

BASIC – Better Assistance in Crises



REVIEW AND ANALYSIS OF IDENTIFICATION AND REGISTRATION SYSTEMS IN PROTRACTED AND RECURRENT CRISES

RIC GOODMAN, EMRYS SCHOEMAKER, CHLOE MESSENGER, RACHAEL STELLER

May 2020

DELIVERED THROUGH THE EXPERT ADVISORY CALL-DOWN SERVICE (EACDS) – LOT B

IMPLEMENTING PARTNERS



SERVICE IMPLEMENTATION BY A
DAI CONSORTIUM



BASIC – BETTER ASSISTANCE IN CRISES

Better Assistance in Crises (BASIC) is a DFID centrally managed programme designed to help poor and vulnerable people cope better with crises and meet their basic needs through more effective social assistance in contexts of recurrent shocks, protracted conflict and forced displacement.

BASIC aims to tackle bottlenecks at global and country level that prevent greater use of social protection approaches in crises through two components:

- Technical Assistance Services – Expert advice and support for the scoping, design and delivery of more effective assistance systems.
- Research – To build a robust evidence base, research that strengthens both global and country-specific learning on using social protection approaches to respond to crises, in different contexts, and the costs and benefits of such approaches.

BASIC Technical Assistance Services are delivered through the Expert Advisory Call Down Service (EACDS) - Lot B, managed by DAI, that delivers high quality support to UK Government across a wide range of development and humanitarian challenges such as programme design, risk and contingency financing, understanding changing systems and strategic integration of humanitarian action and development.

ACKNOWLEDGEMENTS AND DISCLAIMER

This document has been produced by DAI and Caribou Digital, contracted through the EACDS Lot B service 'Strengthening resilience and response to crises', managed by DAI Europe Ltd and funded by the UK Department for International Development.

This document has been approved by DFID for publication but does not necessarily represent DFID's views or policies, or those of DAI or Caribou Digital. Comments and discussion on items related to content and opinion should be addressed to the authors, via info@lotb-resilience.org.

Your feedback helps us ensure the quality and usefulness of all knowledge products. Please email info@lotb-resilience.org and let us know whether you have found this material useful; in what ways it has helped build your knowledge base and informed your work; or how it could be improved.

First Published

May 2020

© CROWN COPYRIGHT

CONTENTS

| | |
|--|----|
| Contents | i |
| LIST OF ABBREVIATIONS | i |
| 1 EXECUTIVE SUMMARY | 1 |
| 1.1 Background | 1 |
| 1.2 Recommendations and ways forward | 1 |
| 2 INTRODUCTION | 4 |
| 2.1 Background | 4 |
| 2.2 Methodology | 4 |
| 2.3 Structure | 5 |
| 3 CONTINUUM OF SOCIAL TRANSFERS | 5 |
| 3.1 From humanitarian transfers towards government-led social protection | 6 |
| 3.2 Cash | 7 |
| 3.3 Increasing pressure for centralisation | 8 |
| 3.4 Conflation of interoperable humanitarian systems with government-led social protection | 9 |
| 4 MANAGEMENT INFORMATION SYSTEMS – RISKS AND BENEFITS | 10 |
| 4.1 Political | 10 |
| 4.1.1 Political misuse of data | 10 |
| 4.1.2 Political Economy | 11 |
| 4.1.3 Government – humanitarian sector tensions | 12 |
| 4.2 Protection | 13 |
| 4.2.1 Fairness | 13 |
| 4.2.2 Discrimination | 14 |
| 4.2.3 Hacking, data leaks and other implications on personal security | 14 |
| 4.2.4 Proportionality | 15 |
| 4.2.5 Data sharing | 15 |
| 4.2.6 Further processing | 16 |
| 4.3 Legal & Ethical | 17 |
| 4.3.1 Domestic legal frameworks | 17 |
| 4.3.2 International standards | 18 |
| 4.3.3 Digital Dignity | 19 |
| 4.3.4 Do no harm and approaches to data protection | 19 |
| 4.3.5 Basis for data processing | 20 |
| 4.4 Commercial | 22 |
| 4.4.1 Value for Money | 22 |
| 4.4.2 Fiduciary responsibility | 25 |
| 4.4.3 Reputational damages | 27 |

| | | |
|-------|--|-----------|
| 4.5 | Operational..... | 27 |
| 4.5.1 | Improved information management | 28 |
| 4.5.2 | Efficiency and effectiveness in registration | 28 |
| 4.5.3 | Sustainability | 28 |
| 4.5.4 | Techno-solutionism and the role of technology | 30 |
| 5 | RECOMMENDATIONS AND WAYS FORWARD | 32 |
| 5.1 | Integration and interoperability..... | 32 |
| 5.2 | Conceptual framework – digital dignity | 32 |
| 5.3 | Data protection standards..... | 33 |
| 5.4 | Ways of working..... | 33 |
| 5.5 | Options for implementation | 34 |
| 5.6 | Compliance – legal and contractual route | 34 |
| 5.7 | Compliance – voluntary route | 35 |
| 5.8 | Supporting transition to government systems..... | 35 |
| 5.9 | Biometrics | 36 |
| 5.10 | Basis for data processing..... | 36 |
| 5.11 | Risk management | 37 |
| 5.12 | Contextualising the recommendations – application in Yemen and South Sudan | 37 |
| 6 | REFERENCES | 39 |
| | ANNEX 1 – MANAGEMENT INFORMATION SYSTEM DEFINITIONS | 47 |
| 1.1 | Introduction to MIS..... | 47 |
| 1.2 | Single registry, social registry, civil registry | 49 |
| 1.3 | Centralised MIS..... | 49 |
| 1.4 | MIS Interoperability | 51 |
| 1.5 | Data sharing agreements..... | 52 |
| 1.6 | Data..... | 52 |
| 1.7 | Biometric data | 53 |
| 1.8 | Blockchain..... | 54 |
| 1.9 | Consent..... | 55 |
| 1.10 | Identity..... | 58 |
| | ANNEX 2 – CASELOAD TYPES | 61 |
| 2.1 | Asylum seekers, refugees, returnees | 61 |
| 2.2 | Internally displaced persons (IDPs) | 62 |
| 2.3 | Host communities..... | 62 |
| 2.4 | Vulnerable people | 62 |
| | ANNEX 3 – RISK TABLE | 64 |
| | ANNEX 4 – ANALYTICAL FRAMEWORK | 78 |

LIST OF ABBREVIATIONS

| ACRONYM | Full title |
|---------|---|
| AML | Anti Money Laundering |
| API | Application Programming Interface |
| BIMS | Biometric Identity Management System |
| BRAVe | Biometric Registration Assistance Verification |
| CaLP | Cash Learning Partnership |
| CCT | Conditional Cash Transfer |
| CPMS | Child Protection Minimum Standards |
| CRVS | Civil Registration and Vital Statistics |
| DCED | Donor Committee for Enterprise Development |
| DFID | Department for International Development |
| DSA | Data Sharing Agreements |
| DTM | Displacement Tracking Matrix |
| DPIA | Data Protection Impact Assessment |
| ECTP | Emergency Cash Transfer Project – Yemen |
| EU | European Union |
| FAM | Famine Action Mechanism |
| FCAS | Fragile and Conflict Affected States |
| GDPR | General Data Protection Regulation |
| GDT | Global Distribution Tool |
| GIZ | German Corporation for International Cooperation GmbH |
| ID4D | Identity for Development |
| IASC | Inter-Agency Standing Committee |
| IATI | Independent Aid Transparency Initiative |
| ICAI | Independent Commission on Aid Impact |
| ICRC | International Committee of the Red Cross |
| ICT | Information Communication Technology |
| ID | Identity |
| IDP | Internally Displaced Person |
| IOM | United Nations International Organisation for Migration |
| IRC | International Rescue Committee |
| ISPA | Interagency Social Protection Assessments |

| | |
|---------|--|
| KFW | Kreditanstalt für Wiederaufbau / German Development Bank |
| KYC | Know Your Customer |
| LMIS | Laboratory Management Information System |
| MENA | Middle East and North Africa |
| MIS | Management Information System |
| MNO | Mobile Network Operators |
| MoU | Memorandum of Understanding |
| M4P | Markets for the Poor |
| NRC | Norwegian Refugee Council |
| NAMCHA | National Authority for the Management and Coordination of Humanitarian Affairs |
| PRIMES | Population Registration and Identity Management EcoSystem |
| ProGres | Profile Global Registration System |
| RApp | Rapid Application |
| SCOPE | WFP's Digital Platform for Beneficiary and Transfer Management |
| SFD | Social Fund for Development |
| SIM | Subscriber Identity Module |
| SMS | Short Message Service |
| SCMCHA | Supreme Council for Coordination of Humanitarian Aid |
| SSSAMS | South Sudan School Attendance Management System |
| SPIAC-B | Social Protection Inter-Agency Cooperation Board |
| SWF | Social Welfare Fund |
| SyRI | System Risk Indication |
| TNH | The New Humanitarian |
| UN | United Nations |
| UNHCR | United Nations High Commissioner for Refugees |
| UNICEF | United Nations Children's Fund |
| VfM | Value for money |
| WB | World Bank |
| WFP | World Food Programme |

1 EXECUTIVE SUMMARY

1.1 Background

This report focuses on the use of identification and registration Management Information Systems (MIS) throughout humanitarian response, including protracted and recurrent crises and transitional contexts, and incipient government participation in social protection transfers. The research explores the feasibility of humanitarian aid MIS being designed to link with social protection systems and to support a transition, in the long-term, to state-led social assistance. While it provides global recommendations based on a literature review and key informant interviews with a range of stakeholders at a global level, case studies focused on Fragile and Conflict Affected States (FCAS), namely Yemen and South Sudan.

Data systems to register and identify recipients of transfers underpin everything in a targeted distribution system, including who is eligible, who is not, why, for what and for how long. Data collection for these systems is often the first contact point between crisis-affected populations and responders. Data is therefore often collected when people are at their most vulnerable, and when their options are limited.

There was a trend among donors and humanitarian actors interviewed as part of this research to increasingly support the development of single or social registries for social assistance programmes (particularly where eventual government ownership is envisioned), or greater interoperability and information sharing, and to move away from separate and disconnected MIS. This is evident in the Joint Donor Statement on Humanitarian Cash Transfers, which envisages “solutions whereby interoperable, non-proprietary, data registries can allow a level of data sharing between humanitarian agencies and private sector service providers” and “ensure that where possible cash programmes link to existing social protection interventions or build the blocks of future longer-term assistance”.¹ UN agencies are pushing for common approaches to humanitarian cash and scaling up collaboration amongst agencies. Both in the literature and stakeholder consultations, the benefits of increased interoperability and/or centralisation are largely defined in terms of efficiency gains, with little reference to protection and other advantages and trade-offs.

In addition to greater interoperability amongst different humanitarian actors, the drive for interoperability between humanitarian actors and government-led social protection is growing. Whilst there is increasing recognition that the success of linkage depends on the level of maturity of the government system and the political and economic context,² there is also a push to bridge the humanitarian-development nexus.

1.2 Recommendations and ways forward

- MIS and data interoperability within the humanitarian sector should be supported, but through standardisation rather than a single system approach. Enabling multiple different systems to interact can help deliver efficiencies, but it is neither realistic nor desirable to achieve this through a single system. Rather than efforts to standardise data collection, categorisation and management would enable different systems to ‘read’ each other, with potential gains in transparency and effectiveness without compromising fundamental rights. For instance, federated systems in which data ownership is maintained by each entity, but data is shared on-demand via a central application, offer a version of interoperability which is potentially more secure and offsets monopolies. Interoperability should also be furthered through opening ‘closed’ systems, such as SCOPE,

¹ Joint Donor Statement on Humanitarian Cash Transfers, June 2019, Cash Learning Partnership <https://www.calpnetwork.org/publication/joint-donor-statement-on-humanitarian-cash-transfers/>

² See, for example, Idris, I. (2019). Linking social protection and humanitarian response: Best practice. K4D Helpdesk Report 684. Institute of Development Studies.

ProGres, PRIMERO and BRAVE, using APIs³ to enable third parties to unlock data monopolies and enabling the development of further services. This could be achieved through establishing a shared standard for data categorisation, such as the Humanitarian Exchange Layer (HXL⁴), to which UNHCR, IOM, IFRC and others are signatories, as well as the Humanitarian Data Exchange (HDX⁵) which employs HXL and is used by over 260 organisations in various ways. Interoperability should also be based on minimising data sharing – for example, through further use of ‘zero knowledge proofs’⁶ – verifying claims without sharing data. However, the further development of interoperability should be considered through a participatory process including all stakeholders, particularly the individuals who these are intended to benefit.

- Whilst focusing on interoperability of MIS in protracted crises, data protection for vulnerable people must be at the forefront. Different types of interoperability and fragmented systems offer implications for beneficiary security and protection. For this reason, the remaining recommendations focus on how to achieve the effectiveness and efficiency gains of interoperability whilst protecting the populations with which we work.
- The design and application of MIS should be guided by the concept of digital dignity. Individuals need to be respected as a data agent, and not purely as a data subject, in the way data are governed, to ensure that data governance aligns with core humanitarian and development principles.⁷ Digital dignity provides a framework that is aligned to existing guidance on aid delivery, including data protection; Value for Money; Do No Harm; and Leave No-One Behind.
- Policies and reporting should be aligned to an agreed sector specific international data protection regime. The lack of such standard guidance is a significant gap. A sector-specific approach would assist because the humanitarian and development sectors are likely to have specific needs and face different challenges due to the particularly vulnerable beneficiaries with which they work, the challenge of operating on behalf of the “international community” in FCAS, etc. This does not mean the sector cannot draw on broader guidance from, or seek to align with, the approaches in other sectors, but the uniqueness of this sector should be considered. This would include standards on:
 - Reaching meaningful consent (or relying on other bases for data processing, if applicable) and updating this consent according to changing circumstances or change of use (for example, if migrating from donor-led response to state-led social protection).
 - Ability of those registered to enquire on full data held and to request changes, updates and delete data held on them.
 - Explanation provided to individuals of which parties have access to this data.
 - Avoidance of catch-all terms such as asking permission to share data “with all parties as decided by the registrar”.
 - Data collected is relevant to the immediate requirements of the good or service being provided and avoid collecting additional data that “might be useful in future” – i.e. data minimisation.
 - Timebound data retention periods and safe data deletion procedures.
 - A risk-based approach to data processing, according to context, including oversight of role played by third party data processors.
- Donor/aid agencies should develop a global multi-disciplinary community of practice on management information systems interoperability, including humanitarian and development perspectives, spanning from aid policy to legal, protection and safeguarding, and IT expertise. The

³ An API, or Application Programming Interface, is a software intermediary that allows two applications to talk to each other. I.e. it is the messenger that delivers your request to the provider that you're requesting it from and then delivers the response back to you.

⁴ <https://hxlstandard.org/>

⁵ <https://data.humdata.org/>

⁶ Zero knowledge proofs are a method by which one party can prove to another party that they know a value x, without conveying any information apart from the fact that they know the value. For instance, Organisation A could state they have Beneficiary A in their system, without sharing the details of that Beneficiary with Organisations B

⁷ Digital Dignity in Practice: Existing Digital Dignity Standards, Pursuing Digital Dignity and Current Gaps in Digital Dignity

key task of an international body should be to inform, facilitate, convene, assess, compare and report on data management in MIS and data registries. This body should have cross sector visibility to ensure coherence, but sector specific workstreams to ensure detail, engagement and impact.

- Compliance with the MIS data protection standard could be implemented legally/contractually or voluntarily. This standard would operate in addition to applicable domestic/regional legal frameworks and standards and help fill the gaps where there is no applicable domestic/regional legal framework to apply. The first means is through collective legal and contractual enforcement of a common approach following agreement by all major donors i.e. obligations being included in contracts or grant agreements issued. Alternatively, an aspirational voluntary code of practice could be developed which aid agencies are encouraged to meet (in part through appropriate donor funding reward or penalty). This could come from a voluntary scheme which sets a standard and encourages aid agencies to meet it.
- Donor support to strengthening state social protection systems should take a holistic, 'ecosystem' approach. This should include providing more assistance to the centralised national functions needed to establish a government-led social protection system, e.g. statistics, civil registry, identity, rather than only for social transfers through parallel projects. Restrictions on support for government authorities might be re-considered – or re-configured whereby this support is channelled through a UN body – to maintain a minimum level of common resource and functionality. In such instances the aim is to create and adopt one system for common collaborative use, and future adoption by government.
- Biometric data should be placed under particular protection. Biometric data are recognised as being particularly powerful and drive system efficiencies, for example in ensuring de-duplication of access to transfers. There is a significant trend towards its use, in many cases without due consideration for the challenges. Due to their immutability and uniqueness, biometrics raise considerable safe data processing risks and require commensurate risk management measures. Adherence to GDPR-like protocols will help assure the security of this data.
- Greater efforts by aid agencies to obtain informed consent are needed. While data registered in many humanitarian contexts may rely on other legal bases for collecting data, such as vital interest or important grounds of public interest, it should not be assumed that this legal basis applies to non-essential onward use of this data. For example, it cannot be assumed to be in the "interests of the beneficiary" to share or merge datasets, just because it makes sense to the project manager and the ultimate donor.
- Donors and aid agencies should introduce data risk assessments and response plans as standard to all MIS activities. A standard, structured Data Protection Impact Assessment approach should be developed and undertaken for humanitarian contexts, including consideration of protection risks. Taking a precautionary approach, potentially the most effective way to minimise risk is to reduce the data that is collected and reduce the degree of centralised management.
- Beyond linked systems, there are opportunities to gain insights into impact and effectiveness without compromising privacy and personal data protection. High-level summary statistics that do not involve anonymised personal data (which involves the risk of de-anonymisation), such as overall reporting on the amount of aid provided by an organisation, can assist in planning and coordination but does not entail the same risks of de-anonymisation of sensitive personal data.⁸

⁸ See, for example, the 5W UN reporting system, which allows for consolidated reporting without hard data sharing: <https://www.humanitarianresponse.info/en/operations/nigeria/document/5w-process-coordinated-and-effective-response>

2 INTRODUCTION

2.1 Background

This report was prepared by a team of experts from DAI and our partner for this project, Caribou Digital. DAI is a global leader in the analysis, design, and implementation of cash programming in humanitarian and social protection contexts, including significant experience in the field of shock responsive social protection. DAI and Caribou Digital have extensive experience in the analysis of management information systems (MIS), beneficiary identification and registration, and data protection, and in working with donors to shape policy and programming around all these key areas.

Protracted and recurrent emergencies increase the need for better connections across humanitarian aid and social protection. However, the necessary information systems are often disconnected and fragmented within humanitarian response, within state assistance and between humanitarian and state social protection systems. This can have negative consequences, such as duplication or exclusion from assistance, implications for data protection, and can lead to confusion for users – failing to put beneficiaries first.

Cash transfers are an increasingly common means of providing state social assistance, while their use in humanitarian aid is also increasing. State social assistance helps build people's resilience before and during crises, increasing people's capacity to resist and respond to shocks. At the same time, humanitarian cash transfer programmes are expected, by some, to provide building blocks for longer-term systems, some attributes of which might be adopted in / transferred to a future national approach.⁹

Data systems to register and identify recipients of transfers underpin everything in a targeted distribution system in terms of who is eligible, who is not, why, for what and for how long. Data collection for these systems is often the first contact point between crisis-affected populations and responders. Data are hence collected as people are at their most vulnerable, and when their options are limited.

