INFORMATION SHARING PROTOCOL

SOMALIA

SEPTEMBER 2021

OVERVIEW

Photo credit: Rita Maingi/OCHA

This Information Sharing Protocol (ISP) is designed to support data responsibility in Somalia. 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, roles & responsibilities for responsible data and information sharing in relation to operational data management activities in the Somalia humanitarian response. It also presents a set of shared principles[1] to serve as a normative guide for responsible data management in this context. It applies to all humanitarian actors present in and supporting response activities in Somalia.

The ISP was developed through a collective exercise led by Inter-Cluster Coordination Group (ICCG) and the Somalia Information Management and Assessment Working Group (IMAWG) in accordance with the Inter-Agency Standing Committee (IASC) Operational Guidance on Data Responsibility.[2]

In this context, this ISP serves as the primary document governing data and information sharing in the Somalia humanitarian response. 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, cluster- and AOR-specific protocols[3] or organizations policies.

The ISP will be reviewed and updated on a regular basis through a collaborative process overseen by the ICCG and IMAWG and subject to review and endorsement by the HCT.

1 See Annex A for a detailed overview of these principles. They should serve as a normative guide for actors implementing the recommended actions for data responsibility outlined in this Operational Guidance. The Principles do not represent a compliance standard.

2 IASC Operational Guidance on Data Responsibility in Humanitarian Action (2021): https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action

3 See Annex B for an overview of the existing cluster- and AOR-specific protocols, guidance, and related documents in-place for the Somalia response.

PURPOSE AND OBJECTIVES

The purpose and objectives of responsible information sharing include:

- Conducting joint analysis (e.g. coordinated assessments) and avoiding duplication of data management efforts
- Ability to provide regular, credible situation analysis, response monitoring and reporting
- Improved inter-agency collaboration and strengthened operational coordination within and beyond the humanitarian community for data sharing
- Improved protection and response that promote safety, dignity, and the rights and capacities to affected populations, including vulnerable groups such as survivors and individuals at heightened risk

APPLICATION AND SCOPE

This ISP applies to all humanitarian actors engaged in the delivery of humanitarian assistance in Somalia, including United Nations entities, other international organizations, international 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 in Somalia to support the humanitarian response.[4]

- 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, 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 clusters/sectors and include, but are not limited to, situational analysis, needs assessments, population data management, registration and enrollment, case management, communicating with affected populations, protection monitoring, and response monitoring and evaluation.[5]

The ISP covers all operational data and information generated and used in the Somalia response. 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:[6]

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 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 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.

4 The following definitions come from the IASC Operational Guidance on Data Responsibility in Humanitarian Action (2021): https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action

5 Where relevant, staff should also refer to cluster- and/or AOR-specific protocols and guidance on responsible data management within cluster/AOR-specific data management activities. See Annex A for a list of available cluster/AOR-specific protocols.

6 Other categories and types of data and information may be added to this Information Sharing Protocol through a formal revision process led by the ICCG and IMAWG as necessary.

DATA AND INFORMATION SENSITIVITY

Photo credit:
WFP

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 the classification of data based on the likelihood and severity of potential harm that may materialize as a result of its exposure in a particular context.[7] If disclosed or accessed without proper authorization, sensitive data and information are likely to cause:

- harm (negative implications of a data processing initiative on the rights of a data subject, or a group of data subjects, including but not limited to physical and psychological harm, discrimination and denial of access to services);
- a negative impact on the capacity of an individual organization or the broader humanitarian community to carry out its activities, or on public perceptions of an individual organization or the response;[8]
- an erosion of trust within the humanitarian community or between humanitarian actors and key stakeholders in the broader response context (e.g. if sensitive data is disclosed without the source's consent, this may impact the relationship with the organization and the data flow on a regular basis).

Both personal and non-personal data can be sensitive. Some types of data are categorically considered sensitive in humanitarian contexts. These include:

- Personal data (e.g. name, phone number, home address, identity number, date of birth)
- Disaggregated (household-level) assessment data
- Unprocessed Individual survey results (microdata)

Under this ISP, data and information should be shared in-line with the parameters presented in the Data and Information Sensitivity Classification below.

