INFORMATION SHARING PROTOCOL

CAMEROON: NORTH-WEST AND SOUTH-WEST CRISIS
JANUARY 2021

INFORMATION SHARING PROTOCOL
CAMEROON: NORTH-WEST AND SOUTH-WEST CRISIS
JANUARY 2021

OVERVIEW

This Information Sharing Protocol (ISP) is designed to support ***data responsibility*** *- the safe, ethical and effective management of data* - for the North-West and South-West crisis of Cameroon. It builds on the previous ISP established in July 2020 and has been updated to reflect the changing context of the crisis, including its geographic expansion, and the evolving sector-wide guidance. This ISP establishes a clear approach, standards, roles and responsibilities for data and information sharing across different humanitarian functions and activities. It provides a common framework for information and data exchange, informed by a shared definition of sensitivity and conditions for disclosure.

This ISP applies to all activated Clusters and AoR (Child Protection, Education, Food Security, GBV, Health, Nutrition, Protection, Shelter & NFI, and WASH) actors. It covers all data and information management activities related to the North-West and South-West crisis humanitarian response. For the purpose of this protocole, 'information' refers to both raw data and the information products developed from it.

In this context, this ISP serves as the primary document governing data and information sharing for the purpose of 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 or organizational policies.

The ISP is adapted from the IASC template provided in the IASC Operational Guidance on Data Responsibility in the Humanitarian Sector[1] and has been developed through a collective exercise led by the Information Management Working Group (IMWG) of the North-West and South-West crisis in accordance with IASC guidelines. *The ISP has been endorsed by the Inter-Cluster Coordination Mechanism (ICCM) and presented to the HCT for information. The ISP will be reviewed and updated on an annual basis - or more frequently if required - through a collaborative process led by the ICCM in close collaboration with the IMWG and subject to review and endorsement by the HCT*. The OCHA coordination unit is responsible for monitoring this ISP and is the first contact for intercluster disputes that may arise.

PURPOSE AND OBJECTIVES OF INFORMATION SHARING

The purpose and objectives of responsible data and information management include:

[1] IASC Operational Guidance on Data Responsibility in Humanitarian Action, 2021, available here: https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action-0

- Conducting joint analysis (e.g. coordinated assessments) and avoiding duplication of data management efforts
- Better triangulation of information
- Ability to provide regular, credible situation analysis, response monitoring, reporting and recommendations
- Improved inter-agency collaboration and strengthened operational coordination
- Improved protection and response to affected populations, including vulnerable groups such as survivors and individuals at heightened risk
- Increase access to information on needs and gaps

APPLICATION, SCOPE AND ACCOUNTABILITY

This ISP applies to all humanitarian actors, including United Nations entities, other international organizations, international and national Non-Governmental Organizations (NGOs), and other stakeholders engaged in the delivery of humanitarian assistance in the North West and South West response. Cluster Lead and Co-Lead Agencies are responsible for ensuring the actions are undertaken within the scope of a given cluster/sector response. This includes efforts to promote adherence to global and national data protection laws (where applicable), norms, policies and standards. The Coordination Team, which is formed by the Coordinator, IMO and Co-coordinator, bears ultimate responsibility for ensuring that their staff adhere to these guiding principles for IM and that they are a key feature of any handover.

The ISP applies to information sharing in the context of all forms of operational data management activities taking place in the North-West and South-West response. 'Information sharing' is defined as the transfer of raw data 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.

The ISP covers all operational data and information generated and used in the North-West and South-West 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[2]:

- **Data about the context** in which a response is taking place (e.g. legal frameworks, political, social and economic conditions, infrastructure, 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

[2] Other categories and types of data and information may be added to this Information Sharing Protocol through a formal revision process led by the ICCM as necessary.

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

ROLES AND RESPONSIBILITIES

Data responsibility requires the implementation of principled actions at all levels of a humanitarian response. These include 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 as defined below. Some agreed actions, including roles and responsibilities are outlined below.

At the cluster level, cluster leads, technical working groups, and individual members can help uphold a high standard for data responsibility through collective action in a number of areas outlined in the IASC Operational Guidance on Data Responsibility in Humanitarian Action.[3]

Coordination Team

The Coordination Team is responsible for:

- Setting standards, operational definitions of indicators, reporting periods, and general organization of the collection of clusters-specific information between regions;
- Collating and analyzing information, as well as developing and disseminating information products;
- Ensuring information is stored, securely and confidentially;
- Ensuring the protection of individuals / communities at risk in the following ways:
    - By only sharing information at an administrative level agreed upon (Admin4 level with OCHA and Admin 2 level public);
    - By only producing reports at an administrative level agreed upon;
    - If data is shared, it has to be agreed with the source first.

The Coordination team is not authorized to share information with their host agency, unless previously approved and in line with the protocol.

DATA AND INFORMATION SENSITIVITY IN CAMEROON: North-West and South-West Context

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.[4] If disclosed or accessed without proper authorization, sensitive data and information are likely to cause:

[3] IASC Operational Guidance on Data Responsibility in Humanitarian Action, 2021, available here: https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action-0

[4] UN OCHA Data Responsibility Guidelines (Working Draft) (2019), available here: https://centre.humdata.org/wpcontent/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

- 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).; or
- 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.[5]
- an erosion of trust within the humanitarian community or between humanitarian actors and key stakeholders in the broader response context.

Some types of data are categorically considered sensitive. These include:

- Personal data (e.g. name, phone number, home address, national 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 table below. 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. Coordinators can distribute disaggregated data for specific purposes related to improving the response if previous and formal written agreement is obtained from all relevant NGO partners and clusters beyond the administrative level agreed upon. Information relating to the North West and South West crisis that are considered too sensitive and/or for reporting purposes should not be shared with other regions.
Ultimately, data responsibility requires the buy-in and participation of all functions across each organization, cluster/sector, and the humanitarian system at large. As the sensitivity of data and information may change over time as the response context evolves, the Inter Cluster Coordination Meeting will aim to review and revise this classification every six months.