This report focuses on these identification and registration systems as part of wider information management throughout a humanitarian response, including protracted and recurrent crises, and at the nexus between humanitarian and developmental approaches. The research aims to identify the implications of separate and disconnected systems on response and ongoing programming following humanitarian crises in the transition to developmental approaches, or during protracted or recurrent crises. It seeks to identify stakeholders' different priorities and concerns and articulate any apparent trade-offs in these priorities. The research also explores the feasibility of humanitarian aid MIS being designed to link with social protection systems and to support a transition, in the long-term, to state-provided social assistance.

2.2 Methodology

The key questions posed by the ToR for this research are:

1. What are the implications of having separate and disconnected MIS for identification and registration among humanitarian and social assistance responders?
2. Does the use of different MIS for identification and registration in crises enable or challenge potential linkages between humanitarian cash assistance and social protection, and how?
3. Can different models of linking MIS improve the effectiveness of crisis response in protracted and recurrent crises?

This assignment used a combination of a literature review, key informant interviews and focus groups. From an initial literature review focusing on key documentation on the humanitarian-social protection nexus and MIS for transfers, the team identified and contacted a stakeholder consultation group and established an analytical framework (see Annex 4) for the research. Questions were developed for the

⁹ How linking social protection and humanitarian action can bridge the development-humanitarian divide. A joint statement of social protection actors to the World Humanitarian Summit, Social Protection Inter Agency Board (SPIAC-B)
<http://pubdocs.worldbank.org/en/436341463577765630/SPIACBstatementWHS.pdf>

stakeholder interviews based on the analytical framework and the ToR question list, to provide a structure for responses. The Stakeholder Consultation Group was invited to participate in the research to provide guidance and feedback. Initial participation by the consultation group allowed us to gather a range of perspectives to fully understand the dimensions of the issue.

Two country case studies, Yemen and South Sudan, were identified to add context to the research. Interviews were conducted with a range of stakeholders involved in oversight and implementation of transfers in both locations (Amman in the case of Yemen, given security context in country, and Juba respectively). In Juba, the research team visited the Protection of Civilians camp on the outskirts of the capital, in order to conduct a number of focus group discussions with camp residents, to receive feedback directly from people whose data has been registered in appropriate MIS (and those whose data has not been recorded – see below for details).

2.3 Structure

The report is organised in the following way.

Following this Introduction, Section Two sets the scene on the humanitarian-development nexus, outlining key issues and concepts as a framing for this research.

Section Three – sets out the risks, benefits and trade-offs identified from the growing literature on MIS interoperability, as well as case studies.

Sections Four and Five provide detailed descriptions of the two country case studies. While all country contexts are unique, and further illustrations would certainly add value, the two cases explore the “MIS context”, i.e. describing the humanitarian scenario, the range of major transfer systems present (both government-related and independent aid agency managed).

Section Six sets out a discussion based on the above theoretical underpinnings from academic literature and the two “real world” country examples and provides reflections and perspectives.

Section Seven makes recommendations and sets out a way forward for their implementation.

Annexes provide further theoretical background and basic information and definitions. Annex 1 aims to explain to those unfamiliar with MIS what the function is, what the purpose is, and what the possibilities for interoperability are. It goes into detail on types of interoperability, and simply explains key issues raised in the main report such as digital identity, consent, and biometric data. Readers unfamiliar with these topics may wish to review this section first. Annex 2 provides definitions of typical beneficiary caseloads and their predicament to illustrate the range of people’s situations which a transfer system needs to respond to – ranging from independent humanitarian aid to government managed systems. Annex 3 comprises a Risk Table to complement section three, outlining the key risks and benefits of MIS in Crises, broken down by type of interoperability (i.e. different types of interoperability vs fragmented), and Annex 4 outlines the analytical framework for this report.

3 CONTINUUM OF SOCIAL TRANSFERS

This section covers the current trends and thinking on Management Information Systems (MIS) in crises, including humanitarian assistance and the transition to social protection. It summarises:

- Learnings from the literature review and key informant interviews regarding the transition from humanitarian transfers towards government-led social protection;
- Trends towards the use of cash in humanitarian action and social protection; and
- Trends toward centralisation, particularly at the humanitarian-development nexus.

3.1 From humanitarian transfers towards government-led social protection

There are many definitions of social protection,¹⁰ a simple version being that it is “the set of public actions that help households address risk and moderate their vulnerability to hazards and shocks”.¹¹ Translating this definition into possible interventions, Devereux and Sabates-Wheeler (2007) categorise social protection into the following themes:

- Protective (recovery from shocks);
- Preventative (mitigating risks to avoid shocks);
- Promotive (promoting opportunities); and
- Transformative (focusing on underlying structural inequalities).¹²

MIS containing personal data on both beneficiaries and non-beneficiaries (or potential beneficiaries) are likely to form key components under each of these themes. For example, a “protective” social protection programme seeking to aid early recovery following a disaster may attempt to maintain a list of potential beneficiaries, including bank details to allow for rapid transfers to affected persons/households following a disaster. With any such system, there will be challenges involved in ensuring that data are kept up to date, particularly with non-beneficiaries who may be unlikely to frequently update their personal details if they are not receiving a regular transfer.¹³

It is widely agreed that social protection should preferably be government owned. Social protection comprises a range of policy, programmatic and legal measures that protect and support individuals, households and populations at different life stages. Decisions over revenue collection and resource distribution are sovereign mandates and form part of a nation’s social contract. While ideally social protection is defined by national policies and institutions, other actors may have supporting and implementing roles to play, where this is beyond government capability.

The Good Humanitarian Donorship initiative, broadly supported by donor governments, states that the objectives of humanitarian action are “to save lives, alleviate suffering and maintain human dignity during and in the aftermath of man-made crises and natural disasters, as well as to prevent and strengthen preparedness for the occurrence of such situations”.¹⁴ Humanitarian action is guided by Humanitarian Principles. Derived from the Fundamental Principles of the ICRC, the four principles endorsed by the UN General Assembly are: humanity, neutrality, impartiality and independence.¹⁵

In less developed countries, including in fragile and conflict-affected states, options and instruments for providing direct assistance are often limited.¹⁶ Humanitarian concerns dominate international engagement, and government motives and capacity are variable. Domestic governments are often not engaged for a variety of reasons, including lack of capacity, or due to their role as parties to the conflict, as well as occasionally out of convenience. This leaves humanitarian efforts often being managed independently of government. Consequently, policy decisions tend to be set by international donors and

¹⁰ See, for example, Appendix A (p101) of the *World Bank 2012–2022 Social Protection and Labor Strategy*, which provides a list of agency definitions of social protection.

¹¹ Poverty Reduction and Policy Regimes Thematic Paper Social Protection and Poverty. Barrientos, A. UNRISD, Social Policy and Development Programme Paper Number 42 January 2010

¹² IDS Working Paper 232 *Transformative social protection*, Stephen Devereux and Rachel Sabates-Wheeler October 2004

¹³ See, for example, Barca and O’Brien, Factors affecting the usefulness of existing social protection databases in disaster preparedness and response (Policy Brief: Shock Responsive Social Protection Research – December 2017).

¹⁴ Good Humanitarian Donorship Initiative, ‘24 Principles and Good Practice of Humanitarian Donorship’ (Stockholm, 2003, as amended by members at the June 2018 High Level Meeting in New York)

¹⁵ See General Assembly resolution 46/182 (1991), which adopted the principles of humanity, neutrality, impartiality, and General Assembly resolution 58/114 (2004), which added independence.

¹⁶ Cooper, R. (2018). Social safety nets in fragile and conflict-affected states. K4D Helpdesk Report. Institute of Development Studies

implementing agencies, without inclusion of domestic political priorities. This goes even further in areas with significant humanitarian access issues, where “remote programming is becoming the norm” and INGOs are increasingly basing their response across borders (for example, remote programming for Yemen from Amman), leading to both remote decision-making, and potentially remote data storage.¹⁷ This has follow-on implications for the applicable legal regime(s), as outlined in Section 4.3.1, below).

Life-saving humanitarian assistance has a very narrow focus, and donor funding tends to be approved for very short finite periods, despite protracted crises extending over many years. These features do not provide continuity or certainty to recipients or a perspective of a pathway to a post-crisis system. While an essential and justified priority, humanitarian support therefore potentially ignores the development process and risks being detrimental to the restoration of a future governance structure. This is particularly problematic in protracted crises.

There is therefore increasing pressure on humanitarian actors to work with governments to smooth the transition from the humanitarian to the development context. For example, one of the Commitments to Action from the World Humanitarian Summit 2016 is to reinforce, rather than replace, national and local systems.¹⁸ The Grand Bargain commitments to provide more support and funding tools for local and national responders, and include people receiving aid in making the decisions which affect their lives, among others, support this effort.¹⁹ Similarly, the Statement from the Principals of OCHA, UNHCR, WFP and UNICEF on cash assistance, setting out their vision for a common cash system, confirms that they “recognize the primary role of governments in supporting vulnerable populations and will build on, utilize and leverage existing government systems, whenever possible”.²⁰ However, in this transition, it is important that beneficiaries’ rights come first. The implications of this transition on the right to privacy, for example, must be carefully considered when transitioning to increased government ownership of social protection.

3.2 Cash

There is growing support internationally for increased use of cash transfers in both humanitarian and social protection programming. For example, the Grand Bargain includes a commitment to “Increase the use and coordination of cash-based programming”.²¹ At the June 2018 High Level Meeting in New York, the Good Humanitarian Donorship initiative members adopted a new principle: “Systematically consider the use of cash transfers alongside other modalities according to context, in order to meet the humanitarian needs of people in the most effective and efficient manner.”²²

Global evidence shows that cash transfers are predominantly used by recipients to improve access to food (improving quantity and quality);²³ to reduce household debt and to improve access to other (non-food) household essentials, water and education. There is increasing consensus that cash-based programming acts as an important means of consumption support for the poor, reducing vulnerability and cushioning the impact of shocks and crises such as drought.

¹⁷ Ismail, Z. (2018). Humanitarian Access, Protection and Diplomacy in Besieged Areas. K4D Helpdesk Report. University of Birmingham

¹⁸ World Humanitarian Summit 2016 ‘Commitments to Action’ (8 September 2016)

¹⁹ Inter-Agency Standing Committee ‘The Grand Bargain (Official website): Workstreams’, <https://interagencystandingcommittee.org/grand-bargain>

²⁰ Statement from the Principals of OCHA, UNHCR, WFP and UNICEF on cash assistance (5 Dec 2018), <https://reliefweb.int/report/world/statement-principals-ocha-unhcr-wfp-and-unicef-cash-assistance>

²¹ Inter-Agency Standing Committee ‘The Grand Bargain Workstream 3: Increase the use and coordination of cash-based programming’, available at: <https://interagencystandingcommittee.org/increase-the-use-and-coordination-of-cash-based-programming>

²² Good Humanitarian Donorship Initiative ‘24 Principles and Good Practice of Humanitarian Donorship’ (Stockholm, 2003, as amended by members at the June 2018 High Level Meeting in New York)

²³ See, for example, The Role of Cash Transfers in Social Protection, Humanitarian Response, and Shock-Responsive Social Protection (IDS Working Paper, Volume 2018 No 517); and Berg and Seferis Protection Outcomes in Cash Based Interventions: A Literature Review (January 2015)

However, this increasing shift towards cash has been accompanied by a push for greater accountability, with a higher standard often applied to cash-based programming²⁴ despite evidence that cash transfers increase accountability to beneficiaries and other stakeholders.²⁵ This focus on accountability, combined with Know Your Customer (KYC) and anti-money laundering (AML) obligations,²⁶ can distract attention from and potentially have adverse impacts on beneficiary privacy rights. This is due to the need to collect and store even more information from beneficiaries, potentially sharing this data to demonstrate compliance, and a shift in treatment of beneficiaries as subjects of potential suspicion of AML violations, rather than as beneficiaries with rights to access services.

These challenges are possibly even greater with conditional cash transfers (CCTs) than with unconditional cash transfers (UCTs). “The inherent complexities of CCT programmes require processing of greater volumes of information. Information flows are more frequent and complex (specifically, information must be shared between schools, health services, social protection authorities and payment-service providers quickly and effectively to monitor conditionality compliance), entailing additional data- and privacy-protection challenges, particularly in countries with weak administrative capacities. Privacy breach and data protection risks increased for CCTs when appropriate safeguards were not in place.”²⁷ As noted in Section 5.6 and Annex 1, reducing the amount of data collected and stored, including by reducing targeting complexity and variation, can help reduce these risks.

Moreover, compliance with the set conditions must be monitored on an ongoing basis, applying sanctions for non-compliance or reinstating a beneficiary, all of which are rarely straightforward, can lead to exclusion errors due to data collection challenges, and require continuous, substantial data collection and ongoing data holding. Streamlined programming that takes a more universal, rights-based approach, is therefore often more appropriate, and likely more effective, as the default means of providing transfers, particularly in environments with low levels of capacity and service provision.

3.3 Increasing pressure for centralisation

This report is written in the context of a trend observed among many of the donor staff and humanitarian actors²⁸ interviewed to increasingly support greater interoperability, and in some cases the development of single or social registries for social assistance programmes and move away from separate and disconnected MIS. The push for greater interoperability is evident in the Joint Donor Statement on Humanitarian Cash Transfers, which envisages “solutions whereby interoperable, non-proprietary, data registries can allow a level of data sharing between humanitarian agencies and private sector service providers” and “ensure that where possible cash programmes link to existing social protection interventions or build the blocks of future longer-term assistance”.²⁹

The UN is pushing for common approaches to cash and the scale-up of collaboration amongst agencies, from “no-regrets moves” which include information sharing, such as the exchange of data between WFP Somalia and UNHCR Kenya to allow beneficiaries to use single payment instruments. At the other end of the spectrum, it sees “game-changers” as solutions where delivery is co-designed, or one UN agency

²⁴ See, for example, FAO ‘Quality and Accountability in Cash Transfer Programming’, available at: <http://www.cashlearning.org/downloads/Quality%20and%20Accountability%20in%20Cash%20Transfer%20Programming.pdf>

²⁵ ODI and CDG ‘Doing Cash Differently: How Cash Transfers Can Transform Humanitarian Aid – Report of the High-Level Panel on Humanitarian Cash Transfers’ (14 September 2015)

²⁶ Key Informant Interviews

²⁷ Sepúlveda Carmona, Magdalena. 2018. ‘Is Biometric Technology in Social Protection Programmes Illegal or Arbitrary? An Analysis of Privacy and Data Protection.’ Extension of Social Security (ESS) Working Paper No. 59. Geneva, Switzerland: International Labour Organization (ILO).

²⁸ In addition to variation across the different organisations interviewed, it is important to note that variation in perspective was also present *within* organisations. Opinions varied between head and country offices, or even within the same office. Not all organisations have a uniform perspective on this issue internally.

²⁹ Joint Donor Statement on Humanitarian Cash Transfers, June 2019, Cash Learning Partnership <http://www.cashlearning.org/resources/library/1363-joint-donor-statement-on-humanitarian-cash-transfers>

uses services of another, such as a central data repository which each system feeds into; or UNICEF and WFP both utilising SCOPE ³⁰for delivery.³¹

Both in the literature and stakeholder consultations, the benefits of increased interoperability and/or centralisation are frequently, though not exclusively, defined in terms of efficiency gains (and in fewer cases, effectiveness), rather than other key VfM elements or protection. This issue is discussed further in Section 4.4.1.

3.4 Conflation of interoperable humanitarian systems with government-led social protection

In addition to greater interoperability between humanitarian actors, the drive for interoperability between humanitarian actors and government-led social protection is growing. Whilst there is increasing recognition that the success of linkage depends on the level of maturity of the government-led system and the political and economic context,³² there is also a push to bridge the humanitarian-development nexus. The Joint Donor Statement on Humanitarian Cash Transfers, following agreements made at the World Humanitarian Summit 2016, states that unless the government is an active stakeholder in the conflict, it should be involved in the response.³³ Whilst this is the case in many humanitarian conflicts and protracted crises, there is a commonly held assumption that a centralised humanitarian transfers system (or parts of such a system) may form the basis of a longer-term or government-led social protection systems.

The literature shows a trend towards management information systems that allow for eventual transition to government, with the aim of increased efficiency and government ownership, but little consideration of the data protection implications. For instance, the report *Humanitarian Capital?*³⁴ outlines numerous cases where humanitarian systems have been rendered interoperable with government-led social protection systems. In the section focused on crisis settings, the report suggests considering how lessons and systems generated by UN agencies might be retained and shared with government post crisis. However, the report does not mention any data protection concerns or issues around consent, even in a setting where data and consent would have been collected in a time of crisis. The same is true of the recent joint GIZ / DFID publication Building an integrated and digital social protection information system.³⁵ However, a recent shift in focus is evident in the latest Social Protection Inter-Agency Cooperation Board (SPIAC-B) issues paper, which intends to initiate a discussion amongst members regarding data protection.³⁶

³⁰ A detailed description of the SCOPE system is available in Annex 1

³¹ Cash Digitization: UN Collaboration, Coordination, and Harmonization Opportunities

³² See, for example, Idris, I. (2019). Linking social protection and humanitarian response: Best practice. K4D Helpdesk Report 684. Institute of Development Studies.

³³ European Union Reference Document on Social Protection across the Humanitarian Development Nexus

³⁴ Gentilini, Ugo; Laughton, Sarah; O'Brien, Clare. 2018. *Humanitarian Capital?: Lessons on Better Connecting Humanitarian Assistance and Social Protection (English)*. Social Protection and Jobs Discussion Paper; no. 1802. Washington, D.C.: World Bank Group.

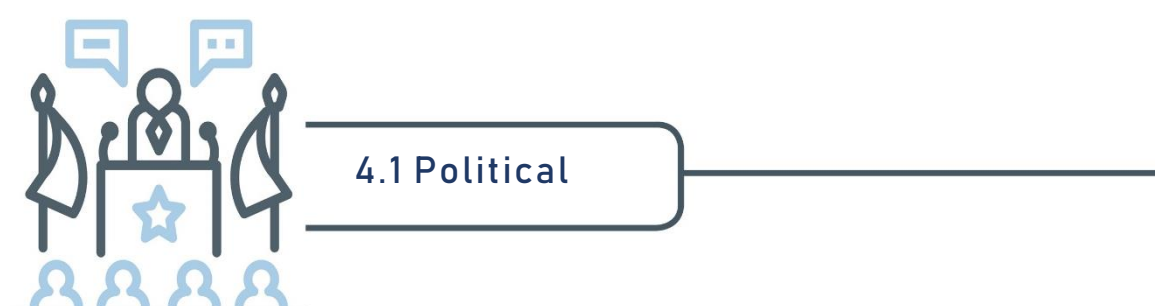
³⁵ Barca, V., Chirchir, R., Building an integrated and digital social protection information system, GIZ and DFID, October 2019 and February 2020 (full technical paper)

³⁶ Data protection for social protection: An issue paper for the SPIAC-B group to discuss key issue areas concerning middle and low-income countries (Draft, April 2020)

4 MANAGEMENT INFORMATION SYSTEMS – RISKS AND BENEFITS

This section discusses the key issues that should be considered by humanitarian and development actors and policy advisors. It comprises an analysis of the risks and benefits of fragmented, interoperable, and centralised MIS, based on the analytical framework (see Annex 4 – for full details see the inception report) defined by the research team through a literature review. An assessment of the literature and existing practice found that implications of fragmented MIS can be grouped into the following thematic areas: political, protection, legal and ethical, commercial, and operational.

