Examples of Data Responsibility in Practice in Practice

Overview/Background:

- This document provides examples of how the Principles and Actions for Data Responsibility in Humanitarian Action can be applied in practice in order to guide their implementation in different response contexts.
- This document is maintained by the Data Responsibility Working Group (DRWG – add link) as part of its ongoing efforts to monitor and support the implementation of the IASC Operational Guidance on Data Responsibility.
- Feedback on these examples or suggested additional examples can be sent to iasccorrespondence@un.org and centrehumdata@un.org.

Implementation of Actions for Data Responsibility

Action	Response Context	Level	Actor	Description
Designing for Data Responsibility	Afghanistan	Organization	OCHA; Afghanistan Humanitarian Fund	OCHA led a process through the Inter-Cluster Coordination Team (ICCT) and Information Management Working Group (IMWG) to develop a system-wide Information Sharing Protocol for the response. This work was initiated at the recommendation of the Humanitarian Country Team as part of collective efforts to ensure accountability to affected people in the current operating environment. OCHA Afghanistan also developed guidance on data responsibility in third-party monitoring (TPM) for the Afghanistan Humanitarian Fund. This guidance outlines roles and responsibilities for responsible data management by TPM service providers and serves as a reference for other actors in the response.
Information Sharing	Cameroon	System-wide	OCHA; IMWG;	Working with relevant coordination structures and key stakeholders in the North-West and South-West, and Far North responses, the IMWG

Action	Response Context	Level	Actor	Description
Protocol			ICCG; ISCG	developed two separate Information Sharing Protocols (ISPs). The NWSW ISP was subsequently endorsed by the ICCG, while the Far North ISP (in French) was endorsed by the ISCG. In addition, a *chapeau* document was published to help practitioners find the relevant protocol for the different response contexts in the country.
Designing for Data Responsibility	Ethiopia	Organization	OCHA	OCHA Ethiopia and its partners developed an interactive platform to visualize community feedback. A Standard Operating Procedure (SOP) for the partners involved in the development and maintenance of the platform was established to support integration of additional measures for data responsibility. This work also informed the development of a template SOP for similar work in other contexts.
Data Responsibility Diagnostic	Indonesia	System-wide	OCHA; IMWG; HCT	OCHA Indonesia supported the IMWG to conduct a system-wide Data Responsibility Diagnostic, which provides observations and recommendations related to data responsibility based on a review of documents and other background information. The diagnostic informed inputs on data responsibility for the Humanitarian Country Team's Contingency Plan.
Information Sharing Protocol; Data Asset Registry; Designing for Data Responsibility	Iraq	Cluster; System-wide	CCCM; OCHA; IMWG	The Iraq CCCM Cluster developed an Information Sharing Protocol including a Sensitivity Classification, referencing this Operational Guidance. OCHA Iraq supported the IMWG to develop a Data Asset Registry as well as a Data Responsibility Diagnostic to track both the types of data managed in the context and an overview of relevant policy and governance instruments, existing processes and procedures, and technical tools that are used in the response.
Information Sharing Protocol	Mozambique	System-wide	ICCG; OCHA; IMWG; HCT	The Inter-Cluster Coordination Group developed an Information Sharing Protocol with support from OCHA. The draft ISP was circulated within the IMWG and was endorsed by the Humanitarian Country Team in Cabo Delgado. The ISP was used to inform data and

Action	Response Context	Level	Actor	Description
				information exchange between humanitarian organizations and government counterparts, and to inform the Multi-Sector Needs Assessment.
Information Sharing Protocol	Niger	System-wide	OCHA; IMWG; ICCG; HCT	OCHA Niger and the IMWG developed a system-wide Information Sharing Protocol with inputs from the clusters. The ISP was endorsed by the ICCG and then submitted to the HCT for information.
Information Sharing Protocol	Somalia	System-wide	OCHA; IMWG; ICCG; HCT	The OCHA Centre for Humanitarian Data supported OCHA Somalia to develop a response-wide ISP, which was endorsed by the HCT in September 2021. In line with the Coordination and Collaboration Principle, this process involved working closely with groups such as the Inter-Cluster Coordination Group and the Somalia Information Management and Assessment Working Group. More information on the Centre's support and overall process for developing the ISP is available in this blog on the Centre site. Sharing the ISP and background on its development followed the Principles on Transparency and on Accountability.
Coordination and Collaboration	Ukraine	Cluster; System-wide	OCHA; CWG; AAP Task Force; ICCG; IMWG	The humanitarian community in Ukraine initiated a number of actions for data responsibility at the outset of the crisis in early 2022. These included the development of a Data and Information Sensitivity Classification to inform the responsible sharing of different types of operational data and information across the response, the integration of data responsibility advisory support into the Cash Working Group (CWG) and its different task teams, and the conduct of an Information Ecosystem Mapping exercise by the Accountability to Affected People (AAP) Task Force to inform collective efforts on AAP and related data management activities. The classification also helped to protect Health Facilities that were at risk of being attacked in the context.