This Sensitivity Classification was developed through a collective exercise in which different stakeholders aligned on what constitutes sensitive data in Somalia. While this 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 ICCG and IMAWG will review and revise this classification every six months.

7 IASC Operational Guidance on Data Responsibility in Humanitarian Action (2021): https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action

8 International Committee of the Red Cross, "Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence," (2018): https://shop.icrc.org/professional-standards-for-protection-work-carried-out-by-humanitarian-and-human-rights-actors-in-armed-conflict-and-other-situations-of-violence-2512.html?___store=default

Data and Information Sensitivity Classification for Somalia

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.	- HNO and admin level 3 aggregate survey results - CODs - 3W/4W data[9] (at admin levels 1,2 and 3) - Multi cluster/cluster specific Needs Assessments and related data aggregated at admin level 2	**Classification: Public** Data or information may be publicly disclosed. Methods for sharing public data: - ReliefWeb - HRInfo - HDX - Other response-specific public sites
Moderate Sensitivity Information or data that, if disclosed or accessed without proper authorization, are likely to cause minor harm or negative impacts and/or be disadvantageous for affected people and/or humanitarian actors.	- Aggregated survey results (e.g. aggregated to admin level 1) - Access restrictions (at admin 1 i.e. regional level)	**Classification: Restricted** Data or information can be shared within the wider humanitarian community, based on a clearly specified purpose and related standards for data protection. Methods for sharing restricted data: - HDX [via HDX Connect] - Intra-cluster / intra-AOR mailing lists
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.	- Aggregated survey results (e.g. aggregated to the household level and with additional disaggregation based on different indicators) - Aid-Worker Contact Details / Lists - Access restrictions (at admin 2 i.e. district level)	**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 inter-cluster sharing only - Inter-cluster sharing on 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.	- Raw survey data, e.g. individual survey responses at HH-level data - Personal data of beneficiaries (i.e. Beneficiary lists, patient records, etc.)[10], - Personal data of children[11] - Line lists / line listing data	**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 protections. Methods for sharing strictly confidential data: - Bilateral disclosure between organizations based on formal requests (see Annex D) and, in some cases, bilateral data sharing agreements.

Whenever possible, ICCG and IMAWG 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.

9 For the Child Protection AOR,3W/4W data at area level is considered to have moderate sensitivity and thus classified as restricted.

10 Personally identifiable data like beneficiary lists should only be shared within bilateral agreements based on organizational policies framed in accordance with the minimum standards prescribed by the UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, as adopted by Resolution A/Res/45/95 of 14 December 1990, available at: http://www.refworld.org/docid/3ddcafaac.html and other international instruments concerning the protection of personal data and individuals' privacy.

11 In-line with guidance from the Somalia Child Protection AOR, access to Personal Data of children should be limited only to those who need to know it (e.g relevant staff/case workers and other service providers, such as referral agencies) for the purpose of providing services. Respect Need-to-know: recognizing that personal data is sensitive, it can only be shared with an individual when two conditions are met: (1) the requester has the appropriate clearance and access right and, (2) she/he needs to know the information in order to perform his or her job functions. For further details please refer CP AoR DPISP.

ACTIONS FOR DATA RESPONSIBILITY

Data responsibility requires the implementation of principled actions at all levels of a humanitarian response. These include for example actions to ensure data protection and data security, as well as strategies to mitigate risks while maximizing benefits in all steps of operational data management. See the IASC Operational Guidance on Data Responsibility in Humanitarian Action[12] for a complete overview of the actions.

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 reoccurring. A standard approach for data incident management in humanitarian response is outlined in this guidance note.[13]

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 IMAWG, and the individual Clusters are tasked with supporting this activity.

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 should 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.