This section focuses on both the literature regarding these thematic areas, and two country case studies, Yemen and South Sudan, which provide context for this research and informed these discussions. This section is complemented by a comprehensive risk and benefits table in Annex 3 which looks at these against different interoperability options.



Concerning the implications of political economy realities. For instance, organisational tensions, beneficiary trust in government, and government involvement in conflict (potential contribution to conflict resolution and stability).

4.1.1 Political misuse of data

There is widespread recognition in the literature of the potential for politicisation of identification and registration data and political manipulation and control of databases by host governments, particularly during crises. The value of personal data (and even more so, biometric data³⁷) for identifying individuals of concern to State, law enforcement, security and judicial bodies, is clear. Devereux and Vincent note that “the potential for political abuse will only increase as the use of technology and databases becomes more widespread”³⁸. They assert that political manipulation and control of centralised databases are the main risks of ICT. Whilst there is little other than anecdotal evidence of government manipulation of personal data, there is common understanding that centralised (including single) databases increase the risk of political access, both in terms of attractiveness of large datasets, and technical weakness of having significant datasets in one location. Risks are always prevalent, so the best path of action is to minimise the number of entities accessing data and ensure any possible holes in security are monitored, among other measures like data minimisation and proportionality, as discussed in Section 5.6 and Annex 1.

The fear here is not necessarily the legality of access to the data but concerns around the implications of political access. Whilst data access may be provided for in national law, it may not be compatible with human rights, the level of consent gained, or the principles of humanitarian action (see Legal & Ethics section below). This access may be covert or overt, and both carry risks: while overt access may appear to be more likely to be subject to democratic scrutiny than overt access, this assumes well-functioning

³⁷ More details on the risks associated with biometric data can be found in Annex 1

³⁸ Devereux, Stephen, and Katharine Vincent. “Using Technology to Deliver Social Protection: Exploring Opportunities and Risks.” *Development in Practice*, vol. 20, no. 3, 2010, p 374. JSTOR, www.jstor.org/stable/27806713

rule of law and the ability to challenge powerful actors. There are numerous implications of political access to personal data, including:

- Personal security – highly sensitive data such as religion or ethnicity may allow a government authority to identify and target groups in opposition, or other minority groups. Ethnicity is not commonly collected due to recognition of the risks, but there are cases where it is included on national ID, for instance Rohingya refugees demanded an ID card listing their ethnicity in order to counter Myanmar's erasure of their ethnicity and citizenship.³⁹ Other data not considered highly sensitive, such as birth place or surname may enable government to conclude or assume ethnicity or tribal affiliation.
- Discrimination – access to humanitarian data by government actors is often problematic in humanitarian contexts, particularly in protracted crises. Government may seek to discriminate against those with refugee status, against a particular ethnic group, or rebel groups. Access to this data allows for the easier identification of such groups. For instance, through key informant interviews the research team learned of a case in Syria whereby government are attempting to gain access to data collected by enumerators, humanitarian actors and journalists. Such actors are required to wipe information off their devices after collection to ensure they or those whose data they collected are not put at risk.



Example: Government Pressure for Personal Data

According to key informants, the Nigerian Government requested data on beneficiaries from Action Against Hunger and Mercy Corps. On refusal, the army claimed it had credible intelligence the charity was one of a number involved in subversive activities and was aiding and abetting terrorists. The NGOs were subsequently prevented from operating in Nigeria.⁴⁰

4.1.2 Political Economy

There are numerous political risks and benefits of each type of database, due to the specific governance environment and conflict sensitivities, as well as the political economy of aid. Barca sees integration between humanitarian and government MIS as principally a policy issue, requiring political and institutional arrangements rather than technical fixes.⁴¹ The challenges of transition from humanitarian to government-led social protection systems are clearly outlined in the literature. Integration requires the appropriate policies, government capacity and budget, data protection policies, technical capacity, coherence/lack of fragmentation across relevant government departments, trust between citizens and government – to name a few. However, as noted by the Cash Learning Partnership, other than discrete examples, systemic discussion on and practical examples of linkages between humanitarian cash voucher assistance and government social protection are in early stages and visions of what synergies could look like are not clear or agreed.⁴²

However, the prevalence of politics extends beyond government structures, with implications for integration of or interoperability between separate humanitarian MIS – an issue which is not fully defined in the literature. A central cause of the fragmentation of MIS amongst humanitarian agencies is political tensions, protectionism, and competition between organisations.

The humanitarian sector is still prone to market forces, such as competition for funding and a draw towards the latest technology for the sake of innovation. As such, agencies may tend to prefer development and promotion of their own MIS and endeavour to dominate the market, using the latest technology to differentiate themselves from competing agencies. By utilising a proprietary system, an

³⁹ The Engine Room, "Understanding the Lived Effects of Digital ID" <https://digitalid.theengineroom.org/>

⁴⁰ <https://www.theguardian.com/world/2019/sep/29/nigeria-warned-it-risks-humanitarian-disaster-by-expelling-charities>

⁴¹ Barca, V. Integrating Data and Information Management for Social Protection: Social Registries and Integrated Beneficiary Registries (2017)

⁴² Cash Learning Partnership (CaLP) and Inter-Agency Research and Analysis Network (IARAN), The Future of Financial Assistance: An Outlook to 2030 (November 2019)

agency can maintain control over its own data, including collection processes, storage, and to limit sharing to protect its perceived competitive advantage through its greater access to and control over data on target populations.⁴³ Though open source software is not necessarily more or less secure,⁴⁴ it is more transparent and open to scrutiny.

Competition for funding may mean that an agency is reluctant to share data, for instance, to maintain dominance in a geographical area where that agency has the most detailed information. Some key informants also expressed concern that by sharing their data, flaws or gaps would become known to competitors or donors.⁴⁵ Separate mandates are also a critical inhibitor to full integration, as agencies such as UNHCR understandably need to protect their mandate, in order to protect the data of the most vulnerable. The Cash Learning Partnership notes a lack of trust between agencies, stating that the “creation of a single registry and a single framework for cash transfers would be a challenge due to the number of actors, differing priorities, objectives and interests.”⁴⁶

Much of the debate is around the advantages of MIS interoperability, while in fact the trend is towards the predominance of a few proprietary systems. There are few examples of collaboration between humanitarian agencies. There are many areas of single systems development where more collaboration would deliver better outcomes. Some are mentioned in the UN Statement: “This common cash system will also encompass joint cash feasibility assessment, coordinated targeting of beneficiaries, a single transfer mechanism, joint post-distribution monitoring and pursuing accountability to affected populations through agreed complaints and feedback mechanisms.”

Even as the technology is still developing, there is a trend towards consolidation of larger systems in humanitarian contexts – SCOPE, Brave, PRIMERO and ProGres. The UN agencies and the World Bank responsible for these systems view them as proprietary, giving them a competitive advantage over others, offering donors a unique proposition when considering financing options. Several key informants noted that this has created a one-upmanship culture in a quest to prove who can be the most innovative and dominate the market. Whilst some NGOs have their own MIS such as World Vision’s LMMS, users are increasingly looking to operate under these four systems. Alongside this there are bespoke systems being developed for government – such as SSSAMS and SSSNP in South Sudan and SWF and SFD in Yemen.

Matters of political economy both in humanitarian assistance and its transition to social protection are echoed in the Digital Cooperation Report.⁴⁷ The authors state that the need for digital cooperation isn’t concerned with the technical nuts and bolts but with the “unprecedented economic, societal and ethical challenges that they cause”⁴⁸.

4.1.3 Government – humanitarian sector tensions

In situations where humanitarian actors are in tension with the government,⁴⁹ the collection or presentation of data may be controversial, or cause further tensions with government. For instance, data may be perceived to be collected in a dishonest way and/or misreported by humanitarian agencies for their own aims. In such cases, the collection of data in and of itself may worsen political tensions and put enumerators or humanitarian workers at risk. The study team heard of such examples over the course of this research.

⁴³ Key informant interviews.

⁴⁴ Collins, H. ‘Is Open Source Software More Secure than Proprietary Products?’ (Government Technology, 30 July 2009), <https://www.govtech.com/security/Is-Open-Source-Software-More-Secure.html>

⁴⁵ Key informant interviews, and ACAPS South Sudan Analysis Ecosystem (<https://www.acaps.org/special-report/south-sudan-analysis-ecosystem>) and Yemen Analysis Ecosystem (<https://www.acaps.org/country/yemen/special-reports#container-1270>).

⁴⁶ Cash Learning Partnership (CaLP) and Inter-Agency Research and Analysis Network (IARAN), The Future of Financial Assistance: An Outlook to 2030, (November 2019)

⁴⁷ “The Age of Digital Interdependence” Report of the UN Secretary-General’s High-level Panel on Digital Cooperation (2019)

⁴⁸ Ibid.

⁴⁹ This is likely to be the case in many conflict contexts, particularly where the government(s) is/are a party to the conflict, but may be less so in humanitarian responses to disasters, for example.



4.2 Protection

The tension between protection and inclusion, including obligations to beneficiaries (security, consent, preferences, etc), proportionality (in data collection and sharing) and accountability.

4.2.1 Fairness

It is widely stated in the literature and by key informants that increased interoperability increases the potential for accuracy of targeting and reduces “double dipping”. Claiming duplicate benefits may be in the individuals’ interest to provide for their family and is understandably preferable for the individual to receive more aid. However, in a context of limited resources where one household receiving multiple benefits may mean that another receives none, this can raise concerns regarding fairness and potential corruption. This review did not find evidence regarding the relative impact of providing multiple benefits to one household (potentially increasing the likelihood of a positive impact on that household, especially where none of the benefit packages alone are sufficient to meet basic needs), versus providing only one benefit, likely insufficient on its own, to a larger number of households. Greater data sharing across organisations may help address this gap, but carries the many risks outlined throughout this paper.

Fairness, accountability and transparency of resource sharing is often implied to result from de-duplication, but not explicitly stated due to the focus on operational efficiency gains (see section below). Knowing that distributions accurately follow the defined targeting approach should result in more accurate measurements of impact, which in turn leads to better programme design.

In an analysis of social protection MIS, Barca (2017) notes the potential advantages of integrating data and MIS for social protection on policy, leading to a more equitable approach to the distribution of resources based on shared objective and comparable information. However, such an approach would require coherence of eligibility criteria, not just information sharing through integrated MIS.⁵⁰

Poverty and vulnerability definitions have significant bearing on everything that follows in social transfer design. Definitions used have implications for programming, targeting, access conditions, data use and risk. Humanitarian and development agencies have a range of philosophical, political, and economic views, some seeing poverty as financial deprivation or food insecurity, others identifying a broader range of deprivations. Cash transfers potentially mitigate financial deprivation but there are limits to the impact of direct transfers in addressing multidimensional poverty (e.g. economic, jobs, access to services, governance, security, justice). With limited resources available to meet widespread needs, there is a perceived need to ration and control who is targeted and who is not. Determining eligibility requires considerable amounts of personal data, in turn requiring large field teams to collect and assess this data.

However, assessments of such methodologies conclude these approaches can be perceived as unfair and sometimes divisive and corrupt. In insecure “remote management” conflict contexts, targeting inaccuracies are likely to be magnified – and moreover remain unknown and unaddressed. Targeting of individuals or households requires large data collection and updating (the latter often under-resourced). Data-management, as discussed throughout this work, has risks as well as costs. A precautionary approach should be applied to data registration i.e. by collecting minimal data as needed for programme requirements. Data types should also be segregated, with different types only accessible when required for a specific task – for example, targeting which may require more detailed data on poverty indicators, but would not require information like bank account numbers and contact details, as compared to transfer implementation which would require this information, but would likely not require the types of data used for targeting. While there is a commonly held assumption that large development agencies

⁵⁰ Barca, V. Integrating Data and Information Management for Social Protection: Social Registries and Integrated Beneficiary Registries (2017)

have good risk management approaches to data, what can be expected of host government management in such contexts?

4.2.2 Discrimination

In addition to the concerns outlined in the previous section related to political use of data, other actors such as governance or financial institutions may facilitate discrimination based on an individual's identity or status. For instance, an individual receiving cash transfers through a financial institution may in the future be discriminated against in their pursuit of a loan, due to their status as a beneficiary of assistance. Risks of data misuse increase as more actors gain access to datasets, whether through a single system, or interoperability of different systems.

4.2.3 Hacking, data leaks and other implications on personal security

There are numerous ways in which an individuals' data can be accessed: for instance, there could be a hack by an opposition group or data may be leaked purposefully or through human error. Single or centralised databases are targets for theft (for uses including commercial, security, anti-terrorism, etc.) as they are more attractive targets due to the quantity of data. Single systems, as they are often a merger of numerous systems, often have the security of the least common denominator and, like centralised systems, single systems also have one point of vulnerability. Federated databases⁵¹ are generally lower in risk than centralised systems with their single point of attack and failure, and because they have multiple layers of security, assuming secure design and appropriate data sharing agreements and standards are followed. Privacy International note that "there is a significant difference between storing biometric data⁵² locally than storing them in a centralised database, with the latter being significantly more intrusive to privacy".⁵³ Even those MIS which are considered secure and with comprehensive data protection protocols and cyber security processes are subject to failure through human error or a lack of enforcement. During this research, the team noted - from publicly available reviews - some humanitarian organisations which are not upholding their own data protection standards.⁵⁴

Nevertheless, fragmentation also increases security risks for users' personal data⁵⁵ due to the numerous instances of their data being recorded and accessible to a variety of interested parties. Relatively small organisations may have fewer resources to apply rigorous protection standards and lack the resources, infrastructure, connectivity, etc., to apply them, leading to poor application of these standards. This was observed during key informant interviews with implementing partners for both country case studies.



Example: Hacking

Media staff, military personnel and humanitarian actors in Syria in 2013 were targeted by a large malware attack. The unknown threat group entered the system by sharing malware through Skype, striking up conversations with individuals. The threat group stole information such as Skype conversations, humanitarian needs assessments, humanitarian financial assistance disbursement records, and lists of refugees receiving aid including scans of their ID cards.⁵⁶

⁵¹ For a simple explanation of types of MIS, see the Annex or DAI blog <https://dai-global-digital.com/the-back-end-of-management-information-systems.html>

⁵² More details on the risks associated with biometric data are in Annex 1

⁵³ Ibid.

⁵⁴ <http://www.thenewhumanitarian.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling>

⁵⁵ Cash Learning Partnership (CaLP) and Inter-Agency Research and Analysis Network (IARAN), The Future of Financial Assistance: An Outlook to 2030 (November 2019)

⁵⁶ Regalado, D. et al. 'Behind the Syrian Conflict's Digital Front Lines' (FireEye, February 2015), <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf>

4.2.4 Proportionality

As noted above, a large dataset may be attractive due to the potential for data analysis. Where MIS share data or in the case of a single MIS with multiple users, there is a potential for mission creep, as increasing amounts of data need to be collected to satisfy different parties and their analytical and service provision needs. For instance, in South Sudan in order to align the IOM and WFP systems, IOM collects an additional nine fingerprints from beneficiaries.



Example: Biometric Storage

Biometric passports that store the biometric details of an individual on a chip in the passport, rather than a centralised database, are used in the UK. Storing biometric data locally allows for the use of biometrics for authentication (to be sure that the person with the document is who they claim to be) but prevents its use from the far more intrusive process of identification (finding the identity of a person when it is not known).⁵⁷

As a further example, Organisations A and B may be collaborating on provision of in-kind goods. Organisation A may specialise in child protection and wish to have data on number of children and their ages, whereas Organisation B may require the details of only a head of household. If these organisations were to make their MIS interoperable, they may decide that both need to collect information on the number of children from any household they register (even when Organisation B is conducting the registration and does not otherwise require this information for its own programming), so data can be read. Otherwise, each organisation would have to register the same household separately, eliminating one of the key benefits of interoperability – only requiring a household to register once.

Risks also arise in the case of multiple, fragmented MIS, where data are currently being over-collected, lost and reproduced. Affected populations are often⁵⁸ surveyed multiple times, triggering questions regarding the ethics of beneficiary data collection.⁵⁹

4.2.5 Data sharing

There are implications of ever-increasing interoperability on human rights and data protection standards. Disparate or interoperable systems both may operate in conjunction with a variety of private sector institutions and NGOs serving as enrolment centres. This may increase the number of parties that have access to at least some of an individual's data.

Systems with multiple users bring further implications for individual security. The implications of third-party providers' data standards could be huge on individual security, dignity and data protection. Some concerns have been raised over partnerships between humanitarian agencies and private technology corporations, which are often at the centre of debates around ethics and data protection. Such partnerships have led to some challenges around the credibility in and trust of humanitarian action.⁶⁰ There are wider concerns over the protection of sensitive information and the data protection rules⁶¹ that will apply to third party providers: "information sharing and consent becomes increasingly difficult to obtain as more actors are involved in the collection and storage of data, in turn resulting in affected populations losing control of their personal data."⁶²

⁵⁷ <https://privacyinternational.org/long-read/3067/have-biometric-id-system-coming-your-way-key-questions-ask-and-arguments-make>

⁵⁸ This is likely where multiple agencies are operating. However, this is not always the case, as in some areas (particularly areas that are hard to reach due to geography or conflict) only one, or potentially no, agency may be operating.

⁵⁹ Wilton Park, Digital Dignity in armed conflict: a roadmap for principled humanitarian action in the age of digital transformation

⁶⁰ Ibid.

⁶¹ Cash Learning Partnership (CaLP) and Inter-Agency Research and Analysis Network (IARAN), The Future of Financial Assistance: An Outlook to 2030, (November 2019)

⁶² Digital Dignity in Practice: Existing Digital Dignity Standards, Pursuing Digital Dignity and Current Gaps in Digital Dignity, (Wilton Park, 2019)

4.2.6 Further processing

Systems with multiple users and multiple purposes may also lead to data being utilised for purposes other than those initially intended or understood by the entity collecting the data, or by the data subject. For instance, a data subject may give consent believing that their data will only be used to consider their selection as a beneficiary and identify them as the receiver of aid for a particular agency's distribution. Their data may be used for this purpose, as well as for analytics by government regarding population flow, or shared with a service provider to assess family sizes in a certain area. If they did not consent to this, it raises concerns over the individual's control over their own data, and their dignity. The EU General Data Protection Regulation (GDPR) requires a data processor to have a legitimate interest, and the individual must have a reasonable expectation that their data will be used for such a purpose. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject, for instance, when processing is necessary for humanitarian purposes.⁶³ However, this legal basis generally cannot be relied on when, for example, sharing this data with others in a non-humanitarian context (as discussed below and in Annex 1: Consent).

