of a knowledge base, and fosters more coordinated approaches to incident management over time. Data incidents are events involving the management of data that have caused harm or have the potential to cause harm to crisis affected populations, organizations, and other individuals or groups. Data incidents include:

- Unwarranted or unauthorized disclosure of data
- Loss, destruction, damage, or corruption of data

Organizational processes should provide for clear accountability mechanisms and escalation paths for cases where a data breach or other incident occurs. Data incidents should be addressed as soon as possible and be recorded in order to prevent them from re-occurring. A standard approach for data incident management in humanitarian response is outlined in this guidance note[9].

While data incident management should be handled primarily at the organizational level, it is important to track incidents across the response in a common registry that captures key details about the nature, severity, and resolution of different incidents. Under this ISP, the ICCG, the IMWG, and the individual Clusters are tasked with supporting this activity.

Actions to ensure data responsibility.

Promoting safe, ethical, and effective data management requires the implementation of actions for data responsibility at the system-wide, cluster and organization levels of a response. This includes measures to meet the standards of privacy and data protection by design and by default when designing data management activities,[10] and measures to uphold data security by implementing appropriate organizational and technical safeguards, procedures, and systems to prevent, mitigate, report and respond to security breaches of both digital and non-digital data.[11] It also includes strategies to mitigate risks while maximizing benefits in all steps of operational data management.

The humanitarian community in the Inter-sector coordination recognizes the following actions as a priority in 2025-2026:

- Promoting awareness on this ISP and related actions for data responsibility through training/orientation sessions at the national and sub-national level.

---

[9] OCHA Centre for Humanitarian Data and Yale University (2019). Guidance Note on Data Incident Management. Available here: https://centre.humdata.org/guidance-note-data-incident-management/

[10] See the Personal Data Protection Principle presented in the IASC Operational Guidance on Data Responsibility in Humanitarian Action (2023), available here: https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action.

[11] See the Data Security Principle presented in The IASC Operational Guidance on Data Responsibility in Humanitarian Action (2023), available here: https://interagencystandingcommittee.org/operational- response/iasc-operational-guidance-data-responsibility-humanitarian-action.

- Ensuring coordination and decision-making by the HCT on issues of common concern, including personal data sharing with third parties. Inter- agency and inter-cluster/sector structures should provide a common forum or platform for coordination and decision-making on data responsibility at the system-wide level. These structures should also monitor collective progress and/or challenges and opportunities for data responsibility in the context.
- The ICCG and IMWG are responsible for providing regular updates to the HCT on their respective areas of focus of data responsibility.

Breaches to the protocol and dispute resolution

Should there be a breach of this ISP by any of the participating members, members will work to resolve such issues bilaterally. If a resolution cannot be

reached, the Chair of the ICCG will organize a dedicated meeting with the parties concerned to determine the appropriate course of action.

In case of differences in interpretation of this ISP or other related disputes, the ICCG will be responsible for finding an amenable resolution. If such a resolution cannot be found, the chair of the ICCG will refer the dispute to the HCT.

Annex A - Information Sharing with Third Parties

Beyond the information sharing activities within the humanitarian community in Inter-sector coordination as covered in this ISP, humanitarian actors may be asked to share information with different third parties. Information sharing by organizations subject to this ISP with such third parties who are not subject to the ISP (including donors, authorities, service providers, and others) should be guided by this section. This section covers operational data and information generated and used by humanitarian actors in Syria HCT coordinated response. Raw data and the information products (e.g., infographics, charts and maps, situation reports, etc.) developed from it are referred to collectively as 'information'.

Information sharing with third parties is predicated on the principle of transparency and understanding that sharing of humanitarian information– including on needs assessments, analysis, and response –is key to decision-making in a coordinated and effective response. During such information sharing, the **humanity**, **neutrality**, i**mpartiality** and **independence of humanitarian organizations** and their operations in Syria HCT coordinated response must be ensured, and a level of data responsibility that is similar or equal to that provided by this ISP must be upheld.

In many instances, humanitarian organizations will have formal arrangements (e.g., contracts, MoUs, etc.) in place with different third parties that already specify clear terms for data sharing. Where possible, these terms should align with the overall approach to responsible data management outlined in this ISP while adhering to relevant institutional policies and related requirements.

One main reason for sharing data with the authorities and other third parties is to ensure assistance is provided to those in need without duplication or exclusion. Coordination is essential, however the gaps in achieving this – and any possible failure of better coordination – should not trickle down as a potential protection risk for beneficiaries and humanitarian workers.

Humanitarian actors in Syria may have agreements that prescribe data sharing in place with various ministries. While the members of the humanitarian community have the legal responsibility to abide by these agreements, it is essential that coordination is undertaken in line with previously established policies and agreements rather than through improvised regulations that emerge in localised contexts and are not within the broader national level framework of the relevant ministries and agencies. More specifically, humanitarian agencies will welcome any suggested beneficiary lists provided by such authorities and explain any changes or validations, in accordance with defined vulnerability criteria, but not necessarily provide personally identifiable information of beneficiaries that may contravene the principles of confidentiality or could potentially put the humanitarian organization at risk of violation of beneficiaries' rights.

