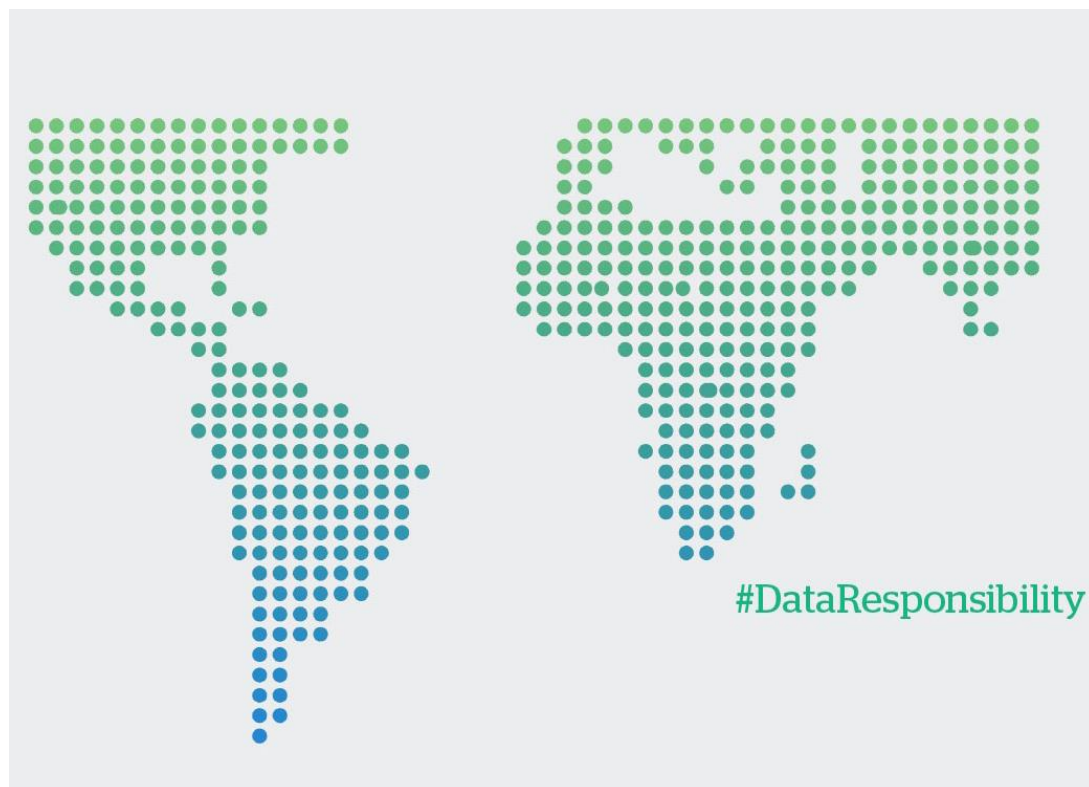Image: OCHA Centre for Humanitarian Data

Report

Data responsibility in humanitarian action: from principle to practice

Monday 20 – Wednesday 22 May 2019 | WP1688

In association with:

Report

Data responsibility in humanitarian action: from principle to practice

Monday 20 – Wednesday 22 May 2019 | WP1688

In association with United Nations Office for the Coordination of Humanitarian Affairs (OCHA) Centre for Humanitarian Data

As part of its efforts to build responsible data management into the daily practices of humanitarians, the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) Centre for Humanitarian Data, in collaboration with Wilton Park, convened an event to advance discussions around data responsibility.

Participants considered the technological, policy, and procedural requirements to ensure the safe, ethical and effective management of data in humanitarian response. They also reflected on how best to balance the risk and benefit of sharing sensitive data as well as how to improve critical incident management through individual and collective action.

The meeting aimed to:

- Build a shared understanding of good and bad practice in the management of humanitarian data;
- Align around a vision and requirements for data responsibility in the humanitarian system; and
- Agree on collaborative mechanisms for realising data responsibility in practice

Key points

- Data responsibility is a critical issue for the sector to address and the stakes are high for not getting this right.