Issues with further data processing are not only relevant to personalised data. Some argue that depersonalisation of data means the data now holds no risk to the individual. However, any depersonalised data, when combined with publicly available data (such as a Facebook profile), can have privacy implications. Nunan and Di Dumenico call this the unintended use paradox.⁶⁴ Big data poses risks to individual security as the amount of data to which supposedly "depersonalised" data can be connected to paint a fuller picture of the individual is ever-increasing. It is therefore imperative that a valid legal basis exists for this onward sharing and processing, even if data is to be de-identified and used for trend analysis. However, this same concern will likely not apply for very high-level summary statistics that do not involve anonymised personal data (which involves the risk of de-anonymisation), such as overall reporting on the amount of aid provided by an organisation, which can assist in planning and coordination but does not entail the same risks of de-anonymisation of sensitive personal data. See, for example, the 5W UN reporting system, which allows for consolidated reporting without hard data sharing.⁶⁵



Example: The possibility of anonymised data for monitoring

Even where personal data are not stored, big data techniques make it possible for organisations or government to identify an individual relatively easily. A piece by the New York Times exposing mobile phone location data, shows how these data can be used to identify an individual, by virtue of where they spend each night, or where they commute to each day. Seemingly harmless data, if combined with other datasets, could pose a risk to an individual's security if analysed by foreign security forces or national government who seek to do harm, marginalise or target.⁶⁶

⁶³ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ.L:2016:119:FULL>

⁶⁴ Herschel, R & Miori, V. Ethics & Big Data. Technology in Society 49 (2017)

⁶⁵ <https://www.humanitarianresponse.info/en/operations/nigeria/document/5w-process-coordinated-and-effective-response>

⁶⁶ One Nation Tracked, an investigation into the smartphone tracking industry
<https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>



4.3 Legal & Ethical

The ethical frameworks, legislation and regulation that guide and govern MIS

4.3.1 Domestic legal frameworks

There are various aspects of a country's legal framework which are essential for data protection, such as constitutional or other fundamental law determining citizenship and rights, duties and entitlements, laws specifically addressing privacy and data protection,⁶⁷ as well as international human rights law.

Governments need to have the authority and capacity to monitor and enforce the laws governing privacy and protection of personal data. As the European Court of Human Rights has noted "any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance" between the State's and the individuals' interests.⁶⁸

Data protection law governs how organisations should process, retain, store and destroy personal data. In some countries where humanitarian and development practitioners work, there may not be a legal framework in place. For instance, in South Sudan there are no national Data Protection laws or regulations. In the absence of bilateral or transnational agreements or standards, like the GDPR or the African Union Convention on Cyber Security and Personal Data Protection and associated regulations, sharing between jurisdictions in theory comes under international human rights law and international guidance on data protection (such as the UNGA Guidelines for the Regulation of Computerized Personal Data Files⁶⁹). However, there is little actual guidance on how to do so when it comes to biometric or other data. In the absence of domestic legal frameworks, international laws and standards become of increased importance.

It is also possible that multiple domestic, regional, and/or international laws will apply to data processing. For example, where the data is:

1. Collected in one jurisdiction with its own domestic and/or regional legal framework; and then
2. Processed in another jurisdiction, with another domestic and/or regional legal framework; or
3. Processed in the same jurisdiction, but by an organisation based in another jurisdiction that places legal obligations on all organisations based within its territory;⁷⁰ and then
4. Stored or backed up in yet another jurisdiction, with its own domestic and/or regional framework.

In such contexts, organisations will need to apply multiple legal frameworks at the same time, reconciling any conflicts between laws in favour of the highest, most rights-protective standard. To reduce this complexity and increase understanding, alignment under agreed international standards is recommended, as outlined in the next section.

⁶⁷ Clark, J (ID4D), The State of Identification Systems in Africa, World Bank Group (2017)

⁶⁸ Beduschi 2019 - (S. and Marper v United Kingdom, para. 112)

⁶⁹ UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, GA Res 45/95 (adopted 14 December 1990)

⁷⁰ For example, GDPR Article 3 states that its regulations apply to "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not".

4.3.2 International standards

The conversation around digital governance is a huge one, with consensus on the concerning lack of regulation and action to date. The technology industry has largely come up with non-binding codes of ethics and standards on digitisation, most of which are not grounded in law – for instance, Tim Berners Lee: Contract for the Web.⁷¹

The situation is similar for humanitarian actors, including the UN, for which there is a proliferation of non-binding guidance, despite strong comments directed at states regarding data protection and the ethics of requiring biometric information collection for enrolment in social protection.⁷² International organisations often benefit from various privileges and immunities from domestic law when operating in country, although this is not absolute and varies based on the organisation's founding documents and status. For example, "local law generally applies to UN premises unless this would be inconsistent with relevant international treaties, other applicable international law, or a regulation made by the UN pursuant to a headquarters or bilateral agreement."⁷³ As such, privileges and immunities must be determined on a case by case basis. In the face of this uncertainty regarding the application of local data protection law, to avoid a protection gap it is necessary to provide a clearer legal framework in international law for international organisations.

As is the case in digital governance more broadly, there is consensus⁷⁴ that humanitarian assistance is digitising faster than the legal and ethical frameworks governing this digitisation. The Digital Cooperation report agrees that it has to date proved difficult to establish international standards or rules for data exchange.⁷⁵

The humanitarian and development sectors are guided by principles such as do no harm and ensuring protection. However, without a common understanding of what do no harm looks like in a digital world,⁷⁶ actors will struggle to enact these principles. The prevalence of inadequate regulation and governance heightens digitalisation related risks for users.⁷⁷ The Digital Cooperation Report states that any standards and practices developed around digital services/activities would need to include clear accountability, to discourage misuse.⁷⁸

Specific guidance is needed in a digital world, with data protection as a key principle.⁷⁹ Digital solutions must be designed to comply with international human rights law to ensure protection of these rights⁸⁰. This is reflected in the literature regarding technology,⁸¹ noting that privacy is not just a human rights issue but is a fundamental technical property: this manifests in privacy enhancing technologies and privacy by design. We therefore need both the legal frameworks and technical properties to protect data and ultimately do no harm.

⁷¹ <https://contractfortheweb.org/>

⁷² See, for example, the concerns raised by the Human Rights Committee regarding the Canadian Government's "increasingly intrusive measures affecting the right to privacy, under article 17 of the Covenant, of people relying on social assistance, including identification techniques such as fingerprinting and retinal scanning. The Committee recommends that the State party take steps to ensure the elimination of such practices." See CCPR/C/79/Add.105 (7 April 1999), at paragraph 16.

⁷³ Kuner, C. 'International Organizations and the EU General Data Protection Regulation', *International Organizations Law Review* 16 (2019) 158-191, at 174

⁷⁴ Cash Learning Partnership (CaLP) and Inter-Agency Research and Analysis Network (IARAN), *The Future of Financial Assistance: An Outlook to 2030* (November 2019), among others

⁷⁵ "The Age of Digital Interdependence" Report of the UN Secretary-General's High-level Panel on Digital Cooperation (2019)

⁷⁶ Cash Learning Partnership (CaLP) and Inter-Agency Research and Analysis Network (IARAN), *The Future of Financial Assistance: An Outlook to 2030*, (November 2019)

⁷⁷ "The Age of Digital Interdependence" Report of the UN Secretary-General's High-level Panel on Digital Cooperation (2019)

⁷⁸ Ibid.

⁷⁹ Weaver, C., Powell, J., & Leson, H. (2019) Open Data, Development Assistance, and Humanitarian Action. In T. Davies, S. Walker, M. Rubinstein, & F. Perini (Eds.), *The State of Open Data: Histories and Horizons*. Cape Town and Ottawa: African Minds and International Development Research Centre.

⁸⁰ Beduschi, A. *Digital Identity: Contemporary challenges for data protection, privacy and non-discrimination rights*. Big Data & Society (SAGE) (2019)

⁸¹ Rachovitsa, A. *Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue*, *International Journal of Law and Information Technology* (2016).

4.3.3 Digital Dignity

Dignity in humanitarian assistance and development programming is not a new concept, and indeed is outlined in relation to digital technologies, such as the protection of an individuals' dignity during biometric data collection.⁸² Application of the concept of Digital Dignity in literature regarding identification and registration systems aims to further develop this and define the dignity of an individual in terms of their digital self: their data.

Digital dignity is defined by Wilton Park as 'the state when the agency, autonomy and identity of individuals, as well as the communities they are part of, is respected, enhanced and empowered through how data that is both derived from them and pertaining to them (inclusive of any interventions that utilise this data) are collected, handled, and employed in ways that realise the human rights and enhance the human security of these individuals and their communities'.⁸³ Importantly, this includes increasing data subjects' agency in both the collection and use of their data in ways that impact their rights, and indeed their lives. As per this definition, individuals should be respected as data agents, and not purely as data subjects. This means looking at the ways in which data is governed, to ensure that data governance aligns with core humanitarian and development principles. The promotion of digital dignity relies on the adoption of appropriate data protection standards and digital do no harm standards and protocols.⁸⁴

4.3.4 Do no harm and approaches to data protection

A 'do no harm' based approach to personal data collection must seek to minimise the possibility of risk, so personal data capture must be kept to a minimum for all agencies (including host governments). This is especially relevant in a high conflict context, as in the focus of this analysis, and has implications on the amount of data donors require for evidence. There are examples for this – the ICRC's most recent Data Protection guidelines recommend a minimal data collection policy⁸⁵ – and its recommendations for the collection of biometric data include storing it on beneficiary cards rather than a vulnerable centralised database. UNICEF's approach in Yemen is another example showing that minimal databased approaches, including non-biometric data, can work in high risk environments. A full Data Protection Impact Assessment (DPIA) can help inform assessment of the risks and potential harms arising from data collection and management.⁸⁶ Project specific M&E requirements should be aligned with DPIA results to ensure that data collection is proportionate and not surplus to cater for donor reporting requirements.

However, a uniform approach to data management and protection is not possible, as organisations have different mandates and resources. For some, different amounts and kinds of data collection and sharing is required to fulfil their obligations. The legal basis for data collection and management should be clearly articulated for any data collection and management practices.⁸⁷ Humanitarian mandates established under international law may grant United Nations agencies, the ICRC and others public interest grounds on which to collect and manage data. For example, UNHCR, unlike ICRC, operates at the request of host states.⁸⁸ Sensitive information is required for refugee status determination, and data sharing with host states may be required under the mandated relationship the organisation has with host states and with countries in which refugees may be resettled. In short, the legal bases for data collection are in part determined by an organisation's mandate.

The approach to providing services also determines the kind of data that needs to be collected and can amplify tensions and divisions. Targeted based benefits require further collection of detailed personal data both to assess vulnerability and to satisfy Due Diligence requirements. The issues around the

⁸² Fundamental rights implications of storing biometric data in identity documents and residence cards: Opinion of the European Union Agency for Fundamental Rights

⁸³ Digital Dignity in armed conflict: a roadmap for principled humanitarian action in the age of digital transformation

⁸⁴ Digital Dignity in Practice: Existing Digital Dignity Standards, Pursuing Digital Dignity and Current Gaps in Digital Dignity

⁸⁵ ICRC Data Collection Policy

⁸⁶ <https://gdpr.eu/data-protection-impact-assessment-template/>; see ICRC guidance on DPIAs, chapter 5 of the Data Protection handbook

⁸⁷ See Annex 1, and ICRC Data Collection Handbook for accounts of the different legal bases for collecting data

⁸⁸ See Statute of the Office of the High Commissioner for Refugees, as revised by GA res. 58/153, 22 December 2003; and UNHCR Division of International Protection, 'Note on the Mandate of the High Commissioner for Refugees and his Office' (October 2013). The issue of mandates is discussed in further detail in Annex 2.

collection of personal data are compounded by fragile field contexts where it may be political or physically difficult to collect information. Targeting is also exclusive by definition – there are winners and there are losers of any rationing system. In fragile contexts this can be divisive and amplify already existing tensions, and in conflict and transition contexts this is even more important to address.

Some of these risks may be mitigated by establishing a global data protection regulation – or at least, sectoral standards to data protection. This could be achieved by leading humanitarian organisations, such as all UN agencies, adopting shared standards for data protection – perhaps adopting an equivalent to European Union’s GDPR. This would have a standard setting effect for the humanitarian sector, as UN agencies and their implementing partners would have to conform to the same standards, and for states where the UN supports service and transfer delivery.

An additional approach to setting standards would be for donors to apply GDPR standards to all funded agencies including the UN – even if done by the EC alone, this would likely lead to widespread global adoption. These directions for mitigating risk are increasingly ones being taken by mainstream humanitarian organisations. ICRC’s Data Protection Policy references GDPR amongst others, and according to stakeholders interviewed as part of this research, UNICEF is also developing a data protection policy that views GDPR as its gold standard. But more needs to be done to encourage others to understand the risks of data management and practical aspects of implementing data protection, and to support smaller organisations including international and national NGOs who may not have the resources or capacity to develop their own approaches to data protection. This should be a key focus area for donors.

4.3.5 Basis for data processing

Conversations around data responsibility in the humanitarian sector centre around the idea of digital agency and the sense of ownership of one’s data, along with an increasing focus on obtaining consent for data collection and processing.⁸⁹ As in the medical sector, humanitarian agencies have more flexibility over the informed consent imperative, due to their mandate to provide life-saving assistance. They can (and often must) rely on other legal bases for data processing, such as vital or public interest. All major data protection standards/laws (ICRC, GDPR, OECD, AU, etc) recognise other lawful bases for data processing beyond consent. As noted by the ICRC Handbook on Data Protection, in some situations consent is not an appropriate legal basis for data processing. Most importantly, a person who has no other option cannot provide valid consent. Nonetheless, the inability to provide consent does not mean that services cannot be provided. This is common in humanitarian settings, and requires relying on another lawful basis, such as vital or public interest.⁹⁰

However, these alternative legal bases are unlikely to apply to future uses of this data, beyond immediate, life-saving support. A particular concern is around how to provide genuine informed consent in a humanitarian situation for (future, hypothetical) onward use of data, after other legal bases like vital or public interest are no longer applicable. It is difficult, and quite often impossible, to ensure that sufficient information on this onward use is provided to beneficiaries to confirm that their consent to this onward sharing is informed, particularly in FCAS where it is unclear who the “government” will be in the future. Ultimately, we need to consider: are we sharing data without consent to save lives in a context where consent is impossible? Or are we doing so for other reasons? This issue is addressed in further detail under the ‘Consent’ section in Annex 1, and recommendations are provided in section 4.3.5: ‘Basis for data processing’.

In addition, “digitalisation-related risks are heightened when the system is not understood by users, when it is not voluntary (or if there is no other option for obtaining assistance)”⁹¹. The UN Special Rapporteur states that policies around “digital by choice” are usually “digital only” in practice, and there should be a genuine non-digital option.⁹² Providing an alternative that allows for user choice, and considers socio-economic (e.g. an alternative to fingerprinting when fingerprints may be worn by labour) and cultural factors (such as providing an alternative to facial recognition for women who wear head

⁸⁹ Bryant, J. Willitts-King, B. and Holloway, K. *The Humanitarian Digital Divide* (2019)

⁹⁰ ICRC Handbook on Data Protection, Chapter 3: Legal Bases for Personal Data Processing.

⁹¹ “The Age of Digital Interdependence” Report of the UN Secretary-General’s High-level Panel on Digital Cooperation (2019)

⁹² Alston, P. Report of the Special Rapporteur on extreme poverty and human rights: Digital technology and the welfare state (UNGA, A/74/493, 11 October 2019)

coverings) is not only good human-centred design practice, but also allows for genuine informed consent. By providing an alternative, users are not forced to provide data they are not comfortable with – or not aware of the consequences of – to obtain the goods or services they need. This is particularly acute in humanitarian scenarios where the services are life-changing. While it may be challenging to develop and offer alternatives in early and/or acute phases of a humanitarian crisis, options can be explored through research outside of such crises, to ensure these options are available when a crisis strikes. In addition, during protracted crises, there may be more time and opportunities to develop these alternatives, even where the aid remains essential and life-saving, providing greater opportunities to seek valid (i.e. not forced), informed consent. Moreover, data protection standards more broadly should continue to improve as a crisis response stabilises. Not only should data use be explained, but beneficiaries should be able to confirm the data held on them and their families, to correct any inaccuracies, and exercise a right to delete or limit access to this data. When considering transition to build government systems, this would seem by definition to no longer be a humanitarian situation and separate consent would need to be sought for such a change of use.

A promising area of innovation is in the development of trust frameworks and schemes. These are approaches to creating an environment in which trust is built between interacting parties – they can refer to a trust framework, a set of requirements, a collection of contracts, a defined form of collaboration, a framework of standards, a system of enforcement mechanisms, and/or a certification scheme. An Open Identity Exchange (OIX) 2010 whitepaper on trust frameworks for identity schemes defines it as *‘A trust framework is a legally enforceable set of specifications, rules and agreements regulating an identity system.’*⁹⁴ A paper from National Institute of Standards and Technology (NIST)⁹⁵ defines a trust framework as *‘the set of rules and policies that govern how the federation members will operate and interact’* which can include conducting identity management responsibilities; sharing identity information; using identity information that has been shared with them; protecting and securing identity information; performing specific roles within the federation; and managing liability and legal issues. In simpler terms, *‘Trust frameworks serve as the basis for the multilateral agreements that enable the trust and governance of a federation’s operations among all of the federation’s members’*.

There are indications that this kind of approach can work in the humanitarian and development context. UNHCR has outlined intention to explore a Trust Scheme for identity management through the issuing of an RFP for a digital wallet for identification credentials⁹⁶, though there is slow progress in its implementation.



Example: Access to personal humanitarian data

A significant breach of the Red Rose data verification system in 2017 alerts to the potential for access and misuse of personal data of the most vulnerable. Mautinoa – a competitor exploring the Red Rose system – was able to access the cloud-based server of Catholic Relief Services and access the administrative dashboard, giving it full control to view and edit financial and personal details, and to download data. They were able to do so using clues from online training videos and technical weaknesses due to human error and inadequate cybersecurity. The system contained financial records totalling about \$4 million, provided by donors including USAID and the European Commission.⁹³

⁹³ The New Humanitarian, *Security lapses at aid agency leave beneficiary data at risk*, 27 November 2017, <https://www.thenewhumanitarian.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk>

⁹⁴ OIX June 2017 Trust Frameworks for Identity Systems, https://www.openidentityexchange.org/wp-content/uploads/2017/06/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf

⁹⁵ NIST January 2018, ‘Developing Trust Frameworks to Support Identity Federations’ <https://doi.org/10.6028/NIST.IR.8149>

⁹⁶ UNHCR November 2018, ‘UNHCR now accepting proposals on digital identity’ <https://www.unhcr.org/blogs/unhcr-accepting-proposals-digital-identity/>



4.4 Commercial

Implications of different types of provisions and interoperability measures on fiduciary responsibility, value for money, set up and maintenance and so on.

4.4.1 Value for Money

DFID generally defines Value for Money (VfM) in terms of economy, efficiency, effectiveness, cost-effectiveness, and equity.⁹⁷ The VfM benefits of de-duplication due to interoperable MIS with biometric registration, claimed by the majority of interviewees for this research, are therefore assessed against each of these components of VfM.

Economy focuses on achieving the best value inputs. However, achieving “economy” does not mean cutting costs regardless of the consequences. It requires understanding and justifying costs, but also recognises that context matters – operating in challenging environments and supporting the hardest to reach people will involve increased costs.⁹⁸

Efficiency seeks to maximise outputs for a given level of inputs. This is not merely about reaching more beneficiaries, but about spending well.⁹⁹ It requires an understanding of whether the inputs provided are having an impact, which requires evidence of what is working on the ground. To understand whether the use of interoperable MIS with biometric registration is efficient, we need to understand the costs involved in implementing these systems and achieving interoperability with other systems, as compared to previous approaches and other viable options. These costs are hard to track and monitor, as they involve a combination of costs from headquarters/field. development/operational, etc.