Action	Response Context	Level	Actor	Description
				The OCHA Ukraine Office worked closely with key stakeholders including the ICCG and IMWG in regularly updating the data and information sensitivity classification, in line with the Coordination and Collaboration Principle. Collaboration with specific clusters allowed for caveats and exceptions for specific data, supporting a Human Rights-Based approach. The public dissemination of the classification supported the practical implementation of the Transparency Principle. Support to the AAP Task Force helped highlight and direct stakeholders to the appropriate communication channels, supporting accountability in line with the Accountability Principle.
Information Sharing Protocol	Venezuela	System-wide	OCHA; IMWG; HCT	OCHA developed an Information Sharing Protocol for Venezuela. The draft ISP was reviewed by the IMWG and endorsed by the HCT. The ISP is published here (in Spanish).
Designing for Data Responsibility	Global	-	UNHCR	UNHCR has established a data curation team as part of its Global Data Service, which works with UNHCR country offices and regional bureaux to improve the consistency of microdata management. This cross-organizational function serves as an internal reference point, providing guidance and technical support to ensure that microdata is standardized, documented, timely, and interpretable, as well as processed and shared appropriately. The work of the team makes datasets more discoverable within UNHCR and, where appropriate, enables responsible wider dissemination through license requests on the UNHCR Microdata Library. The standardized approach taken to data documentation enables cross-listing between platforms such as the World Bank microdata library and HDX, which reduces the risk of version proliferation. To ensure that personal microdata is managed appropriately throughout its lifecycle in UNHCR, processes, roles and responsibilities are governed by newly developed policies and

Action	Response Context	Level	Actor	Description
				mechanisms, in the form of a revised over-arching General Policy on Personal Data Protection and Privacy and complementary internal UNHCR guidance and rules on microdata curation.
Designing for Data Responsibility	Global	-	REACH	This document outlines the first phase in standardizing protection of research data across IMPACT. Specifically, it describes the processes governing personally identifiable information within the research cycle, by specifying four immediate overall action points for implementation. The first chapter (Introduction) presents the motivation for this in the context of growing attention to data protection and the general development of standards across IMPACT. It then defines "personally identifiable information", and outlines related data protection goals. In order to achieve those goals, the second chapter introduces four overall action points. Each action point is then laid out in detail, through *(1) a requirement* with a brief explanation of its *(2) context* and *(3) details*, the step by step *(4) process* for implementation, and finally the associated *(5) accountability / responsibility structure*. Learn more about this work here: Research Cycle Data Management at IMPACT: Personally Identifiable Information Standard Operational Procedure
Coordination and decision-making on collective action for data responsibility	Global	-	UNICEF	From 19–23 September, 2022, the RD4C initiative supported by UNICEF and UNHCR Uganda hosted three workshops ("studios" in the language of the RD4C initiative) in Kampala and Isingiro District, Uganda to map common challenges regarding the responsible use and reuse of refugee children's MHPSS data and prototype a pathway

Action	Response Context	Level	Actor	Description
				forward to address these challenges through the lens of the responsible data for children principles. Learn more about this work here: Responsible Data for Refugee Children in Uganda - Improving Data Systems for Mental Health and Psychosocial Services Through A Studio Series.
Coordination and decision-making on collective action for data responsibility	DRC	System-wide	UNICEF	UNICEF's Cellule d'Analyse Intégrée/Integrated Analytics Cell (CAI) is a cross-sectoral research and analytics unit created in Democratic Republic of the Congo (DRC) to provide local actors, government, United Nations staff, and others with integrated and actionable evidence to respond to public health emergencies. First used for Ebola outbreaks in DRC starting in 2018, the CAI also provided support to Guinea (Ebola outbreak in 2021); the Republic of Congo (COVID-19) and Ghana (Marburg outbreak 2022) among others. CAI applies responsible data use best practices, in alignment with the Data Responsibility in Humanitarian Action and the Responsible Data for Children's principles, by promoting for example the 'coordination and collaboration' principle of including stakeholders with a variety of expertise and perspectives. This has strengthened the understanding of outbreak dynamics and provided solid evidence for decision making. The work of CAI and their responsible data practices has potential to be replicated in other public health emergencies. More details about CAI's work in Responsible Data for Children's case study.