- Ensuring we 'do no harm' with the transfer and use of personal and other forms of sensitive data requires collective action that extends across humanitarian organisations including with government and private sector partners, among others.

- Many organisations have developed policies, guidance, and practices that we can build on as we take this work forward. We need to focus on adoption in field locations with feedback loops for improvement.

- It is critical that organisations know what constitutes a critical incident and how we can report on these to better understand risks, benefits and harms.

- We need to continue to build trust between parties through dialogue and transparency.

This report draws together the discussion from the plenary sessions and seeks to identify areas of work for collective engagement in data responsibility.

Background Points

- **Humanitarian organisations collect and share more data than ever before**. This trend will continue as more systems, sensors and people come online in crisis settings. How the humanitarian community handles the data revolution to inform decisions and improve lives will be a key determinant of its future effectiveness.

- **The technical tools for managing data have evolved faster than the policy instruments that govern their use**. It is easy enough to create a new database or application, but agreeing on a policy framework takes time and requires a different mix of skills (i.e., developers and data managers working with senior managers and lawyers).

- **Data responsibility entails a set of principles, processes and tools that support the safe, ethical and effective management of data in humanitarian response**. This includes data privacy, protection, and security, as well as other practical measures to mitigate risk and prevent harm.

- **Irresponsible management of data in humanitarian contexts can place already vulnerable communities at greater risk**. For example, disclosing the location or particular vulnerability of an individual or community could lead to targeted attacks or social stigma, amongst other potential harms.

- **While personal data (such as names, biometric data, or ID numbers) can categorically be considered sensitive, determining the sensitivity of non-personal data is more challenging**. For example, data about the location of medical facilities in conflict settings can expose patients and staff to harm, whereas the same data is likely less sensitive in a natural disaster response.

- **Humanitarian organisations need to improve how they assess data-related risks, harms and benefits**. More consistent and transparent reporting and management of critical incidents related to data can help in this regard. The establishment of standardised and robust critical incident management procedures should be prioritised by humanitarian actors.

- **Improving data responsibility requires individual and collective action**. The humanitarian system is complex, with many actors working in challenging environments. We need to raise awareness and accountability through transparent processes and partnerships.

Data Responsibility in Humanitarian Action

1. Data is a critical component of humanitarian response. The management of 'humanitarian data'—data relating to crisis contexts, affected people, and humanitarian response operations—enables more effective and efficient response. However, as organizations process increasingly large volumes of data, they face more complex challenges in managing this data in safe, ethical, and effective ways.

2. In order to 'do no harm', humanitarians must be able to navigate the technical and ethical issues involved when working with data. Irresponsible data management in humanitarian contexts can place already vulnerable people and communities at greater risk, for example by exposing their location or identifying a key vulnerability. This is of particular concern when humanitarian actors handle sensitive data - data that is likely to lead to harm when exposed.

3. Humanitarian data can be considered high-risk when it identifies individuals, communities or demographics within a group and ties them to a place (i.e., affected people of a particular gender in a certain age group at a specific location). Data can also create risk in other ways - for example, by exposing the location of medical facilities in areas where these are prone to attack. These risks are typically more severe in conflict settings.

The Humanitarian Data Ecosystem

4. Every crisis context has its own unique data ecosystem, consisting of different national and international organisations, a multitude of data sources, and an increasingly wide range of tools for managing data. These data ecosystems are often interconnected and decentralised, leading to complex flows of data between a wide variety of actors. Because data is increasingly central to all aspects of humanitarian response, data management practices vary considerably across organisations and sectors, and investments to address challenges related to data remain fragmented.

5. Pressures to share data for improved response on the one hand, and to protect data in order to mitigate risk on the other, exist in constant tension. Without clear protocols for which should take precedence at any given point, data management in emergencies tends to prioritise immediate, clear benefits over long-term, uncertain risks to affected populations.