Effectiveness requires ensuring outputs are delivering outcomes. In a social protection context, relevant outcomes can include reduced extreme poverty and inequality, along with longer term development outcomes like improved resilience to life-cycle related vulnerabilities.¹⁰⁰ Beneficiary feedback and opinions are particularly important here. This requires strong mechanisms for obtaining and addressing feedback. Key criteria for effectiveness in a humanitarian setting identified by DFID include: coverage, appropriateness, timing, relevance, quality, equity, coordination, cost savings, and costs.¹⁰¹

Cost-effectiveness focuses on achieving impact for the lowest cost. Potential metrics in a social protection context include the percentage of GDP spent per 1% reduction in poverty incidence or the poverty gap. In a humanitarian context and in protracted crises, quantitative data like this may be difficult to obtain. External factors, such as renewed or intensified conflict, can have a confounding effect. Attribution challenges may be particularly high, especially where many different actors are simultaneously implementing a variety of programmes. In such contexts, it is important to obtain qualitative evidence from beneficiaries to understand the impact achieved for a given cost.

⁹⁷ In some humanitarian contexts, particularly in rapid onset crises, DFID recommends assessing speed, quality, and cost, in place of economy, efficiency, and effectiveness. However, in prolonged or recurrent crises, DFID generally recommends shifting back to the more “traditional” framework. See Humanitarian Value for Money Toolkit, May 2015. The latter is therefore considered more relevant here.

⁹⁸ DFID’s Approach to Value for Money (July 2011), at page 5.

⁹⁹ CHASE External reference for partners: DFID Value for Money in Humanitarian Programming, at page 2.

¹⁰⁰ DFID, Value for Money in Social Protection Systems, (November 2015), at page x.

¹⁰¹ DFID Humanitarian VfM Toolkit (2014), at pages 7–8.

While noting that shared MIS can provide VfM in a social protection context, DFID guidance on the topic notes that “key requisites are a supportive policy environment, an effective national ID system, sufficiently well-trained staff at all levels, sufficiently high capacity ICT and extensive internet coverage. Ensuring confidentiality of private information, data security and prevention of information abuse is unlikely to be cost-free but is fundamental to safeguarding dignity within the system.”¹⁰² All of these costs will need to be accounted for in a cost-effectiveness analysis of the use of interoperable MIS in protracted crises. Many of these pre-requisites will also be difficult to achieve in protracted crises and/or in FCAS.

Equity requires ensuring that benefits are distributed fairly and reach the most vulnerable and/or marginalised. This aligns with commitments to “leave no one behind”. Reaching these populations may involve higher unit costs, but principles of equity require that marginalised populations not be overlooked in the drive to keep costs down. To account for this, it is possible to weight benefits distributed to marginalised groups more heavily to account for these additional costs.¹⁰³

There is a potential value in leveraging shared data for increased coordination amongst social protection and humanitarian actors, leading to (according to key informants interviewed) reduced duplication of efforts, and potentially saving costs. Very few key informants, and almost none at field office level, raised other potential benefits like effectiveness or improved beneficiary experience. During country visits, beneficiary feedback on biometric registration (particularly fingerprint technology) and MIS centralisation/interoperability was generally negative. While noting that biometric registration avoided fears that stolen or lost registration cards would lead to a loss of benefits, those consulted suggested that the drawbacks outweighed these benefits. Concerns included difficulty scanning fingerprints and the time this takes (for more on this issue, see the section on Biometrics in Annex 1), inability to register all family members, errors in registration, and reduction of an already insufficient benefits package. These concerns were conflated with centralisation/interoperability, as the more visible component of this process – the need for biometric registration was explained to beneficiaries as a requirement to enable organisations to work together.

Where systems can speak to one another automatically, these efficiency gains may be valuable. However, initial data sharing such as that by WFP and IOM in South Sudan is done manually, leading to inefficiency and a human resource burden. Pelham et al. (2011) outline cost savings such as administrative costs of data collection, recurring costs of data management, and private costs to citizens.¹⁰⁴ The promise of de-duplication and resultant cost saving can be attractive for the client, making single or interoperable MIS or the use of biometrics an attractive sell for implementers. Indeed, the principal driver for increased interoperability or moves towards a single system, according to the vast majority of key informants interviewed (across both case studies, at HQ and field office, and among donors, implementing partners, and UN agencies) is that of efficiency, which key informants believed was most donor’s key concern.

For most key informants to this research, greater “efficiency” centred around reduced costs, and was often conflated with VfM. Other key components of VfM (notably equity) were often sidelined. Informants therefore focused on the prospects for de-duplication offered by greater interoperability and/or shared MIS accompanied by biometric registration. They noted, for example, up to a 20% reduction in caseload following biometric registration, which was alleged to be based on reduced duplication of beneficiaries across the organisation’s programmes, or programmes implemented by others with which the organisation was sharing information.

However, this reduction was acknowledged by several key informants from both donors and implementing partners to represent not only de-duplication, but also the inability to register those whose fingerprints could not be taken (due, for example, to extended periods of manual labour), those

¹⁰² DFID, *Value for Money in Social Protection Systems*, (November 2015), at page xi.

¹⁰³ ICAI, *DFID’s approach to value for money in programme and portfolio management: A performance review* (February 2018), at page 16.

¹⁰⁴ Barca, V and Beazley, R, *Building Government Systems for Shock Preparedness and Response: The Role of Social Assistance Data and Information Systems* (2019)

who were not present on registration day or could not travel to the registration point, or those who chose not to register for any other reason. No options are offered for those who are unable or unwilling to provide their biometric data, and no data are available regarding the proportion of the reduction in beneficiaries registered that is due to these other factors, rather than de-duplication. It is therefore difficult to assess VfM without this key piece of evidence. For more information on the challenges around the use of biometrics, and fingerprints in particular, see the section on Biometrics in Annex 1.

Nonetheless, particularly in humanitarian settings, decisions about where to direct scarce resources must be made despite the absence of perfect evidence. In such an assessment, it is important to consider qualitative as well as quantitative data to provide “the story behind the numbers”, contextualising the quantitative data measured against indicators, either allowing for triangulation or providing reasons to question assumptions based on numbers alone.¹⁰⁵ This should include beneficiary perceptions and experiences, for example. In a humanitarian setting, confidentiality and the ability to operate in conflict environments have also been noted as key drivers of VfM, even if they at times hinder humanitarian actors’ efforts to provide quantitative metrics that are easier to understand and compare.¹⁰⁶

In a conflict context and situations of acute need, it may be more appropriate to accept some amount of duplication rather than excluding an unknown number of eligible beneficiaries in a drive to increase economy by reducing costs. To gain a greater understanding of this trade-off, more information on exclusion due to factors beyond de-duplication is necessary. For example, if costs savings from “de-duplication” through biometric registration and interoperability/ single systems allow benefits to be distributed more evenly and to more beneficiaries (i.e. if savings are funnelled into expanded coverage, and/or if greater understanding of existing coverage is used to reduce exclusion), this may enhance the equity of an intervention. However, if marginalised groups are left out, such as those who are unable to provide fingerprints due to disability or a lifetime of physical labour, this runs contrary to the principles of equity.

In addition, as noted in Section 4.2.1, it is not clear that more even distribution of a benefit package that may be insufficient on its own will be more effective than overlapping provision of benefits to a smaller number of people, which may in combination be more effective (i.e. be more likely to sustain lives or improve livelihood outcomes). While more data on the occurrence and impact of overlapping benefit packages could improve understanding of the pros and cons (if the potential risks of greater data sharing outlined throughout this report are addressed), key informants interviewed advised that data is not currently used for this purpose. Where they identify “double-dipping”, which they consistently framed in the negative, they advised that they shifted their programming to avoid this, rather than investigating its impacts.

Every intervention has an opportunity cost – VfM analysis can support more effective decision-making in a context of high need and scarce resources. But fundamentally, we need to understand whose VfM we are talking about. This is not just about reaching as many people as possible as cheaply as possible or achieving the lowest possible cost per person, as suggested by most key stakeholders interviewed. It is about achieving real and lasting change for those who will most benefit from it, even if that costs more in the short term. It also requires ensuring that accountability to taxpayers in donor countries does not come at the expense of accountability to the people the humanitarian community is meant to work for – those in humanitarian need. Greater effectiveness and accountability to beneficiaries can be supported by greater transparency, improved accuracy in reporting, and a better understanding of impact, all of which can be supported by greater information sharing. However, this must not come at the expense of fundamental rights to privacy and data protection. To achieve these effectiveness and accountability goals, information sharing should focus on summary statistics (e.g. total spend on various types of aid, or geographic coverage where this does not pose risks to vulnerable, identifiable groups) rather than personal data, even if it is anonymised, due to risks around de-anonymisation (discussed above in section 4.2.7).

¹⁰⁵ OPM’s Approach to Assessing Value for Money (September 2018), at page 5.

¹⁰⁶ How to Define and Measure Value for Money in the Humanitarian Sector (SIDA, 2013).

4.4.2 Fiduciary responsibility

All types of management information systems have cost implications. In a single system, the burden for data protection and security is passed on to the central system holder. In fragmented (separate) systems, the costs are carried by each agency, some of whom may struggle under the burden (such as small NGOs). Separate but interoperable systems (i.e. federated or centralised) will have implications for each agency in rendering the systems interoperable, such as refining data. This still requires one organisation or agency to take responsibility for the management of the central data repository, including oversight, but allows a spread of costs with regards to data collection, data protection, hardware and software, and maintenance.

Cost burdens that apply to any MIS will be further enhanced when adding high-tech aspects, such as biometrics. Costs such as security, community sensitisation, and staff training will all be increased when introducing biometric technology, and there is little evidence in either the literature or fieldwork observations, that these outweigh the efficiency savings.

Several people interviewed by the research team, responsible for donor support to humanitarian and social protection responses at headquarters and in Yemen and South Sudan, indicated that they had limited knowledge of the data collected by the organisations delivering aid. For example, a donor to UN agencies indicated that they were not aware of the details of the current agreement around biometric data collection and sharing. Key informant interviews indicated that this lack of knowledge was attributable to a range of factors such as a lack of transparency (including limited information sharing between agencies and donors, and across agencies), insufficient internal technical expertise within organisations, limited resources (financial, human, etc, especially among smaller organisations), unclear allocation of responsibilities, and limited oversight.

This limited technical knowledge is particularly true with regards to the data protection policies and practices of humanitarian and social protection MIS – very few of those we interviewed, and none with a direct role in supporting or delivering humanitarian response in Yemen and South Sudan, were able to articulate either their organisations' or their grantees' approach to data protection.

For most, there is a pattern of delegating understanding and responsibility to their grantees, or assuming that senior leadership within the organisation are addressing/responsible for these issues. Others suggested that growing concerns about these issues within their organisations were not matched by additional resources – staff were instead expected to address this issue within existing (already stretched) resources, and without additional specialised, technical support. This disjunct means that when faced with demands or expectations that organisations share data to achieve organisational goals such as efficiency or fraud reduction, or to maintain specific standards around data protection, there is insufficient knowledge on which to base a robust discussion, or to steer organisations beyond their own self-interest.

This limited knowledge and access to information means that the lessons learned in other fields experiencing the digital revolution are not applied to the humanitarian sector. For example, Palantir, an American data company with a controversial data analytics contract with WFP,¹⁰⁷ has a record of working with public services such as policing and failing to protect sensitive data¹⁰⁸ and of working with intelligence and immigration enforcement agencies. More broadly, the controversy around SCL Group's claims of influencing public opinion and political will, including its subsidiary Cambridge Analytica's use of personal data in electoral and political processes in the UK and US, has been the subject of great attention and discussion. This includes recognition that large population data sets have not only planning and administrative value, but increasing commercial value. For example, a key informant advised that the OCHA data centre in the Hague has multiple large-scale downloads of data from US-based data farms, although these data sets do not appear to have a clear value for OCHA. Health data are of interest to a wide range of healthcare interests from regulatory bodies to insurance companies, who can use it to profile patients or potential clients.

¹⁰⁷ 'New UN Deal with Data Mining Firm Palantir Raises Protection Concerns'.

¹⁰⁸ 'How Palantir, Peter Thiel's Secretive Data Company, Pushed Its Way Into Policing | WIRED'.

This applies not just in conflict contexts but in wealthy countries – a risk identified in the handing over of UK National Health Service patient data to third party private companies.¹⁰⁹ In the health sector, concerns around the exploitation of sensitive personal information for commercial or other reasons has led to the development of recommendations for the effective governance of health data – notably the OECD's primary recommendations that national health data governance frameworks should be developed, and that frameworks should be harmonised between countries.¹¹⁰ Note that the recommendations emphasise governance frameworks, principles and standards over specific system and data sharing regimes.

While the health sector is often held up as an example for its perceived high standards of data protection compared to other sectors, cracks in this system have been demonstrated in the response to the COVID-19 outbreak. For example, reported data handovers by health authorities to private technology firms serve as an important reminder that even apparently robust systems, with a strong focus on protection, can falter in the face of crisis.

Without appropriate learning from other applications of identity and data management, further development of MIS in humanitarian and social protection work in fragile and conflict contexts risks further exclusion, marginalisation and political polarisation. The populations and kinds of data involved in humanitarian and social protection service provision in fragile states are vulnerable to exclusion in emerging identity and data management systems. In India for example, individuals with contested citizenship in Assam have been excluded from the national ID scheme (Aadhaar) and thus from accessing welfare provision.¹¹¹ Kenya's new national digital ID scheme the Huduma Namba has been linked to further exclusion of the already marginalised Nubian, Masai, Borana and other assimilated peoples.¹¹² The Kenyan High Court recently ruled that the scheme be suspended until adequate data protection measures are put in place.¹¹³

In another significant example, the District Court of The Hague in The Netherlands ordered the halt to a digital benefit fraud detection tool, claimed to reduce misuse of targeted vulnerable household social protection benefits. The System Risk Indication (SyRI) identifies specific individuals as more likely to commit benefit fraud and gives authorities wide-ranging powers to share and analyse data that was previously kept in separate "silos". SyRI employs a hidden algorithmic risk model and has been exclusively targeted at neighbourhoods with mostly low-income and minority residents. Entire poor neighbourhoods and their inhabitants were spied on digitally, without any concrete suspicion of individual wrongdoing.¹¹⁴

This limited understanding, compounded by the need for immediate action, limited resources and a growing number of experiences and challenges, suggests that the treatment of humanitarian and citizen's data in emergency contexts and in fragile states faces the same issues. Research conducted for DFID by Caribou Digital found that in many refugee response service providing organisations – both national and international NGOs – there was a high level of insecure data management practices such as the use of insecure platforms including Excel and Google Sheets, and data sharing without permission¹¹⁵. A similar case was also shared anecdotally in South Sudan, with reference to NGOs sharing personal data of beneficiaries by email.

¹⁰⁹ <https://www.wired.co.uk/article/google-apple-amazon-nhs-health-data>
<https://www.theguardian.com/commentisfree/2020/feb/03/longer-healthier-lives-privacy-technology-healthcare>

¹¹⁰ OECD, 2019, Recommendation of the Council on Health Data Governance, OECD/LEGAL/0433,
<https://www.oecd.org/health/health-systems/Recommendation-of-OECD-Council-on-Health-Data-Governance-Booklet.pdf>

¹¹¹ A new layer of exclusion? Assam, Aadhaar and the NRC (LSE Blog, September 2019)
<https://blogs.lse.ac.uk/southasia/2019/09/12/a-new-layer-of-exclusion-assam-aadhaar-and-the-nrc/>

¹¹² Waziri, Kedolwa. 'The Ones Who Are, But Don't Exist: Being Nubian, and Kenyan' (The Elephant, 5 July 2019),
<https://www.theelephant.info/reflections/2019/07/05/the-ones-who-are-but-dont-exist-being-nubian-and-kenyan/>

¹¹³ <https://www.bbc.co.uk/news/world-africa-51324954>

¹¹⁴ <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865>;
<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25522&LangID=E>

¹¹⁵ Caribou Digital, Identity at the Margins: refugee identity and data management, Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2018 <https://www.cariboudigital.net/wp-content/uploads/2020/03/Identity-At-The-Margins-Identification-Systems-for-Refugees.pdf>

4.4.3 Reputational damages

Using any MIS involves risks of data breaches such as hacking or data leaks. A breach could result in reputational damages and implications for user trust in the operator and any partners involved. The risk of such a breach and the implications of this on reputation increase as more organisations have access to the data, particularly in cases where third parties are controversial such as the WFP Palantir partnership.

Collection and management of personal data presents a risk, which increases as more data are collected and as more data management is centralised. Breaches of data protection are inevitable – it happens all the time. The hacking of Red Rose – a provider of a closed loop registration and transfer software used by a range of NGOs – carried out by a competitor as a “wake up call” is a notable example. A recent report in *The New Humanitarian* describes an unreported major breach of UN staff data in Geneva and Vienna in late 2019.¹¹⁶ This follows a critical internal audit of WFP SCOPE in late 2017.¹¹⁷ There are numerous other examples of data theft from banking, communications, healthcare sectors to name a few. Perpetrators range from commercial competitors to foreign governments. It is reasonable to suppose that vulnerable group data would be of potential interest in connection with, for example, commerce (spanning from consumer behaviour to the mining sector), security, migration, etc. A rigorous risk management approach is required for all aspects of MIS to identify major risks (see Annex 3) and ensure mitigation approaches are applied. Taking a precautionary approach, potentially the most effective way to minimise risk is to reduce the data that is collected and reduce the degree of centralised management.



Example: UN Cyber Attack

A cyber-attack in July 2019 on UN Networks in Geneva and Vienna compromised staff records, health insurance, and commercial contract data. The breach was not reported by the UN. The UN is often immune from domestic legal proceedings due to its diplomatic status (see section 4.3.2), and it is – unlike most US and European firms – under no legal obligation to report the breach to a regulator or the public. It is also not subject to Freedom of Information requests.¹¹⁸

Because of these trends and practices, regardless of the levels of risk mitigation, the inadvertent and deliberate leaking and sharing of personal and anonymised data must be considered inevitable. There is clearly a need for capacity, systems and standards that better support data protection, but the operating assumption must be that all collected data are likely to be exposed at some point.



The effectiveness of different types of systems with regards to response, targeting and sustainability.

Operational improvements are often stated as the key benefit of integrated or centralised MIS, following a growing trend in the humanitarian and development sectors for the superior competence, efficiency and sustainability of technologies.¹¹⁹ Leite et al (2017) state that approaches such as the Integrated Social

¹¹⁶ <https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack>

¹¹⁷ <http://www.thenewhumanitarian.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling>

¹¹⁸ <http://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack>

¹¹⁹ Bryant et al (2019), Ibid.