12 IASC Operational Guidance on Data Responsibility in Humanitarian Action: https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action

13 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/

ANNEX A:

Principles for Data Responsibility in Humanitarian Action[14]

The following Principles for Data Responsibility in Humanitarian Action (hereafter 'the Principles') are designed to inform safe, ethical and effective operational data management within organizations, clusters/sectors, and the broader humanitarian system in a given response context. They should serve as a normative guide for actors implementing the recommended actions for data responsibility outlined in this Information Sharing Protocol. The Principles do not represent a compliance standard.

These Principles are based on a review of existing principles for data management (including data protection) across the humanitarian and development sectors.[15] The review revealed gaps in guidance for operational data management at the system-wide and cluster/sector level, as well as gaps in guidance for the management of non-personal data at all levels of humanitarian response. The Principles help to fill these gaps and to ensure safe, ethical and effective data management. In this way, they reinforce humanitarians' overarching commitment to Do No Harm while maximizing the benefits of data in humanitarian action.[16] The Principles also reaffirm the centrality of affected people and their rights and well-being in humanitarian action.

The management of personal data should be informed by the Personal Data Protection Principle,[17] while the management of non-personal data should be informed by the other Principles. The Principles are presented in alphabetical order, and no hierarchy is intended.

Wherever these Principles conflict with one another in their interpretation or application, they should be balanced against each other based on the particular dynamics of the response context. In the event that the Principles conflict with either internal policies or applicable legal obligations, the latter take precedent.

14 IASC Operational Guidance on Data Responsibility in Humanitarian Action (2021): https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action

15 This includes the humanitarian principles and widely accepted standards articulated for example in Sphere, the Core Humanitarian Standard and the Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief, the United Nations Data Strategy, and the UN Personal Data Protection and Privacy Principles. In addition, it includes more topical or thematic guidance specific to different aspects of data management, including the Professional Standards for Protection Work, the Protection Information Management (PIM) Framework, and the ICRC Handbook on Data Protection in Humanitarian Action, among others. Finally, the Principles draw on existing IASC guidance, including IASC Operational Guidance on Responsibilities of Cluster/Sector Leads & OCHA In Information Management, and IASC Operational Guidance for Coordinated Assessments in Humanitarian Crises. A complete list of the documents analyzed by the Sub-Group on Data Responsibility is available in Annex C.

16 Broadly acknowledged across the humanitarian sector, the concept of Do No Harm finds its roots in medical practice, from which it was developed into an axiom of humanitarian response in Mary B. Anderson, Do No Harm: How Aid Can Support Peace - Or War, (1999). For the purposes of this document the term is used as follows: 'Doing no harm' entails that data management in humanitarian response should not cause or exacerbate risk for affected people and communities, host communities, humanitarian personnel or other stakeholders, through actions or omissions. Harm is defined as 'Negative implications of a data management activity on the rights of a data subject, or a group of data subjects, including but not limited to physical and psychological harm, discrimination and denial of access to services.' 'Maximizing the benefits' of humanitarian data management entails that data is shared when a purpose requires it, in an appropriate and safe way, upholding the necessary data protection requirements. It also entails that data is managed in ways that increase the likelihood of positive impact for affected people.

17 This includes the UN Personal Data Protection and Privacy Principles.

Principles for Data Responsibility in Humanitarian Action

Accountability

In accordance with relevant applicable rules, humanitarian organizations have an obligation to account and accept responsibility for their data management activities. Humanitarian organizations are accountable to people affected by crisis, to internal governance structures, to national and international humanitarian partners, and, if applicable, to national governments and regulatory bodies. To achieve their accountability commitments, humanitarian organizations should put in place all measures required to uphold and monitor adherence to these Principles. This includes establishing adequate policies and mechanisms and ensuring the availability of sufficient competencies and capacities, including but not limited to personnel, resource and infrastructure capacity.[18]

Confidentiality

Humanitarian organizations should implement appropriate organizational safeguards and procedures to keep sensitive data confidential at all times. Measures should be in line with general confidentiality standards as well as standards specific to the humanitarian sector[19] and applicable organizational policies and legal requirements, while taking into account the context and associated risks.