6. In many response environments, regulatory frameworks remain underdeveloped or insufficient to mitigate irresponsible data practice. Despite well-established principles, norms and professional standards regarding the protection of affected populations in humanitarian emergencies, the application of these existing frameworks in regard to data is inconsistent within and across response contexts. 'Translators' fluent in data science, ethics, and humanitarian practice are needed to help humanitarian actors move from principle to practice.

7. Donors play a unique role in this space. Accountability and transparency requirements increasingly generate data that can compromise the primary humanitarian responsibility of protecting affected people. Demonstrating how protection and accountability principles operate in tension with one another—and how those tensions may be resolved—will be an important step forward for practitioners and donors alike. Once these tensions are clarified, donors can become more deliberate in the data they do and do not request.

8. Private sector actors further complicate the landscape. Many private sector platforms already in wide use for sharing and engagement with affected populations (e.g. social media) are not designed for responsibility, but for user engagement and scale. Data responsibility considerations should be better reflected in procurement standards and processes, and humanitarian organisations need to better align these standards as a sector. Further, collaborative technology design should be promoted to help ensure that tools and platforms are fit for purpose.

Understanding Risks, Harms and Benefits

9. The risks, harms and benefits associated with data in humanitarian contexts are not well documented or sufficiently understood. Protection of personal data has received increasing attention in recent years, resulting in the adoption of various data protection and privacy policies. However, risks associated with the management of non-personal but still sensitive humanitarian data are often overlooked and poorly prevented or mitigated. Harms resulting from irresponsible management of humanitarian data can vary widely and currently remain untracked and undocumented. The sector needs a theory of harm showing the causal connection from data management decisions, to risk, and ultimately to harm for affected people or other stakeholders. The absence of such a theory of harm remains a major barrier to organisational understanding and action to invest in data responsibility.

10. Finally, there is only limited understanding of the benefits of using data, and therefore on the risks associated with 'missed use': the opportunity cost of failing to use and share data in humanitarian response. Better understanding of these positive impacts and their associated opportunity cost is a prerequisite for an informed risks, harms and benefits assessment.

11. The lack of procedures for critical incident management related to data further undermines efforts to understand and design interventions around the attendant risks, harms and benefits. Establishing such procedures within organisations - and ultimately between partners - will create a record of risk and harm, which is needed to improve risk mitigation and collective learning. More advanced critical incident management procedures increase the resilience of the sector and its ability to anticipate and adapt to the impact of technological advancements.

12. To help illustrate risks, harms and benefits, humanitarian actors should invest in the development of case studies on humanitarian data management. These case studies should take a holistic perspective: the risks of inaction must be studied alongside the risks of action. Developing these case studies jointly would also help create a common frame of reference for determining the appropriate course of action with data in different response environments.

Challenges and Opportunities for Data Responsibility in Practice

13. Improving data responsibility requires a better appreciation of humanitarian operational and organisational realities. In field offices, basic digital security hygiene is often lacking. Password management and encryption is weak or non-existent, and multi-factor authentication and intrusion detection are not currently common practice. Data on insufficiently protected devices can be exposed when passing through security checkpoints and borders. Unprotected devices may be confiscated, corrupted and compromised.

14. Organisational culture may present a challenge even greater than technical issues. A mentality that, "all our information is out there anyway," or "if they want the data, they will find a way to get it," pervades humanitarian operations. This cynicism may be well-founded when dealing with technically sophisticated actors, but the fact that some actors could get illicit access to humanitarian data does not mean that all data protection should be let go.

15. Investment in capacity building at the field and headquarters levels is required to remedy these shortcomings. The importance of responsible data management should be broadly recognised, and the impact of irresponsible behaviour should be commonly understood. In response, basic data responsibility actions should be considered easy to execute and irresponsible to avoid. Beyond these everyday actions, capacity for more advanced data responsibility measures are needed to ensure the prevention or mitigation of risk and harm.

16. Further, work being done at the headquarters level needs to align with these operational and organisational realities. Much of the guidance produced on this topic remains abstract and legalistic. Translating policy into practically applicable guidance accompanied by examples, templates and other supporting documentation is needed to move from formal adoption of policy to practical behaviour change.