Protection Information Systems in Turkey and Chile serve as powerful tools for assessing demand for programmes, profiling needs of certain groups, monitoring and coordinating the supply of benefits and services, and assessing gaps and duplications. They state that fragmented systems can create duplications, inefficiencies, and wasted resources for providers, and reduce capacity in government due to high caseload burdens.¹²⁰

4.5.1 Improved information management

Single, centralised or federated data sets may provide more data for better identification of trends and of populations in need. Where data are held in separate and fragmented MIS, there is little opportunity to use these data to recognise trends for more effective planning and response. Barca and Beazely (2019) recognise that there is little evidence in the literature, but argue that using existing data, information systems, and capacity can positively affect both the predictability and sustainability of shock responses. Barca (2017) notes that if data are updated regularly, and systems can capture the dynamics around poverty, integrated systems may better serve those vulnerable to shocks. Larger datasets may also allow organisations to understand where individuals are receiving other benefits to better target or coordinate their response. However, this requires appropriate policies on responsiveness and continuous data updating.¹²¹

4.5.2 Efficiency and effectiveness in registration

Interoperable (federated, centralised) systems will need to align the data collected to ensure data can be translated by each MIS. This requirement of consistency in data collection means there may be more questions to be asked, to cover the needs of different organisations, and more data will need to be held (as discussed above in Section 4.2.4). This risks unnecessary collection of extra data to meet each organisation's anticipated need, particularly where one of the goals is to register each individual or household only once while enabling them to potentially access services from each organisation. This also requires a common ID, which itself requires a single registry – if you have one ID for multiple services, you ultimately must still have one database. This is addressed further in Annex 1, in the subsections on Introduction to MIS and Identity.

This is also likely to further slow down the registration process for individuals. Leite et al note that, for citizens, fragmented systems can be frustrating and costly as they need to go to multiple locations to apply for different benefits and services, often with multiple visits to the same location.¹²² However, the beneficiary interviews carried out for this report in South Sudan found that the vast majority did not mind being registered multiple times, even if this meant being asked the same questions multiple times. Their main concern was around the time involved in benefit distribution, which occurs much more frequently than (even duplicate) registration. Beneficiaries in the two Juba PoCs had observed that, following the new single registration process, distributions took longer due to the challenges and delays in scanning fingerprints at monthly distributions, which caused them more difficulties on a practical level than repeat registration.

4.5.3 Sustainability

As noted in the introduction to this section, there is an assumption that humanitarian MIS need to be designed to ensure their sustainability for potential ultimate transfer to government. For instance, research in Somalia claims that all humanitarian actors and donors should harmonise operations and cash transfer programme data systems to work towards a government-led integrated beneficiary registry.¹²³ However, the main issue here is not the type of system, but the data sharing understanding and consent between beneficiaries, organisations and government.

Assuming data sharing is fully consented, transfer to a government-led social protection system would be easiest if data are transferred from a single MIS, or from a centralised data warehouse. In the case of federated systems, on project close-down, the data would need to be centralised and handed to

¹²⁰ Leite, P. George, T. Sun, C. Jones, T. Lindert, J. *Social Registries for Social Assistance and Beyond: Guidance Note and Assessment Tool* Protection & Jobs no.1704 (July 2017)

¹²¹ Barca, V. *Integrating Data and Information Management for Social Protection: Social Registries and Integrated Beneficiary Registries* (2017)

¹²² Leite, P. George, T. Sun, C. Jones, T. Lindert, J. *Social Registries for Social Assistance and Beyond: Guidance Note and Assessment Tool* Protection & Jobs no.1704 (July 2017)

¹²³ Boniface, O. *Harmonising registrations and identification in emergencies in Somalia* (Development Initiatives, 2019)

government, assuming the MIS has unique identifiers. The future government system would require a unique identifier to recognise individual records, such as a unique ID number or biometric. Fragmented systems would render this transfer challenging, due to disparate datasets, the lengthy process of data translation, and the numerous data sharing agreements which would be required. However, such systems are preferable from a security perspective.

Alternatively, to better support governments in the transition to government-led social protection without the risks discussed above with onward data sharing, humanitarian and development actors should explore opportunities to share the technology infrastructure, human resource capacity, etc. with government, rather than the data itself, as part of this transition.

This even has the potential to improve the likelihood that rights to privacy and data protection will be safeguarded after humanitarian actors leave, by providing a system for domestic governments to populate (following their own data collection efforts) which includes principles of privacy by design from the outset and is tailored to local needs. For example, this could include some of the privacy by design features currently being explored by the World Bank for its South Sudan Safety Net Project (SSSNP),¹²⁴ which include:

1. Integrating standard and proven approaches for data protection as a default.
2. Implementing data minimisation and deletion policies (including deletion as a default after a certain time) and processing personal data in a distributed manner, such that personal data, biometric templates, and biometric images are always physically and logically separated from each other.
3. Utilising a tamper-proof and secure audit log of all transactions/activities to ensure user accountability, the possibility to reconstruct events and detect potential intrusions, and to identify any other problems.
4. Recognising the limited connectivity in South Sudan and ensuring that the design features it proposes will not be hindered by this (i.e. do not require a strong and consistent internet connection for key features to function).

To ensure sustainability, this approach will require working closely with national governments on system design, to ensure the systems are well suited to the local context and can smoothly transition to government ownership. Donors can then support the further use of these systems through TA to support data collection to populate these systems, and ongoing training and human resource support.

It is also essential that donors consider the local political economy, and in particular the strength of local rule of law, when designing and handing over systems, even if these are devoid of data. For example, the World Bank's digital ID approach has been criticised for potentially increasing information asymmetries, leading to (further) rent extraction and political exclusion, by assuming that the jurisdiction in question has a functioning rule of law.¹²⁵ Khan and Roy note evidence that:¹²⁶

1. Linking identities to tax, welfare and other databases can make informal businesses unviable as a result of "premature formalisation".
2. Access to identity data can help the powerful control opposition more easily or expropriate from particular groups more effectively, with "adverse impacts on political and economic inclusion."
3. "In the context of ethnic and religious conflicts and contestations over citizenship, digital identities can be used to deprive targeted groups of access to banking, public-sector jobs, land transactions and the operation of sim cards, allowing coercive repression for political ends that, in extreme cases, can facilitate ethnic cleansing at the push of a button."

The benefits and risks of proposed systems, and their impacts on these dynamics, must therefore be carefully considered, particularly where rule of law is weak, such as in FCAS.

¹²⁴ Michiel van der Veen, 'Options Paper for Biometric Data Security and Protection in the South Sudan Safety Net Project' (Version 1.0, 21 January 2019)

¹²⁵ Mushtaq Khan and Pallavi Roy, 'Digital identities: a political settlements analysis of asymmetric power and information' (SOAS, Working Paper 015, October 2019)

¹²⁶ Ibid. at page 7

4.5.4 Techno-solutionism and the role of technology

There is a global and cross-sectoral trend towards techno-solutionism: the view that technology will provide benefits and offer solutions to major problems. As asserted by Bryant et al (2019), this is found in the humanitarian sector just as it is elsewhere.¹²⁷ This often involves focusing on technology while avoiding solving longer-term and complex social, political and economic issues. Arguably, this may be the case in the drive towards single government-led social protection systems, and the use of technology to create a firewall between the government and the data.¹²⁸ Technology is bridging the trust gap between humanitarian ownership of data and transition to a government-run system. In some cases, the technology may be trusted over the individual e.g. in Mauritania refugees were denied access due to biometric system errors, but their status was questioned before the technology was.¹²⁹

It may be argued that agencies are embracing new technologies to appear to be at the cutting edge. Globally we are seeing the implementation of frontier technologies: biometrics are used as the basis for ID in many cash transfer and social protection MIS, and the UN's Blockchain-based Building Blocks initiative seeks to be the meta-platform that connects the various elements of the humanitarian ecosystem. Whilst piloting new solutions is inevitable and helpful to test use cases, the humanitarian sector meets people at their most vulnerable, and so the testing of these products here is ethically questionable. Indeed, attention to the rollout of blockchain for digital identification of the Rohingya community has been largely critical due to the sensitivity of their identity.¹³⁰

However, there are emerging technologies and innovations that may have the potential to achieve the benefits of linked systems and data whilst mitigating the risks. Organisations such as ICRC and Mastercard are exploring approaches that create algorithmically generated encrypted 'hashes'¹³¹ of biometric data – in other words, encrypted representations of personal data are used as proxies for the actual data, with the encryption algorithm being the proprietary technology that ensures data protection and security. Authentication and verification would be carried out by comparing the hashes, not the actual data – using a proprietary algorithm to match the hash presented by the beneficiary against the hash held by the organisation.

Simpler cryptographic innovations include the further use of privacy techniques such as 'Zero Knowledge Proofs' (ZKPs). Zero-knowledge techniques are mathematical methods used to verify things without sharing or revealing underlying data¹³² – for example, an individual's entitlement to a service could be verified without having to reveal any further personal information, or a data holder could confirm a subject is over a certain age without revealing the actual age. Mastercard has proposed an identity platform based on such techniques, but there remain many questions about its application in practice.¹³³ However, one of the biggest challenges to cryptographic based approaches to data protection and identity management is the strength of the encryption, for instance a design flaw may make it easier for a hacker to reverse-engineer a hash to access the original data. The rapid development of technologies such as quantum computing threaten cryptographic based security technologies.¹³⁴

These considerations have implications for the suitability of humanitarian agency/development actor MIS and identity management systems for transfer to government systems. While new technologies may provide safer avenues for data sharing, or allow for concentration of more data in a single system, similar advances may be made by those seeking to break encryptions and hack into systems. In short, these considerations point towards limited possibility or suitability for increased concentration of data in single systems and/or interoperability of MIS and related data sharing, either within the humanitarian sector or between the humanitarian sector, development actors, and state systems.

¹²⁷ Bryant, J. Willitts-King, B. and Holloway, K. *The Humanitarian Digital Divide* (2019)

¹²⁸ See, for example, the former World Bank Safety Net and Skills Development Project in South Sudan

¹²⁹ Bryant et al, *ibid*.

¹³⁰ <https://www.ictworks.org/blockchain-digital-identity-cards-rohingya-refugees/>

¹³¹ A hash converts one value to another, for instance a person's name becomes an identifying number

¹³² 'What Are Zero-Knowledge Proofs?' *Wired*. Accessed 19 January 2020. <https://www.wired.com/story/zero-knowledge-proofs/>

¹³³ 'Mastercard Wades Into Murky Waters With Its New Digital ID'. *Wired*. Accessed 19 January 2020, <https://www.wired.com/story/mastercard-digital-id/>

¹³⁴ 'How a Quantum Computer Could Break 2048-Bit RSA Encryption in 8 Hours'. MIT Technology Review. Accessed 19 January 2020, <https://www.technologyreview.com/s/613596/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/>

This is both a technical and a principle issue. At a technical level, the information that humanitarian and state systems collect is often different, even while there may be overlaps. For example:

- Vulnerable groups are only part of a greater population. Data collected is determined by the agency managing the project, which can be different from criteria chosen by another agency or government authority, due to different definitions and different programme approaches. For example, a food distribution requires different data to a maternal support transfer.
- Different transfer modalities (e.g. food, cash and vouchers) may require different data. Cash transfers require detailed data (generally including bank/mobile money account numbers, official ID numbers, and other personal details required to set up a bank account) on individual recipients to manage Know Your Customer (KYC) due diligence.
- Vulnerability data for, say, a household food consumption transfer will be different from conditional maternal healthcare support. These data are also likely to be stored in different systems with no built-in mechanism for interoperability.

Although there are some existing community standards to support interoperability at this level, such as the Humanitarian Exchange Layer (HXL), these have not been embraced sector wide.¹³⁵ Moreover, vulnerability during the early stages of a humanitarian crisis may involve different priorities than those in protracted humanitarian/development crises or in the transition to later developmental phases. In addition, information is often stored in ways that fails to support data sharing.

While donors and humanitarian and development actors can seek to align data collection, this does risk increasing the amount of data collected. If each entity pushes for the continued collection of the types of data it has always collected, and is unwilling to compromise, the end result could be increased data collection overall (as outlined in Section 4.2.4, above). Such efforts to align data collection while ensuring data minimisation is achieved will require entities collecting and using this data to forgo some of the data types they usually collect to reach agreement on a data set that worked for everyone without continuously expanding. There are likely to be political barriers to reaching this level of compromise.

Based on principle, there are also good reasons not to pursue greater system integration. There have been a number of publicly reported data hacks, privacy breaches or identified vulnerabilities¹³⁶ – and there must be the presumption that there are many that remain unreported. Where consent is relied on as a legal basis (see below), it can also be more challenging to gain truly *informed* consent where significant data sharing and/or integration are envisioned. For example, what if some beneficiaries consent to data sharing with other entities, while others do not, instead opting to only share their data with only one or some entities? Does it help to share these potentially incomplete data sets, or does it generate more confusion? A fully integrated system could even make it impossible to offer this level of choice to beneficiaries, limiting the likelihood that consent is truly freely given.

Instead of system integration, an approach that emphasises specific standards around data collection and identity management would enable data sharing and system interaction that meets data protection, privacy and protection requirements. As discussed below, rather than focusing on ways to share data with governments in particular, donors should consider supporting nascent government-led social protection systems through the development of systems that meet these requirements, which can then be handed over to governments to populate with data they collect.

¹³⁵ These are established standards to indicate that columns containing data such as names are equivalent.

¹³⁶ An *internal audit* of WFP's beneficiary management, dated November 2017, found a litany of data protection failings across the UN agency's digital and paper-based systems. *New Humanitarian – January 2018 – EXCLUSIVE: Audit exposes UN food agency's poor data-handling* <http://www.thenewhumanitarian.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling>

5 RECOMMENDATIONS AND WAYS FORWARD

As noted throughout this research, the implications of type of MIS and levels of interoperability are not only a consequence of the technology in and of itself. In this section, we outline recommendations and ways forward related to different models of linking MIS, not only through the technology, but also ways of working and frameworks within which to work which protect individuals, whilst reaping benefits of increased data sharing.

5.1 Integration and interoperability

Greater collaboration and data sharing within the humanitarian sector should be supported, but through standardisation (interoperability of secure MIS) rather than a single system (e.g. integration of existing MIS or creation of a new single system). Enabling multiple different systems to interact can help deliver efficiencies, but it is neither realistic nor desirable (due to the significant risks outlined above) to achieve this through the copying of data into one single system. Whether greater collaboration and data sharing with the domestic government is possible will depend on local factors, including the extent of respect for rule of law, whether the government is a party to the conflict, and government capacity. This will need to be assessed on a case by case basis.

Rather than efforts to standardise data collection, categorisation and management, interoperability would enable different systems to 'read' each other – for instance in a federated structure (see Annex 1 on types of MIS). Examples of standards for data exchange include the Humanitarian Exchange Language (HXL)¹³⁷, a simple addition to excel based data storage and management which allows for interoperability across data sources. Interoperability should also be based on data sharing minimisation – for example through further use of 'zero knowledge proofs'¹³⁸ – verifying claims without sharing data.

Interoperability should also be furthered through opening 'closed' systems, such as SCOPE, ProGres, PRIMERO and BRAVE, using APIs to enable third parties to unlock data monopolies and enabling the development of further services.

At the same time, to minimise protection risks of greater interoperability, data sharing should be governed by strict, auditable and accountable compliance with data protection regulation (see below).

5.2 Conceptual framework – digital dignity

The design and application of MIS should be guided by the concept of digital dignity. This issue is particularly prevalent where data are being shared amongst organisations or MIS are made interoperable. Individuals need to be respected as a data agent, and not purely as a data subject, in the way data are governed, to ensure that data governance aligns with core humanitarian and development principles. The promotion of digital dignity relies on the adoption of appropriate data protection standards and digital do no harm standards and protocols.¹³⁹

To ensure data and vulnerable group protection standards are upheld, both within a humanitarian context and for government-led social protection systems, digital dignity provides a framework that is aligned to existing guidance on aid delivery, including:

¹³⁷ <https://hxlstandard.org/>, currently used by organisations such as UNHCR, IOM

¹³⁸ Zero knowledge proofs are a method by which one party can prove to another party that they know a value x, without conveying any information apart from the fact that they know the value. For instance, Organisation A could state they have Beneficiary A in their system, without sharing the details of that Beneficiary with Organisations B

¹³⁹ Digital Dignity in Practice: Existing Digital Dignity Standards, Pursuing Digital Dignity and Current Gaps in Digital Dignity

- Data protection (considering vulnerability context and risk of unauthorised access and unintended use of data);
- Value for Money (considering measures beyond Efficiency in systems design, including a focus on Effectiveness and Equity);
- Do No Harm (considering the implications and risks of civilian protection) and
- Leave No-One behind (considering inclusiveness of transfer modalities, targeting approaches).

5.3 Data protection standards

Policies and reporting should be aligned to an agreed sector specific international data protection regime, before data are shared or MIS made interoperable. This will ensure all involved in data sharing are committed to the same principles. Alignment with the EU GDPR standard is highly desirable (particularly in the absence of robust domestic legal and regulatory frameworks) given its already wide adoption, including by donors and aid agencies headquartered in the EU, for internal purposes if not yet for data held on transfer recipients outside the EU. This would include standards on:

- Revisiting the basis for data collection, and seeking (renewed) consent where required, according to changing circumstances (governance, security, need, etc.) or change of use (providing other services, collaboration with other organisations and authorities).
- Ability of those registered to enquire on full data held.
- Ability for individuals to request changes, updates and delete data held on them.
- Explanation provided to individuals of which parties have access to this data (and renewed explanation if access for new parties is considered).
- Avoidance of catch-all terms such as asking permission to share data “with all parties as decided by the registrar”.
- Data collected is relevant to the immediate requirements of the good or service being provided and avoid collecting additional data that “might be useful in future”.
- Timebound data retention periods and safe data deletion procedures.
- Data managers should adopt a risk-based management approach to data management, according to context, including oversight of role played by third party data processors.

5.4 Ways of working

Donor/aid agencies should develop a global multi-disciplinary community of practice on management information systems interoperability, including humanitarian and development perspectives, spanning from aid policy to legal, protection and safeguarding, and IT expertise.

The key task of the above body should be to create or appoint an independent international body to inform, facilitate, convene, assess, compare and report on data management in MIS and data registries, guided by the principles and frameworks set out above. Its main output would be the creation and oversight of a data protection standard suitable for application in FCAS. Examples of this approach, in the field of international development assistance, already exist, such as the Independent Aid Transparency Initiative (IATI), and the Social Protection Inter-Agency Cooperation Board (SPIAC-B)¹⁴⁰

¹⁴⁰ <https://socialprotection.org/institutions/social-protection-inter-agency-cooperation-board-spiac-b>

and Interagency Social Protection Assessments (ISPA¹⁴¹). MIS might even be an appropriate topic as an extension to this already established organisation. The UK's Independent Commission on Aid Impact (ICAI) and equivalents in other bilateral donor countries examine international development topics on an *ad hoc* basis; improved compliance and alignment with data protection standards requires a more consistent longer-term approach.

Country level agency staff in donor and UN missions involved in aspects of direct aid provision, both independent humanitarian aid and those working to support country systems, need to be aware of the range of wider policy implications of personal data management, and the constraints on consolidating datasets.

5.5 Options for implementation

The MIS data protection standard could be implemented in two ways. The first is through collective legal and contractual enforcement of a common approach by all major donors i.e. obligations being included in contracts or grant agreements issued. Alternatively, an aspirational voluntary code of practice could be developed which implementers are encouraged to meet (in part through appropriate donor funding reward or penalty). This could come and/or from a voluntary scheme which sets a standard and encourages aid agencies to meet it.