Coordination and Collaboration

Coordinated and collaborative data management entails the meaningful inclusion of humanitarian partners, national and local authorities, people affected by crisis, and other stakeholders in data management activities, all where appropriate and without compromising the humanitarian principles[20] or these Principles. Coordination and collaboration should also aim to ensure that appropriate connections are established between humanitarian operational data management activities and longer-term development-oriented data processes and data investments. Local and national capacity should be strengthened wherever possible, and not be undermined.

Data Security

Humanitarian organizations should implement appropriate organizational and technical safeguards, procedures and systems to prevent, mitigate, report and respond to security breaches. These measures should be sufficient to protect against external breaches as well as unauthorized or inappropriate internal access or manipulation, accidental disclosure, damage, alteration, loss, and other risks related to data management. Measures should be adjusted based on the sensitivity of the data managed and updated as data security best practice develops, both for digital data and analogue data.

Defined Purpose, Necessity and Proportionality

Humanitarian data management and its related activities should have a clearly defined purpose. The design of processes and systems for data management should contribute to improved humanitarian outcomes, be consistent with relevant mandates and relevant rights and freedoms, and carefully balance those where needed. In line with the concept of data minimization, the management of data in humanitarian response should be relevant, limited and proportionate – in terms of required investment as well as identified risk – to the specified purpose(s).

Fairness and Legitimacy

Humanitarian organizations should manage data in a fair and legitimate manner, in accordance with their mandates, the context of the response, governing instruments, and global norms and standards, including the Humanitarian Principles. Legitimate grounds for data management include, for example: the best interests of people affected by crisis, consistent with the organization's mandate; public interest in furtherance of the organization's mandate; the vital interests of communities and individuals not able to make a determination about data management themselves; and any other legitimate ground specifically identified by the organization's regulatory framework or applicable laws.

18 This includes upholding the IASC, Commitments on Accountability to Affected People and Protection from Sexual Exploitation and Abuse (2017), available at: https://interagencystandingcommittee.org/accountability-affected-populations-including-protection-sexual-exploitation-and-abuse/documents-56.

19 The ICRC Handbook on Data Protection in Humanitarian Action (2020) and the IASC Policy on Protection in Humanitarian Action (2016) offer guidance on confidentiality. These standards should be interpreted in line with existing organizational policies and guidelines.

20 For more information on the humanitarian principles, see OCHA on Message: Humanitarian Principles, available at: https://reliefweb.int/sites/reliefweb.int/files/resources/oom-humanitarianprinciples- eng-june12.pdf.

Human Rights-Based Approach

Data management should be designed and implemented in ways that respect, protect and promote the fulfilment of human rights, including the fundamental freedoms and principles of equality and non-discrimination as defined in human rights frameworks, as well as the more specific right to privacy and other data-related rights, and data-specific rights promulgated in applicable data protection legislation and other applicable regulation.

People-Centered and Inclusive

Affected populations should be afforded an opportunity to be included, represented, and empowered to exercise agency throughout data management whenever the operational context permits. Special efforts should be made to support the participation and engagement of people who are not well represented and may be marginalized in the data management activity at hand (e.g., due to age, gender and other diversity factors such as disability, ethnicity, religion, sexual orientation or other characteristics), or are otherwise 'invisible', consistent with commitments to leave no one behind. A people-centered and inclusive approach is particularly important in the development of context-specific norms and standards for data management.

Personal Data Protection

Humanitarian organizations have an obligation to adhere to (i) applicable national and regional data protection laws, or (ii) if they enjoy privileges and immunities such that national and regional laws do not apply to them, to their own data protection policies.[21] These laws and policies contain the list of legitimate bases for the processing of personal data, including but not limited to consent.[22] When designing data management systems, humanitarian organizations should meet the standards of privacy and data protection by design and by default. Humanitarian organizations should take personal data protection into consideration when developing open data frameworks. In line with their commitment to inclusivity and respect for human rights, they should ensure the rights of data subjects to be informed about the processing of their personal data, and to be able to access, correct, delete, or object to the processing of their personal data.