17. Developing a 'maturity model' for data responsibility enables organisations to map their current and future states of data responsibility, identify areas of work, assign roles, and triage priorities as necessary. Implementing a Data Responsibility Maturity Model prompts users to rank data responsibility needs by maturity level: unaware, ad hoc, developing, mastering, and leading. In defining data responsibility across these stages, involving the perspective of affected people is critical to setting the right priorities.

18. While donors can create risk by requiring more granular and disaggregated data for monitoring and transparency purposes, their influence on data activities and management can also be used to promote responsible data practices, advancing sector-wide alignment. The donor community is well positioned to encourage and provide resources to support the proactive advancement of data responsibility.

19. When practitioners are afraid to share learnings—especially from critical incidents—they lose out on the benefits of collective action and shared responsibility for failures. Data responsibility is not primarily about reducing and mitigating risk to any humanitarian organisation: it is first and foremost about reducing and mitigating risk to the affected people they serve.

Collective Leadership, Collective Action

20. Because humanitarian data ecosystems are inherently interconnected, no individual organisation can tackle all of these data responsibility challenges alone. Inter-organisational leadership is required to guide collective, sector-wide action. Solidarity among practitioners sharing best practices, use cases, and warnings will also be essential to long-term success.

21. The humanitarian sector's investments in collective leadership, standards, and action have generated major improvements in humanitarian response, particularly through mechanisms such as the Inter-Agency Standing Committee (IASC), the Sphere Standards and the cluster system. In developing data responsibility approaches, the sector should build on existing mechanisms for sector-wide action and advocate for inclusion of data responsibility on the IASC agenda. This could include developing high-level commitments, working-level operational guidance, and shared mechanisms for addressing ongoing issues such as critical incident management.

22. Alongside humanitarians, donors are presented with an opportunity to spread data responsibility objectives throughout the work they sponsor. A donor roundtable on data responsibility could be convened on the side-lines of the next UN General Assembly meeting or a similar opportunity in the near term to advance this effort.

23. Given the persistent gaps between global guidance and principles versus response-level practice, humanitarian organisations need to work together on translating and further developing practical, field-facing guidance on different aspects of data responsibility. Topics for operational guidance could include: the safe handling of sensitive data; methods for conducting risk, harm and benefit assessments; and technical processes for statistical disclosure control, among others.

24. The challenges and opportunities related to data management require approaches for ongoing learning. All humanitarian actors should invest in case documentation on data management practices across different contexts, with support from researchers from academia and civil society. Documenting the maturity of data management in humanitarian action is critical to improving collective understanding and supporting more adaptive and responsive practice.

25. Beyond detailed case studies from actual response contexts, there is value in researchers and practitioners working together to develop and publish scenarios of the potential risks, benefits and harms for using data in crisis. If anticipated and mitigated appropriately, many potential risks and harms will never manifest in practice. Nevertheless, it is essential that humanitarians understand the risks, harms and benefits clearly and design data management exercises with these in mind.

Next steps

Over the course of the event, there were rich discussions on the critical and complex areas of ensuring data responsibility in humanitarian response. From these discussions, a number of next steps have been identified:

- Develop an approach for including data responsibility on the agenda of the Inter-Agency Standing Committee. This may include developing high-level commitments, working-level operational guidance, and mechanisms for addressing ongoing issues.

- Organise a donor roundtable on data responsibility on the side-lines of the UN General Assembly or similar opportunity.

"Given the persistent gaps between global guidance and principles versus response-level practice, humanitarian organisations need to work together on translating and further developing practical, field-facing guidance on different aspects of data responsibility"

- Prepare joint guidance on different aspects of data responsibility with partners.

- Publish case studies on the maturity of data management practices in two country contexts.

- Publish scenarios of risks, benefits and harms for using data in crisis contexts.

Authors

Jos Berens
Data Policy Officer, Centre for Humanitarian Data

Stuart Campo
Team Lead, Data Policy, Centre for Humanitarian Data

Caitlin Howarth
Communications Consultant, Centre for Humanitarian Data

Wilton Park | June 2019