5.6 Compliance – legal and contractual route

Donor agencies should consider insisting on compliance with data protection standards in contracts and grant agreements issued to NGOs, UN and other private sector suppliers. Specifically, donor agencies should require proposals to articulate data protection measures, comparison to the agreed adopted standard, including how any gaps are to be addressed, and an assessment of data protection measures in monitoring and evaluation of all projects. Domestic legal frameworks for privacy and data protection should be the first consideration here. However, where these are lacking, GDPR can provide a 'gold standard' benchmark. Key factors donors should consider will include, as a minimum:

1. The extent to which privacy and user-centred design have been incorporated from the outset, including working with data subjects to ensure the proposed system meets their needs. This should include political economy analysis to understand both current issues, and the potential for the proposed approach to either address or exacerbate these issues.
2. Requirements to conduct DPIA at the start of and throughout the lifetime of the project, and to ensure recommendations for improvement arising from DPIA are implemented.
3. A clearly defined legal basis for data collection, and where this is consent, ensuring that it is freely given, specific, informed and unambiguous.
4. Policies and plans in place regarding data sharing, breaches, and data deletion at end of use.

This could be partially achieved done though individual donors introducing conditions on a donor by donor basis. Such conditions could be supported through a joint agreement and adoption by several global donor governments. Agreement of the World Bank would be particularly relevant given its support to developing national systems in transition countries, and its clients including host governments and (increasingly in the light of IDA18 and the Famine Action Mechanism, FAM) UN agencies. Enforcement of data protection standards by donor organisations worldwide could facilitate near universal adoption. As a starting point, the World Bank ID4D programme's 'Principles on Identification for Development'¹⁴² – endorsed by the UN – provide a foundation but require more detailed specification for application. For example, as discussed above, the World Bank's digital ID approach has

¹⁴¹ <https://ispatools.org/>

¹⁴² The World Bank's Identification for Development (ID4D) programme developed the Principles on Identification for Sustainable Development which cover specific points across themes of Inclusion, Design and Governance, and have been endorsed by more than 20 organisations including United Nations, multi-lateral and private sector organisations. DFID has in the past considered joining.

been criticised for potentially increasing information asymmetries, leading to (further) rent extraction and political exclusion, by assuming that the jurisdiction in question has a functioning rule of law.¹⁴³

Data protection standards need to be referred to in bilateral cooperation agreements between UN agencies, donor countries and recipient country governments, where these exist. It is possible that where national data protection laws, regulations and policy exist, the international standard might contradict the national standard. In this case the prevailing legal obligation of entities needs to be agreed in advance, along the lines of the exchange of letters between the United Nations Under-Secretary-General for Legal Affairs and the EU delegation to the United Nations regarding the applicability of GDPR.¹⁴⁴ When addressing any conflict between domestic and international law, an approach that focuses on the fundamental rights underlying the need for data protection, rather than a narrow focus on technical compatibility between the potentially conflicting legal systems, is desirable.¹⁴⁵

5.7 Compliance – voluntary route

Donors and aid agencies involved in the registration, management and storage of beneficiary data should be required to publish clear and specific data protection policies, including reporting on the implementation of these policies and how shortfalls are being addressed. Examples of voluntary industry approaches to meeting standards include SPHERE standards¹⁴⁶, and the Donor Committee for Enterprise Development (DCED) standard for Making Market systems work for the Poor (M4P)¹⁴⁷.

Aid agencies developing and operating MIS are urged to agree a common standard for protection of data held on vulnerable groups. Agencies should report back regularly on their compliance to this common standard at country and global levels.

5.8 Supporting transition to government systems

Donor support to strengthen state social protection systems should take a holistic, ‘ecosystem’ approach. This should include providing more assistance to the centralised national functions needed to establish a government-led social protection system, e.g. statistics, civil registry, identity, rather than only for social transfers through parallel projects. Restrictions on support for government authorities might be re-considered (or re-configured whereby this support is channelled through a UN body) to maintain a minimum level of common resource and functionality. In such instances the aim is to create and adopt one system for common collaborative use, and future adoption by government.

As noted above, donor-funded systems can entrench or exacerbate existing power imbalances, or can reduce these while increasing protection of rights to privacy and data protection. Even where data cannot or should not be shared with domestic governments due to the concerns outlined above, systems and best practice standards can be. By sharing technology infrastructure, human resource capacity, etc with government, and not necessarily data itself, as part of a transition, humanitarian/development actors can include principles of privacy by design and rights protection from the outset, in a manner that is tailored to local needs.

To ensure sustainability, this approach will require working closely with national governments on system design to ensure a smooth transition to government ownership. Donors can then support ongoing use of these systems through TA to support data collection to populate these systems, and

¹⁴³ Mushtaq Khan and Pallavi Roy, ‘Digital identities: a political settlements analysis of asymmetric power and information’ (SOAS, Working Paper 015, October 2019).

¹⁴⁴ Kuner, C. ‘International Organizations and the EU General Data Protection Regulation’, *International Organizations Law Review* 16 (2019) 158–191, at 165

¹⁴⁵ See, for example, *NJCMcs/De Staat der Nederlanden (NJCM vs the Netherlands)*, also known as the “SyRI case”, in which the court’s ruling was largely based on fundamental human rights as outlined in the European Convention on Human Rights, rather than technical compliance with GDPR.

¹⁴⁶ <https://spherestandards.org/>

¹⁴⁷ <https://www.enterprise-development.org/>

ongoing training and human resource support to ensure that developments in best practice are incorporated into these systems, and that high protection standards are maintained.

5.9 Biometrics

Biometric data are recognised as being particularly powerful and driving system efficiencies – for example, in ensuring de-duplication of access to transfers. There is a significant trend towards its use, in many cases without due consideration for the implications. Due to their immutability and uniqueness (see Annex 1), biometrics raise considerable safe data storage risks and require commensurate risk management measures. GDPR categorises biometric data in a special category, leading to stricter guidelines on storage and sharing, so adherence to this or GDPR-like protocols will help assure the security of this data. Organisations such as ICRC have excellent biometric data protocols.

It is also important for donors and implementers to note that their choices regarding biometric data use may become embedded in future government-led social protection, either where donor-funded systems are handed over (as discussed above), or because approaches used in protracted crises become the norm and are expected of future systems. If humanitarian and development actors chose to utilise biometric data, they must ensure that their choice of biometric data is appropriate and that essential safeguards are in place. See Annex 1: Biometrics.

5.10 Basis for data processing

Where consent is relied on as the legal basis for data processing, greater efforts by aid agencies to obtain informed, unambiguous, and freely given consent are needed. The degree of consent required, sought and provided to those registered on MIS is by and large inversely proportional to humanitarian need, potentially allowing for (or even requiring) other legal bases for data processing to be relied on (see Basis for Data Processing above, and Consent, in Annex 1). However, when using data for other purposes in the future, this should not be an excuse to deprioritise consent as a fundamental right of those registered – consent should be gathered for every intended use where it will be relied on as a legal basis for data processing. Where intended future use of data is unclear (for example, in FCAS where there is little clarity regarding the future shape and composition of the domestic government) it will likely be inappropriate to rely on consent as a legal basis for onward data sharing and processing. Data subjects cannot be expected to provide truly informed consent for these ambiguous intended uses.

When a sudden onset emergency becomes protracted, and government authority is eventually re-established, increasing clarity on who potentially can access and how the data might be used should be provided to those registered, along with an opportunity to withdraw consent if desired. This is due to both the change of use and the increased likelihood that the aid is no longer immediately lifesaving and of such urgency that another legal basis besides consent must be relied upon. While data registered in many humanitarian contexts (including but not solely those defined as Humanitarian System-Wide Scale-Up Activation Responses), rely on other legal bases for collecting data, such as vital interest or important grounds of public interest, it should not be assumed that this legal basis applies to non-essential onward use of this data.

For example, it cannot be assumed to be in the “interests of the beneficiary” to share or merge datasets, just because it makes sense to the project manager and the ultimate donor. Where consent is relied on as the legal basis for this sharing or merging, the change in use that requires re-gathering of consent includes a change in data processor, data system and/or purpose of data use. In essence, it is important to consider whether the legal basis under which the data was collected still applies. If this was vital interest, for example, is it in the beneficiary’s vital interest for this data to be shared? Is it the only way for them to access lifesaving aid? If consent was relied on as the legal basis for the initial data collection, did the beneficiary understand that such onward sharing was likely, and unambiguously consent to it?

If and when conditions are conducive for the creation of government-lead MIS, informed consent must be obtained afresh (or potentially for the first time, depending on the circumstances surrounding initial data collection) from those registered during a crisis. This implies that data previously collected by an independent agency (UN, NGO, private sector supplier) under a different legal basis should not be accessible to a government authority.

Data required by government should be collected afresh, with the intended use of this data clearly explained by government representatives when seeking voluntary consent. This also helps to ensure data is up to date, as key data points may have changed since the time of collection by another agency. It can also support data minimisation efforts, by encouraging government representatives to only collect the data needed for their programme, rather than having access to all types of data collected by other actors, regardless of its relevance to current needs. Where more than one organisation is considering collaboration, unless data are registered based on this joint purpose, and this is explained to those registered, consent and data registration would need to be re-captured. For more on consent, see Annex 1.

5.11 Risk management

Donors and aid agencies should introduce data risk assessments and response plans as standard to all MIS activities. A standard, structured Data Protection Impact Assessment approach should be developed and undertaken for the humanitarian contexts, including consideration of risks to civilian protection. During transition, donors and aid agencies should encourage domestic governments to take up similar approaches, and should support their efforts to do so as outlined above.

5.12 Contextualising the recommendations – application in Yemen and South Sudan

This section provides examples of how these recommendations can be applied in practice, by reference to the two case study countries – Yemen and South Sudan. It provides concrete examples of how these recommendations can be implemented in these two (and similar) contexts.

- In the design of any future MIS, beneficiary experience should be placed at the centre of design consideration, rather than the benefits for the agency / donors. This means prioritising digital dignity and protection, and recognising that these are not necessarily in opposition with, and can enhance, efforts to achieve value for money (particularly key VfM components like equity and effectiveness). This could include, for example, co-designing future state led (or quasi-state led) social protection systems with beneficiaries in countries like South Sudan where these currently do not exist, or involving beneficiaries in improvements to existing systems like SWF and SFD in Yemen.
- Agencies and donors should consider broader measures of quality of transfer systems. While variation in perspective is evident between, and even within, organisations, currently, there is a strong focus on efficiency and value for money among many of the donors and the vast majority of implementers interviewed, but a lack of consideration around effectiveness, economy, and importantly equity, which includes gender, safeguarding, inclusion and conflict sensitivity considerations. This will require moving beyond the observed drive for more quantifiable metrics from a *perceived* imperative to collect, retain, and share more and more personal data, to a deeper understanding of impacts on beneficiaries at a personal level. Gathering this qualitative data will be difficult in countries like South Sudan and Yemen where access can be challenging. Findings from discussions with beneficiaries in areas with greater access may need to be extrapolated to others until access is restored.
- The assumption that datasets held by separate organisations can / should be merged does not hold. Donors and organisations should take care to consider the implications of data sharing, look closely at any consent taken, and where possible make a data protection impact assessment on the potential sharing of this data. Where it is deemed necessary, donors and organisations should garner advice on how to share data securely and ensure that data sharing agreements are in place covering proportionality, further process, and limiting further sharing. This will be particularly important in

the nearly 30 per cent of nations which have no data protection law¹⁴⁸, and countries where data protection policies are limited and enforcement is not consistent. Where domestic frameworks are lacking, protections in data sharing agreements can fill gaps.

- Transition to government single / social registries would require fresh collection of registration data, or gaining/renewing consent for this new data use. In fragile and conflict-affected environments, it may not be appropriate to assume that data can be shared with government, particularly where they may play an active role in the conflict and/or are targeting certain portions of the population. In the face of these significant issues, it is not appropriate to assume a transition based on data sharing is in the best interest of beneficiaries.
- As a means to support the ultimate development of a government-led social protection system, donors could consider supporting governments to develop institutional capacity to collect and manage data (for instance building civil registration capacity); and supporting government to develop a comprehensive national data protection law & policy, and agreement on data management between development partners and government authorities (where feasible). This will need to include development of a legal framework from scratch in South Sudan, and from a very limited starting point in Yemen.
- End the vision of a single management dashboard for all social transfers and referrals. Despite several respondents interviewed for this study stating an interest in a single, unified system, if pushing towards greater interoperability, country offices should step back and consider the type of interoperability required, for what purpose, and how risks might be mitigated and data collection minimised. In the more immediate term, for further information, the Risk Table in Annex 3 provides a useful starting point, as does the ICRC Data Protection Handbook (the key points of both have been outlined above). Country context must be carefully considered, particularly the role of government and its access to data.

¹⁴⁸ https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

6 REFERENCES

The below table is drawn from the criteria outlined in DFID's How to Note: Assessing the Strength of Evidence (March 2014). Note that this table does not include primary materials reviewed, such as programme documentation, surveys, and other sources of statistics. It also does not include news articles referenced.

| Citation | Research Type and Design | Context | Topic | Study Quality |
|--|--|---|--|---------------|
| ACAPS, <i>South Sudan Analysis Ecosystem</i> (Thematic report, March 2020) | Primary (interviews and data collection) | South Sudan | Mapped the information landscape in South Sudan to identify information gaps and needs, as well as good practices in data collection and analysis. | High |
| ACAPS, <i>Yemen Analysis Ecosystem</i> (Thematic report, April 2019) | Primary (interviews and data collection) | Yemen | Mapped the information landscape in Yemen to identify information gaps and needs, as well as good practices in data collection and analysis. | High |
| Alston, P. <i>Report of the Special Rapporteur on extreme poverty and human rights: Digital technology and the welfare state</i> (UNGA, A/74/493, 11 October 2019) | Secondary (other review) | Global | Impact of digital technology use on human rights of the poorest in welfare states, based on case studies and literature | High |
| Baker, S. and Rahman, Z. <i>Understanding the Lived Effects of Digital ID</i> (The Engine Room, January 2020) | Primary (reporting of quantitative and qualitative research) | Case studies on Bangladesh, Ethiopia, Nigeria, Zimbabwe, Thailand | Documents many of the lived effects of digital ID systems from design to roll-out among mostly marginalised communities. | High |
| Barca, V. <i>Integrating Data and Information Management for Social Protection: Social Registries and Integrated Beneficiary Registries</i> (2017) | Secondary (other review) | Global | Literature review on best practice in harmonising MIS in social protection, providing practical policy guidance. | High |
| Barca, V and Beazley, R. <i>Building Government Systems for Shock Preparedness and Response: The Role of Social Assistance</i> | Secondary (other review) | Global | Draws on international experience to analyse the specific role of social assistance data and broader | High |

| | | | | |
|---|--|---|--|------|
| <i>Data and Information Systems</i> (2019) | | | information systems and capabilities. | |
| Barca, V. & Chirchir, R., <i>Building an integrated and digital social protection information system</i> , GIZ and DFID, October 2019 and February 2020 (full technical paper) | Secondary (other review) | Global | Reasons for, components of, challenges, and risks in developing digital and integrated information system is a crucial step in building a national social protection system. | High |
| Barca, V and O'Brien, C. <i>Factors affecting the usefulness of existing social protection databases in disaster preparedness and response</i> (Policy Brief: Shock Responsive Social Protection Research – December 2017). | Secondary (other review) | Global (case studies Lesotho, Mali, Mozambique, Pakistan and the Philippines) | Policy brief on the characteristics of existing social protection databases that enhance or limit their potential use in emergencies. | High |
| Beduschi, A. <i>Digital Identity: Contemporary challenges for data protection, privacy and non-discrimination rights</i> . Big Data & Society (SAGE) (2019) | Secondary (other review) | Global | Review of the impact of digital identity technologies on the protection of human rights, in light of international human rights law and GDPR. | High |
| Berg, M. & Seferis, L. 'Protection Outcomes in Cash Based Interventions: A Literature Review' (January 2015) | Secondary (literature review) | Global | Examines existing research to determine whether the use of cash and vouchers is contributing to the promotion of protection and gender outcomes for beneficiary communities. | High |
| Berthaut, A. et al. 'Cash Digitization: UN Collaboration, Coordination, and Harmonization Opportunities' (December 2018) | Secondary (other review) | Global | Identifies short-, medium-, and longer-term actions to improve collaboration in the delivery of CBTs in humanitarian contexts, including through digital payment solutions. | High |
| Boniface, O. <i>Harmonising registrations and identification in emergencies in Somalia</i> (Development Initiatives, 2019) | Primary (research in Somalia) and secondary (other review) | Somalia | Overview of MIS in Somalia and assessment of the levels of interoperability. | High |

| | | | | |
|--|--|--|---|--------|
| Bryant, J. Willitts-King, B. and Holloway, K. <i>The Humanitarian Digital Divide</i> (2019) (Humanitarian Policy Group) | Secondary (other review) | Global | A literature review of the adoption of technologies on furthering or limiting inclusion. | High |
| Cash Learning Partnership (CaLP) and Inter-Agency Research and Analysis Network (IARAN), <i>The Future of Financial Assistance: An Outlook to 2030</i> , (November 2019) | Secondary (other review) | Global | Mapping of the architecture of the global financial assistance and project to 2030 using IARAN scenario toolkit. | High |
| Clark, J (ID4D), <i>The State of Identification Systems in Africa</i> , World Bank Group (2017) | Primary (data collection and analysis) Secondary (other review) | Africa | Synthesis of findings from Identity Management System Analyses across Africa and conclusions on the state of ID systems. | High |
| Cliem, N. and McKenzie, A.M. 'Digital Dignity in armed conflict: a roadmap for principled humanitarian action in the age of digital transformation' (Wilton Park, 2019) | Primary (report on event and key findings) | Global | The Wilton Park conference was convened to interrogate the implications of digital transformations in humanitarian action in armed conflict and other situations of violence and explore the notion of digital dignity. | High |
| Cliem, N. and McKenzie, A.M. 'Digital Dignity in Practice: Existing Digital Dignity Standards, Pursuing Digital Dignity and Current Gaps in Digital Dignity' (Wilton Park, 2019) | Secondary (other review) | Global | Review of standards and best practices for digital dignity in humanitarian contexts. | High |
| Collins, H. 'Is Open Source Software More Secure than Proprietary Products?' (Government Technology, 30 July 2009) | Primary (interviews) and Secondary (other review) | Global | Comparison of security levels in proprietary and open source software. | Medium |
| Cooper, R. (2018). Social safety nets in fragile and conflict-affected states. K4D Helpdesk Report. Institute of Development Studies | Secondary (other review – case studies and literature) | Global, with case study on Afghanistan, Iraq, Mali, South Sudan, Sudan, Syria, and Yemen | Review of evidence on social safety nets working in fragile and conflict-affected states, and how have they been supported by national governments and the international community. | High |