Humanitarian interventions require cooperation and coordination with stakeholders such as national government, other humanitarian organizations (international and national), and donors. In these relationships it is possible that the beneficiary data of humanitarian partners might need to be shared externally, and that humanitarian partners may need to receive such data. Whenever personal data needs to be shared, a data sharing agreement should be established between the parties involved in data sharing. In exceptional circumstances it may not be possible

to establish a data sharing agreement in time. This includes situations in which sharing personal data is immediately required by the intended recipient to provide lifesaving assistance to affected people. In these exceptional situations, the minimum personal data required to provide lifesaving assistance may be shared without a data sharing agreement. In such cases, the entities involved should follow the guidance in the ISP and in this annex, and the entities involved should establish a data sharing agreement without undue delay once the circumstances allow.

Receiving beneficiary data from the government and other organizations responding to the same emergency to establish a preliminary beneficiary list and to verify eligibility of those in the list is also essential. Similar data sharing may be needed for coordination between the various actors to avoid costly duplication of efforts and assistance. For donors, there could be some obligations to audit and demonstrate transparency and accountability by ensuring the beneficiaries that have received assistance are real people, were indeed eligible, and that they did receive their entitlements.

Humanitarian organizations need to inform and build understanding of the authorities that their assistance is provided on the basis of needs assessments, based on clear vulnerability criteria. These are based on the humanitarian principles of humanity, impartiality, neutrality, and independence.

Members of the humanitarian community have a duty to uphold their neutral, impartial, and independent nature when it comes to humanitarian action. Yet, humanitarian organizations that do not have privileges and immunities under international law are subject to national laws where there could be legal obligations to share certain data with the government.

Besides the specific national laws, there are other purposes for which data may be required by the government from a humanitarian organization:

- **Gaining an understanding of targeting and delivery of humanitarian assistance.** The government often want to be informed about humanitarian interventions organized in their jurisdiction, as the government is ultimately responsible for the safety and well-being of citizens and inhabitants in their areas. Additionally, if there are disagreements between some community members on why they are not included in the programme, they bring their complaints to the government. Typically, the government would like to understand the purpose, duration, target groups and agreed targeting criteria, financial scale, security requirements, resources and support needed from them. For the government to develop an understanding of the programme, it is normally sufficient to provide general information and aggregated data (target criteria, areas, number of people supported, percentage of elderly/children, amount of cash grant, etc.) rather than disaggregated or personal data. In some cases, they might be interested in seeing the final list of beneficiaries that have been targeted. It is good to gain an understanding of why the government may need such a list and negotiation may be required, to limit any personal data provided.

- **Coordinating to avoid duplication of assistance.** In an emergency, the government may already have programmes in place to support affected communities. In some contexts, the government may request beneficiary data from organizations to check for duplication, and in some cases may even require validation of the list before the organization can proceed with the distribution. The intention to avoid duplication can be reasonable and requires the government to know the beneficiaries' names. Other personal data, though, is not necessary to be shared for this purpose. Also, there is generally no need to give the government access to your database. Where possible, negotiate to minimize the amount of data and the level of

detail to share with the government in order to enable coordination and duplication checks while safeguarding sensitive data.

- **Monitoring the implementation of partnerships/joint interventions.** Some humanitarian partners could be in a partnership with the government to distribute aid on behalf of the government. Social protection programmes and large distributions where the government may rely on the national NGOs reach and capacity. In such partnerships, a formal agreement is typically created. Such agreements should be negotiated in-line with the principles for data responsibility and related best-practices.

Requests for Data and Information

Data and information sharing should only be done based on a specific request by third parties, and take into account the sensitivity of the information, the burden of requests on the sharing organization, the criticality of access needs, and longer-term impact of sharing and interference in programming and operations. To meet this requirement, third party requests for information should adhere to the following criteria:

1. **Written, formal and specific:** Requests for information should be (a) made in writing, (b) specify clearly which data is requested, (c) the format desired, and (d) the other elements specified below.
2. **Define a specified purpose:** The purpose for which information is requested should be clear and explicit from the request.
3. **Proportionate and necessary:** The information requested should be proportionate and necessary to fulfil the specified purpose.
4. **Restricted in scope and duration:** Third parties should only request the information required to meet the specified purpose for which it is being requested and should indicate a timeline for destruction of the data.
5. **Coordinated and consistent:** Third parties should ensure that requests for information of a similar type are consistently formulated to all partners concerned. Where relevant, third parties should direct requests for information from joint or coordinated data management exercises to the appropriate cluster lead or inter-agency body.

Responses and Information Sharing

All requests for information should be logged by the organization receiving the request. If the third-party request meets the criteria specified above and if an individual organization's policy allows for data sharing as requested, organizations subject to this ISP may share the requested information with the following safeguards in-place:

1. **For personal data**, inform beneficiaries that data will be shared with the third party and explain why. Clarify which counterparts within the third party will primarily have access to the data. This may deter certain beneficiaries from sharing their data and should be addressed by the programme.
2. **Establish a data sharing agreement** if feasible given the urgency of data sharing. Such agreement will formally outline the purpose for which data is shared and will limit the usage of the data to this very purpose. It also requires the recipient to keep the data safe and stored for no longer than necessary.
3. **Secure information transfer as informed by the sensitivity Classification:** Identify the channel through which information will be shared based on the sensitivity of the information as indicated by the latest version of the sensitivity classification included in this ISP.
4. **Confidentiality requirements:** Organizations will set appropriate restrictions regarding onward sharing and publication of the information upon sharing. This should include an obligation to notify the sharing organization in case information is intentionally or accidentally shared with other parties than those agreed.
5. **Consultation and alignment:** In cases where individual organizations are unsure whether a given request for information should be granted, they may consult the ICCG and HCT for guidance.