Action	Response Context	Level	Actor	Description
Coordination and decision-making on collective action for data responsibility	Global	-	UNICEF	UNICEF aligned the HOPE with the Responsible Data for Children (RD4C) principles.

Balancing the Principles for Data Responsibility in Practice

Principles	Response Context	Actors	Description
Coordination and Collaboration; Defined Purpose, Necessity and Proportionality; Confidentiality	Hypothetical	-	After conducting a survey, the humanitarian organization that conducted it uses the data to correct its own programming and then stores all the raw survey data in its database. The data manager in charge receives a request to share this data with a humanitarian partner. She wants to comply with the request in line with the **Coordination and Collaboration** Principle. However, survey respondents have not given their consent for this data to be shared with third parties, although they have given consent for the humanitarian organization to use the data collection to inform improvements of the humanitarian response programme in district X. Aggregating the data resolves any tension with the rules for the management of personal data, provided that persons are no longer identifiable. In order to follow the Principle of **Defined Purpose, Necessity and Proportionality**, the data manager checks back to inquire about the intended use of the data by the humanitarian partner. The partner reports that the defined purpose is consistent with their shared humanitarian cluster objectives and will help to demonstrate potential issues of exclusion of a vulnerable population group in similar programming by that humanitarian partner in a neighboring district. If the data is not shared, programming in the neighboring district may not be corrected and vulnerable populations may continue to be excluded. The data manager reviews the Data and Information Sensitivity Classification that was developed by their office and determines that sharing the aggregated survey data, rather than the raw data, does not involve sharing any sensitive data. This satisfies the purposeful request for information, while **Doing No Harm** and upholding the protection of survey respondents' data according to the **Confidentiality** Principle. Going forward, the humanitarian organization adjusts the information provided as part of its consent procedures to explain the provisions for the sharing of non-personal data with humanitarian partners for use consistent with the

			humanitarian outcomes in the programme.
Coordination and Collaboration; Defined Purpose, Necessity and Proportionality; Confidentiality; Security	hypothetical	-	After conducting a survey, the humanitarian organization that conducted it uses the data to correct its own programming and then stores all the raw survey data in its database in accordance with its data protection regulations. The data manager in charge receives a request to share this data with a humanitarian partner. The data manager wants to comply with the request in line with the **Coordination and Collaboration** Principle, but needs to assess whether the other Principles can be met. In order to do this, the data manager: ● First, checks the Data and Information Sensitivity Classification that was developed by their office to determine whether the data includes sensitive data and what legal basis was used for the collection and processing of the data. The data manager notes that the database includes both personal data and other sensitive non-personal data of survey respondents and that the legal basis for processing was consent. Survey respondents have not given their consent for this data to be shared with third parties, although they have given consent for the humanitarian organization to use the data collection to inform improvements of the humanitarian response program in district X. The data manager concludes that the consent is insufficient to share the raw data under data protection requirements, but – depending on the partner's intended use of the data – there may be another legitimate basis for sharing the data. ● Second, checks back to inquire about the intended use of the data by the humanitarian partner, whether the intended use can be satisfied by access to aggregate, anonymized data*, rather than raw data, and whether the partner has appropriate confidentiality and data protection policies and mechanisms in place to assure the confidentiality of the data. The partner reports that the defined purpose is to help to demonstrate potential issues of exclusion of a vulnerable population group in similar programming by that humanitarian partner in Y which neighbors district X. If the data is not shared, programming in the neighboring district may not be corrected and vulnerable populations may continue to be excluded. The partner confirms that aggregate,