Data and Information Sensitivity Classification for North-West and South-West Cameroon

[5] 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. Available here: 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

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.	Consolidated, aggregated and cleared anonymized information, at an administrative level agreed by the group [admin 2, unless otherwise specified], including: - Operational presence infographics monthly infographics - Factsheets - Situation report - Humanitarian snapshot - Bulletin and Other clusters public documents	**Classification: Public** All National humanitarian actors' email, ReliefWeb | HRInfo | HDX | other response-specific public sites etc. [the names of partners involved in the activity are to be removed prior to dissemination]
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.	- 5W matrix in Excel or infographics at deeper than admin3 level - Aggregated assessments reports - Figures (population, response) - Meeting minutes - Humanitarian contact list - Assessment reports not anonymized - Email communication not anonymized - Other IM products or document classified by its author	**Classification: Restricted** Professional email only | HDX [via HDX Connect] | Hub-level mailing lists | intra-cluster 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.	- Disaggregated assessments reports - Sensitive infographics - Field activity planning - Any other document classified by its author	**Classification: Restricted** HDX [via HDX Connect] | Internal intra-cluster sharing only | Inter-cluster sharing on a case by case basis using professional emails.
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.	- Aid-Worker personal Contact Details - Individual survey responses - Personal data (i.e. beneficiary lists),[6] etc. - Access information - Any other document classified by its author - Health facility and operational partners names (only where explicit and written permission has been given by the relevant hub)	**Classification: Strictly Confidential** Bilateral disclosure between intra-cluster partners When sharing information regarding an individual agency or a health facility, the Coordination Team will contact the cluster coordinator and copy the IMO . Data Access Form

Whenever possible, cluster leads and members, and individual organizations should strive to share data in a timely manner through the appropriate channels, based on the classification and recommended dissemination methods in the table above.

AGREED COMMITMENTS

- The clusters will abide by IASC guidelines on data responsibility and information management, sharing and confidentiality, and operate on the principle that humanitarian information/data should be made accessible to all humanitarian actors, unless sharing the

[6] Personally identifiable data like beneficiary lists should 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.

data threatens the humanitarian space and safety of the organization, its staff and partners.[7]

- The Clusters coordinators and IMOs agree to store information and data shared by cluster's members in a secure manner.
- When sharing sensitive information, cluster members are responsible for applying a 'protective marking' to the information shared to ensure that the clusters coordinators and IMOs adopt suitable security measures to prevent the information from being compromised or inappropriately disclosed.
- Ensure that the terms of this document shall be considered binding upon every person who has entered it, including after separation from the participating organization. Instances where a participant becomes aware that information has been used improperly shall be considered grounds for discontinuing information-sharing.
- The Cluster coordinator and co-coordinator are responsible in assuring that information provided by them is verified. All information and data should always mention its source.
- OCHA will present drafts of any infographics that are derived from NWSW data for validation by the Lead.

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[8].

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.[9] Under this ISP, the ICCM is tasked with supporting this activity.

---

[7] IASC Operational Guidance on Data Responsibility in Humanitarian Action, 2021, available here: https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action-0

[8] 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/

[9] For more detailed actions related to data incident management, see IASC Operational Guidance on Data Responsibility in Humanitarian Action, 2021, available here: https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action-0

BREACHES TO THE PROTOCOL AND DISPUTE RESOLUTION[10]

Should there be a breach of this Protocol by any of the participating members, a meeting will be called for all members within ten days to discuss the breach and develop a resolution. If a full meeting is not possible within ten days or if a resolution cannot be reached, the Coordination team lead holds a meeting to determine the course of action. If needed, an external interlocutor may be approached to facilitate the discussion and resolution.

All Clusters members may stop sharing data if the protocol is breached and will inform the Coordination team lead in writing of their reasons for stopping the flow of data. While the matter is being resolved, and if the Coordination team lead is not involved in the breach, it is recommended that All Clusters members continue to share data to inform field level response. The consolidated information will not be shared externally until the breach is resolved.

The resolution of a breach or suspected breach must be agreed to by all members of the Cluster.

In case of differences in interpretation of this ISP or other disputes, the Coordination team lead will be responsible for finding an amenable resolution. If such a resolution cannot be found, the Coordination team lead will refer the dispute to the Humanitarian Coordinator.

[10] Adapted from the GBVIMS Inter-Agency Information Sharing Protocol, http://www.gbvims.com/gbvims-tools/isp/

ANNEX A: Information Sharing with Third Parties

Background

Beyond the information sharing activities within the humanitarian community in the North-West and South-West crisis response of Cameroon 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 the North-West and South-West crisis of Cameroon. 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 the North-West and South-West crisis of Cameroon 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 anonymisation 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.

ANNEX B: Other Information Sharing Protocols and Related Guidance in Cameroon

At the time of writing, the following information sharing protocols or related documents are in place:

- Data Access form to agree on specific constraints related to the sharing of information between humanitarian actors

ANNEX C: IASC Principles for Data Responsibility in Humanitarian Action[11]

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.[12]

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[13] 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[14] 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

---

[11] These principles are outlined in the IASC Operational Guidance on Data Responsibility in Humanitarian Action, Feb 2021, available at: https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action-0

[12] 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.

[13] 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.

[14] 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.

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.

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.[15] These laws and policies contain the list of legitimate bases for the processing of personal data, including but not limited to consent.[16] 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

[15] 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.

[16] 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).

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.