Quality

Data quality should be maintained such that users and key stakeholders are able to trust operational data management and its resulting products. Data quality entails that data is relevant, accurate, timely, complete, up-to-date and interpretable, in line with the intended use and as appropriate within the given context. Where feasible and appropriate, and without compromising these Principles, organizations should strive to collect and analyze data by age, sex and disability disaggregation, as well as by other diversity characteristics as relevant to the defined purpose(s) of an activity.

Retention and Destruction

Sensitive data should only be retained for as long as it is necessary to the specified purpose for which it is being managed or as required by applicable law or donor audit regulations. When its retention is required, safe and secure storage should be ensured to safeguard sensitive data from being misused or irresponsibly exposed. All other data may be retained indefinitely, provided that its level of sensitivity is reassessed at appropriate moments, that access rights can be established, and – for anonymized or aggregate data – that a re-identification assessment is conducted. Regardless of the sensitivity level, a retention schema should indicate when data should be destroyed and how to do so in a way that renders data retrieval impossible. Specific durations for retention should be defined where possible and, where this is not the case, specific periods for review of necessity should be set.

Transparency

Data management in humanitarian response should be carried out in ways that offer meaningful transparency toward stakeholders, notably affected populations. This should include provision of information about the data management activity and its outputs, as well as data sharing in ways that promote genuine understanding of the data management activity, its purpose, intended use and sharing, as well as any associated limitations and risks.

21 In respect to UN-system organizations, the HLCM has adopted the Personal Data Protection and Privacy Principles, which should serve as a foundational framework for the processing of personal data by UN entities. For organizations that do not enjoy privileges and immunities, reference should be made to applicable data protection legislation as well as sets of principles and other guidance such organizations are subject to.

22 For more information on processing of personal data and the use of 'consent' as a legitimate basis in humanitarian response, see the ICRC Handbook on Data Protection in Humanitarian Action (2nd edition, 2020).

ANNEX B:

Other Information Sharing Protocols and Related Guidance in Somalia

At the time of writing, the following information sharing protocols or related documents were in place for humanitarian action in Somalia:

- IDP Working Group
    - Data Management Protocol (July 2021)

- Child Protection AOR
    - Somalia- Interagency Data Protection and Information Sharing Protocol Child Protection Case Management Task Force
    - Declaration of Agreement to be bound by and uphold the Inter-Agency Child Protection Case Management Data Protection and Information Sharing Protocols (DPISP)

The list above is not exhaustive and Humanitarian actors are requested to inform the ICCG when new protocols are developed at the Organization, Cluster/Sector, and/or System-Wide Level in Somalia so that these protocols can be reflected here.

ANNEX C:

Information Sharing with Third Parties

Background

Beyond the information sharing activities within the humanitarian community in Somalia 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 Annex.

This Annex covers operational data and information generated and used by humanitarian actors in Somalia. 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. In such information sharing, the humanity, neutrality, impartiality and independence of humanitarian organizations and their operations in Somalia 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. Where formal arrangements are being developed, the following considerations can help inform the design of such arrangements. Where such formal arrangements are not in place, the following considerations should inform the different steps of data sharing between humanitarian actors and third parties.

Requests for 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:

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.

Define a specified purpose

The purpose for which information is requested should be clear and explicit from the request.

Proportionate and necessary

The information requested should be proportionate and necessary to fulfil the specified purpose.

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.

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:

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.

Appropriate anonymization and other preparation of information

Prior to sharing the requested information, the responsible organization will ensure the appropriate precautions are taken, including the removal of names and other unique identifiers, and the application of methods such as Statistical Disclosure Control as needed.

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.

Consultation and alignment

In cases where individual organizations are unsure whether a given request for information should be granted, they may consult the Inter-Cluster Coordination Mechanism and the Humanitarian Country Team for guidance.