			anonymized data is sufficient to meet this purpose and that it has no intention or ability to seek to re-identify the individual survey respondents. The partner also provides assurance of its policies and systems for maintaining the confidentiality of sensitive data. On this basis, the data manager reviews the Data and Information Sensitivity Classification that was developed by their office and determines that the partner's intended use is consistent with the humanitarian organizations' shared humanitarian cluster objectives, and that the risks to the survey respondents and their communities of sharing the aggregate, anonymized survey data (including risk of breach of privacy, confidentiality or security in their data) are low. Together, these considerations lead the data manager to determine that sharing the aggregate, anonymized survey data satisfies the **Defined Purpose, Necessity and Proportionality** Principle, while **Doing No Harm** and upholding the protection of survey respondents' data according to the **Confidentiality** and **Security** Principles. The organizations conclude an appropriate data sharing agreement. Going forward, the humanitarian organization adjusts its consent procedures to include provisions for the sharing of non-personal data with humanitarian partners for use consistent with the humanitarian outcomes objectives of in the program, being careful to ensure that the provisions of the consent form continue to meet the Principles for Data Responsibility in Humanitarian Action and comply with its own policies for data protection and, if relevant, applicable law. * Aggregating and anonymizing the data mitigates risks, provided that individuals are no longer identifiable or capable of being re-identified through reasonable means.
Confidentiality; Coordination and Collaboration; Defined Purpose, Necessity and Proportionality;		Ministries; NGOs; UN Agencies; national healthcare providers	An NGO working in refugee camps compiled personal data on suicide deaths and survivals for the purpose of delivering Mental Health and Psychosocial Support Services (MHPSS). The NGO wanted to make this data available to key stakeholders, such as national authorities, UN Agencies and other NGOs operating in the camp in order to inform the development of a comprehensive public health strategy for suicide prevention among refugees and asylum seekers. The raw dataset, which contained data that had been collected over five years,

Accountability			included names and basic biodata, shelter locations, dates of death or suicide survival, as well as, for most individuals, socioeconomic variables such as family size and composition, employment, education, country of origin, and date of arrival into the country of asylum. Even if names were pseudonymised, the dataset would still be considered personal data due to the presence of spatio-temporal direct identifiers such as location and date. The sharing of personal data is guided by adherence to the rules on personal data protection, which include establishing the specific purpose of data sharing and ensuring that the sharing is strictly proportionate to this purpose and that the organization has a legitimate basis to share the data. The NGO determined that in order to advocate for better strategies and policies on suicide prevention in refugee camps, they had to first demonstrate that suicide deaths and attempts had increased over time, especially among young people (below 30) of both sexes who had been in the country of asylum for longer than five years. This did not require the sharing of personal data, as aggregate statistics would be sufficient to develop and deliver the advocacy messages. Expert staff in the NGO therefore anonymised the dataset to the extent that the likelihood of reidentification was reduced to an acceptably low level, provided that the access to the anonymised data be restricted to a defined list. Before the dashboard was made available to organizations on the list, the NGO decided to engage survivors in the camp and the families who had lost someone to suicide. The NGO explained the purpose of the dashboard, and individuals were given an opportunity to ask that their record be excluded from the aggregate statistics. The NGO had to balance such requests for exclusion with the need to present suicide statistics that were as accurate and complete as possible. Therefore, the NGO provided additional counsel to individuals to reiterate that records were not identifiable, and that the dashboard was only available to actors that were actively working on suicide prevention. That said, the NGO was aware that the subject of suicide was culturally sensitive in the operational context. Based on its data sensitivity classification, the NGO concluded that even sharing anonymous statistics on suicide could be harmful to refugee communities (Human Rights-Based Approach Principle). If aggregated data was made publicly available with an undefined number of recipients, there was a

			risk that the statistics could be taken out of context or otherwise poorly interpreted, or deliberately used against refugees on social media, in traditional media, or in the camps themselves. Therefore, considering the benefits and risks, the NGO concluded that even for sharing non-personal statistical data, the circle of users should be narrowly defined, based on the specific purpose of sharing, i.e., advocacy for better policies and strategies in suicide prevention. The NGO therefore established a list of ministries, NGOs, UN Agencies, and national healthcare providers that would be given exclusive and restricted access to a dynamic dashboard with aggregate statistical data (**Confidentiality Principle**; **Coordination and Collaboration Principle**; **Defined Purpose, Necessity and Proportionality Principle**). Finally, to strengthen its own accountability, the NGO conducted a series of workshops for its staff in order to strengthen their understanding of key principles on statistical disclosure control and other technical, legal and operational safeguards that need to be undertaken in order to use the suicide data for advocacy in a way that reduced the risk of harm to individuals and the refugee community (**Accountability Principle**).