| | | | | |
|---|--|--|--|------|
| Devereux, S. and Vincent, K. "Using Technology to Deliver Social Protection: Exploring Opportunities and Risks." <i>Development in Practice</i> , vol. 20, no. 3, (2010), p 374. JSTOR | Secondary (other review) | Southern Africa | Uses examples from Southern Africa to provide a review of the risks and benefits of using technology to deliver social protection. | High |
| European Commission (February 2019) 'Social Protection across the Humanitarian-Development Nexus: A Game Changer in Supporting People through Crises' <i>Tools and Methods Series: Reference Document No 26</i> | Secondary (other review) | Global | Reference document aimed at developing a common 'Guidance Package' on Social Protection across the Humanitarian-Development Nexus. | High |
| Gentilini, U. Laughton, S. and O'Brien, C. <i>Humanitarian Capital? Lessons on Better Connecting Humanitarian Assistance and Social Protection</i> Social Protection & Jobs no. 1802 (November 2018) | Secondary (other review) | Global | Summary of findings from 12 country case studies exploring the linkages between humanitarian assistance and social protection systems. | High |
| GSMA, The Mobile Economy of Sub-Saharan Africa, 2017 | Primary (data collection and analysis) Secondary (other review) | Sub-Saharan Africa | GSMA Intelligence data from global mobile network operators and analysis gives a summary of the mobile economy of the region. | |
| Herschel, R & Miori, V. <i>Ethics & Big Data</i> . Technology in Society 49 (2017). | Secondary (other review) | Global | Assessing impact of big data in light of ethical theories. | High |
| ICRC 'Handbook on Data Protection in Humanitarian Action' (July 2017) | Primary (guidelines) Secondary (other review) | Global | Review of the legal framework surrounding data protection in a humanitarian setting, along with organisational guidelines | High |
| Idris, I. (2019). Linking social protection and humanitarian response: Best practice. K4D Helpdesk Report 684. Institute of Development Studies. | Secondary (other review – case studies and literature) | Global, with case studies on Turkey, Lebanon, and Cameroon | Reviews alignment of humanitarian response in refugee crises with national social protection systems. | High |

| | | | | |
|---|---|---|--|------|
| Internet Society and the Commission of the African Union <i>Personal Data Protection Guidelines for Africa</i> (9 May 2018) | Secondary (other review) | African Union member states | Review of current initiatives and global best practice to inform recommendations for future regulation | High |
| Ismail, Z. (2018). Humanitarian Access, Protection and Diplomacy in Besieged Areas. K4D Helpdesk Report. University of Birmingham | Secondary (other review – case studies and literature) | Global, with case studies on Iraq, Syria, and Yemen | Examines the lessons learned in terms of providing humanitarian access and protection for civilians in besieged areas. | High |
| Kalin, W. <i>Commentary on the Guiding Principles</i> (American Society of International Law, 2000) | Secondary (other review) | Global | Leading authoritative statement on the Guiding Principles on IDPs. | High |
| Khan, M. & Roy, P. 'Digital identities: a political settlements analysis of asymmetric power and information' (SOAS, Working Paper 015, October 2019). | Secondary (other review) | Asia and Africa | Analytical framework to explain the anomalous effects of digital identity systems, reviewing the available literature on relevant systems in Asia and Africa. | High |
| Kroener, I. et al, <i>Agile ethics: an iterative and flexible approach to assessing ethical, legal and social issues in the agile development of crisis management information systems</i> , Ethics and Information Technology (Springer), 11 February 2019 | Primary (qualitative description of process) and secondary (other review) | Global review, case study focussing on a multi-country platform | Development of an Agile Ethics and Privacy Impact Assessment process to support iterative technology development | High |
| Kuner, C. <i>International Organizations and the EU General Data Protection Regulation</i> , International Organizations Law Review 16 (2019) 158–191 | Secondary (other review) | Global, but focussed on EU law and organisations within the EU | Impact of GDPR on international organisations operating in or processing data from the EU, and potential conflict with international law on privileges and immunities. | High |
| Leite, P. George, T. Sun, C. Jones, T. Lindert, J. <i>Social Registries for Social Assistance and Beyond: Guidance Note and</i> | Primary (guidelines) Secondary (other review) | Global | Outlines typologies and trajectories of country experiences with Social Registries and provides a guidance note. | High |

| | | | | |
|--|------------------------------------|---|---|--------|
| <i>Assessment Tool</i> Protection & Jobs no.1704 (July 2017) | | | | |
| Makaay, E. et al 'Trust Frameworks for Identity Systems' (OIX, June 2017) | Secondary (other review) | Global | Describes trust frameworks and their role in governing an identity system. | High |
| Masiero, S. A new layer of exclusion? Assam, Aadhaar and the NRC (LSE Blog, September 2019) | Secondary (other review) | India | Prospects for those excluded from the final National Register of Citizens in Assam and how they could become ineligible for Aadhaar – the Government's digital identification project linked to access to welfare services. | Medium |
| Open Society Foundation 'Complying with the GDPR: Best Practices for Civil Society Organizations' | Secondary (other review) | Global, but with a focus on organisations with a connection to the EU | Review of both best practice and compliance challenges, and recommendations for improved future compliance | High |
| ODI and CDG 'Doing Cash Differently: How Cash Transfers Can Transform Humanitarian Aid – Report of the High-Level Panel on Humanitarian Cash Transfers' (14 September 2015) | Secondary (other review) | Global | Reviewed evidence about what cash transfers mean for humanitarian action and for affected people, and what opportunities cash presents for doing aid better. | High |
| Rachovitsa, A. <i>Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue</i> , <i>International Journal of Law and Information Technology</i> , Volume 24, Issue 4, Winter 2016, Pages 374–399, https://doi.org/10.1093/ijlit/ea012 | Secondary (other review) | Global | Article argues why policymakers and lawyers must understand the value of privacy as a fundamental technical property. | High |
| Regalado, D. et al. 'Behind the Syrian Conflict's Digital Front Lines' (FireEye, February 2015) | Primary (results of investigation) | Syria | Report on hack of Syrian Opposition groups | High |
| Roelen, K., Longhurst, D., and Sabates-Wheeler, R. The Role of Cash Transfers in Social Protection, | Secondary (other review) | Global | Overview of the use of cash transfers as (1) long-term support within social | High |

| | | | | |
|---|--------------------------|--------------------------------------|---|--------|
| Humanitarian Response, and Shock-Responsive Social Protection' (IDS Working Paper, Volume 2018 No 517) | | | protection systems; (2) immediate and short-term support as part of humanitarian assistance; and (3) a key component in scaling up social protection provision and coverage in the event of large-scale emergencies, or smaller-scale, household- and community-level shocks. | |
| Sepúlveda Carmona, Magdalena. 2018. 'Is Biometric Technology in Social Protection Programmes Illegal or Arbitrary? An Analysis of Privacy and Data Protection.' Extension of Social Security (ESS) Working Paper No. 59. Geneva, Switzerland: International Labour Organization (ILO) | Secondary (other review) | Global | Review of legislation, guidelines, and examples of the use of biometric technology in social protection systems, along with recommendations for improved privacy and data protection | High |
| Seyfert et al, <i>Unbundled: A framework for connecting safety nets and humanitarian assistance in refugee settings</i> (World Bank, Social Protection and Jobs Discussion Paper No. 1935, September 2019) | Secondary (other review) | Global | Outlines options for, and implications of, different ways to like humanitarian assistance to refugees to host country systems. | High |
| Temoshok, D. & Abruzzi, C. 'Developing Trust Frameworks to Support Identity Federations' (National Institute of Standards and Technology, January 2018) | Primary (description) | Global, but focus on United States | Explores the concepts around trust frameworks and identity federations and provides topics to consider in their development and implementation. | High |
| Thompson, S. & Warzel, C. 'One Nation Tracked' (New York Times Opinion, 19 December 2019) | Primary | Global, but focused on United States | An investigation into the smartphone tracking industry. | Medium |
| " <i>The Age of Digital Interdependence</i> " Report of the UN Secretary-General's High-level Panel on Digital Cooperation (2019) | Primary and Secondary | Global | From primary research and evidence, the panel highlight issues and give recommendations on digital cooperation going forward. | High |

| | | | | |
|--|---|-------------------------------|---|------|
| Weaver, C., Powell, J., & Leson, H. (2019) 'Open Data, Development Assistance, and Humanitarian Action'. In T. Davies, S. Walker, M. Rubinstein, & F. Perini (Eds.), <i>The State of Open Data: Histories and Horizons. Cape Town and Ottawa: African Minds and International Development Research Centre.</i> | Secondary (other review) | Global | Overview of the state of open data in the development and humanitarian space. Critical assessment of progress and pitfalls in the global transparency movement. | High |
| Woods, L. & Perrin, W. (April 2019) 'Online harm reduction – a statutory duty of care and regulator' (Carnegie UK Trust) | Secondary (other review) | Global, but focused on the UK | Proposes model regulatory regime for harm reduction in social media that respects freedom of expression. | High |
| Zuboff, S. <i>The Age of Surveillance Capitalism</i> (2019) | Primary (interviews) and secondary (other review) | Global | Reviews use of personal data by private companies and governments to track, predict, and modify behaviour. | High |

ANNEX 1 – MANAGEMENT INFORMATION SYSTEM DEFINITIONS

For better emergency response, the humanitarian community needs to collect, analyse, disseminate and act on key information. Currently many agencies use different systems that are not interoperable, with some moving towards greater interoperability and others stating that such a move is not possible.

This section aims to explain to those unfamiliar with MIS what the function is, what the purpose is, and what the possibilities for interoperability are. This section goes into detail on types of interoperability, and simply explains key issues raised in the main report such as digital identity, consent, and biometric data.

1.1 Introduction to MIS

Barca and O'Brien (2017) describe an MIS as "tailored software that transforms data retrieved from a database (and elsewhere) into usable and useful information." This MIS could be internal to one organisation, or it could retrieve, transform, and distribute information from multiple organisations (and their internal MIS). Broadly, an MIS consists of the people collecting data, the tools/software used to collect the data, a database to store the data, the interoperability layers and software to translate the data into information, analysts to translate the data to information, and the overall organisational structure that surrounds everything previously mentioned.

The general structure of any MIS will often be defined by the context in which it is applied and the requirements of the system overall. All have specific requirements, regulations and structures that surround security, sharing, communication, and consumption of data, but they all implement those structures in different ways. A high-level example of what might an MIS look like functionally is provided in Figure 1, below:

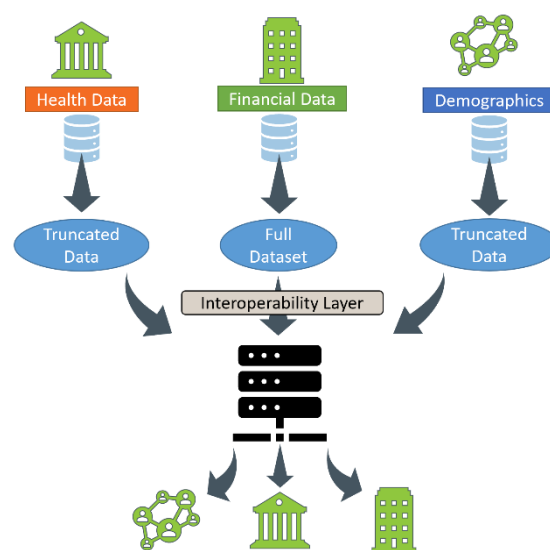



Figure 1 MIS diagram (interagency)

The text box below provides a summary of some relevant MIS operating in humanitarian crises. Each agency has its own mandate and their MIS have been established separately as proprietary systems. There is a clear drive towards greater interoperability, with organisations such as WFP and IOM starting to share data manually, as a first step towards collaboration.

| | | |
|---|--|--|
|  | Relevant Systems | |
| | SCOPE (WFP) | SCOPE is WFP’s beneficiary information and transfer management platform. The SCOPE platform is a web-based application used for beneficiary registrations, intervention setups, distribution planning, transfers and distribution reporting. SCOPE can support all transfer modalities including in kind, cash and voucher. SCOPE is a central repository for WFP beneficiary data and can be customised for specific interventions. The system can capture and store various personal data such as name, age, gender, household size, photos, fingerprints and iris scans. Through their systems SCOPE and BRAVe, WFP and IOM currently share data using manual data sharing processes. |
| | Primero (UNICEF) | Primero ¹⁴⁹ (Protection-related Information Management) is an open source (browser-based) software platform that provides case management, family tracing and incident monitoring. It is a public good, available for download on GitHub. Primero was developed as an inter-agency initiative in response to disparate and disconnected MIS and the detrimental effect this was seen to have on tracing beneficiaries, collaboration and information-sharing. ¹⁵⁰ Databases include the CPIMS (Child Protection Information Management System) used by IRC, Save the Children and UNICEF. Primero was developed in line with the Principles for Digital Development guided by the Do Not Harm, Need to Know, Informed Consent and Best Interests of the Child principles. Information management standards followed are the <i>Child Protection Minimum Standards in humanitarian action</i> (CPMS). All data are stored on UN Information Computer Center servers to ensure data are stored in accordance with UN and European Union Standards. |
| | BRAVe (IOM) | The B.R.A.Ve (Biometric Registration Assistance Verification) software is used for biometric data collection, card issuance, data processing and archiving, data sharing, response planning, and service provision. The software is also being used by Food partners for distributing food in sites where Biometric registration is completed. |
| | DTM (IOM) | The Displacement Tracking Matrix (DTM) is a Camp Coordination and Camp Management (CCCM) cluster tool developed by the International Organisation for Migration (IOM). DTM is a survey-based information management tool used to gather baseline information on internally displaced persons (IDPs) and their conditions where they have temporarily settled. |
| | PRIMES (UNHCR) Population Registration and Identity Management EcoSystem | PRIMES is a propriety MIS which encompasses all interoperable registration, identity management and caseload management tools and applications used by UNHCR. This includes <ul style="list-style-type: none"> • proGres, UNHCR’s Profile Global Registration System – the main repository in UNHCR for storing individuals’ data. The PRIMES platform allows different applications to access the proGres population registry. • BIMS, the Biometric Identity Management System that captures biometrics |

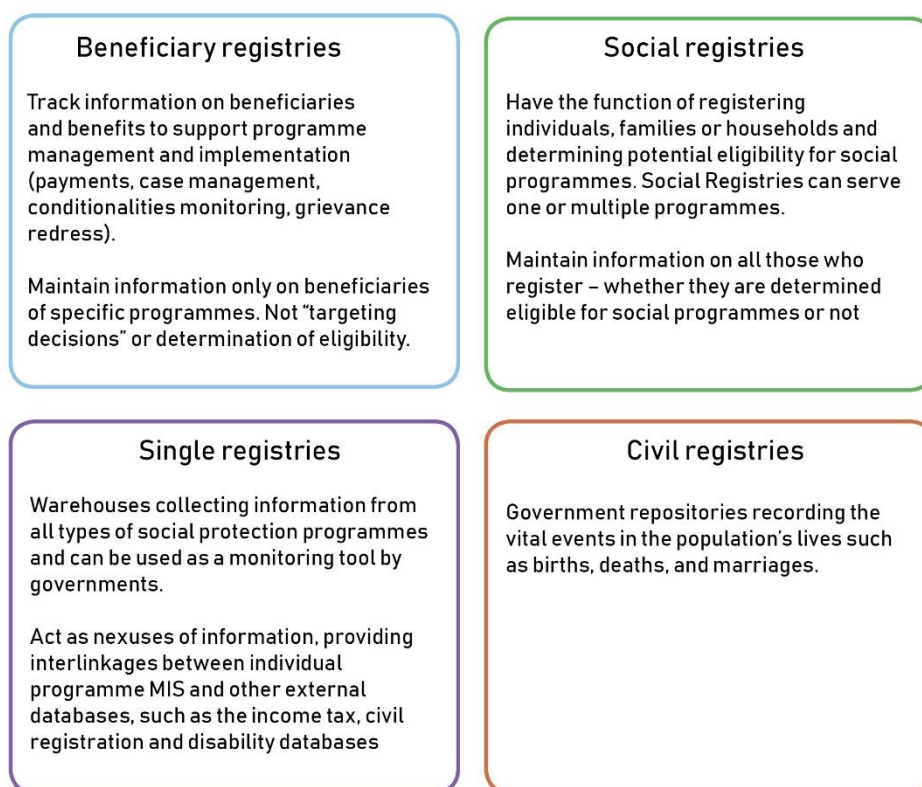
¹⁴⁹ <https://www.primer.org/>

¹⁵⁰ https://bettercarenetwork.org/sites/default/files/CPIMS%2B%20Review%20Report%20%28Full%20Version%29%20-%20A%20Review%20on%20the%20Utility%2C%20Systems-Effectiveness%2C%20and%20Deployability%20of%20the%20Tool%20%282018%29_.pdf

- CashAssist, that enables registered refugees to receive cash assistance
 - GDT, the Global Distribution Tool, allowing registered refugees to receive in-kind assistance
 - Rapid Application (RApp) – which allows offline data collection (later uploaded to pro-Gres) for refugees, IDPs, and others.
- UNHCR aim for PRIMES to be interoperable with the IT systems of government (civil and population registries), and partners (UNICEF PRIMERO, WFP SCOPE). UNHCR's Policy on Data Protection is applicable to PRIMES.

1.2 Single registry, social registry, civil registry

In this report we use the terms database and registry interchangeably to refer to data repositories and systems to organise, store and retrieve large amounts of data easily. As defined above, MIS are the software that transforms data retrieved from databases/registries into usable information. Databases/registries are components of wider MIS. Some examples¹⁵¹:



1.3 Centralised MIS

An MIS that is designed to function solely as an internal system is much simpler to implement than one that communicates between two or more organisations. However, such a fragmented arrangement is

¹⁵¹ Definitions from World Bank Group, Social Registries for Social Assistance and Beyond: A Guidance Note & Assessment Tool, 2017

not as beneficial as collaboration because, in humanitarian contexts, sharing resources and information successfully is likely to improve outcomes and quality of implementation.

Centralised MIS present numerous challenges ranging from system and data architecture, to data sensitivity, sharing agreements, and system management. Each organisation collects data of different types, on different platforms, for different purposes, at different frequencies, with varying levels of privacy and security requirements. In short, creating a single database information system to house and share data is both institutionally and technologically difficult.

In an illustrative ideal scenario, an MIS would be designed before implementation begins, garnering input from all potential participants in data exchange. This means bringing all actors to the table to decide what will be shared and how. Because of varying project start dates, project sizes, collection methods and data types, it would be technologically impractical and quite nearly impossible to require all actors to connect to a single database MIS. A centralised or federated MIS can solve this problem by collecting complete approved/required datasets from all actors and transforming or “translating” them to information usable across organisations using interoperability layers. This is an important function of any MIS and is most effective when designed and agreed upon at least at MIS design stages and ideally before participating projects decide on their internal architectures or begin collecting data. In reality, this ideal situation is elusive. Implementation schedules and start-up rarely if ever align across organisations and agencies, making coordination at outset next to impossible. Projects and institutions are frequently faced with poor structural or architectural design (data or otherwise), or low levels of interagency cooperation, contributing to implementation delays, service duplication, or service absence to name just a few.

Common data models – e.g. storing complete addresses in one field/cell or breaking out into number, city, state, etc- means of collating, and cross-referencing data, are most effective and simpler to implement when agreed upon and created before any data are input into any independent systems. There needs to be a common and logical way to associate or relate data from one data model to another across organisations, whether that be by standardised location data, standardised national identification number, standardised indexing method, etc. Interoperability layers enable that interrelation and association of data.

Throughout this report, we refer to different types of system architecture, in order to identify how fragmentation, one “super” single system, and different forms of interoperability (centralised vs federated) may impact upon the effectiveness of humanitarian aid and social protection programming. The graphic below defines these different types – single database, federated¹⁵², and centralised.

¹⁵² Centralized vs. Federated: State Approaches to P-20W Data Systems, National Center for Education Statistics

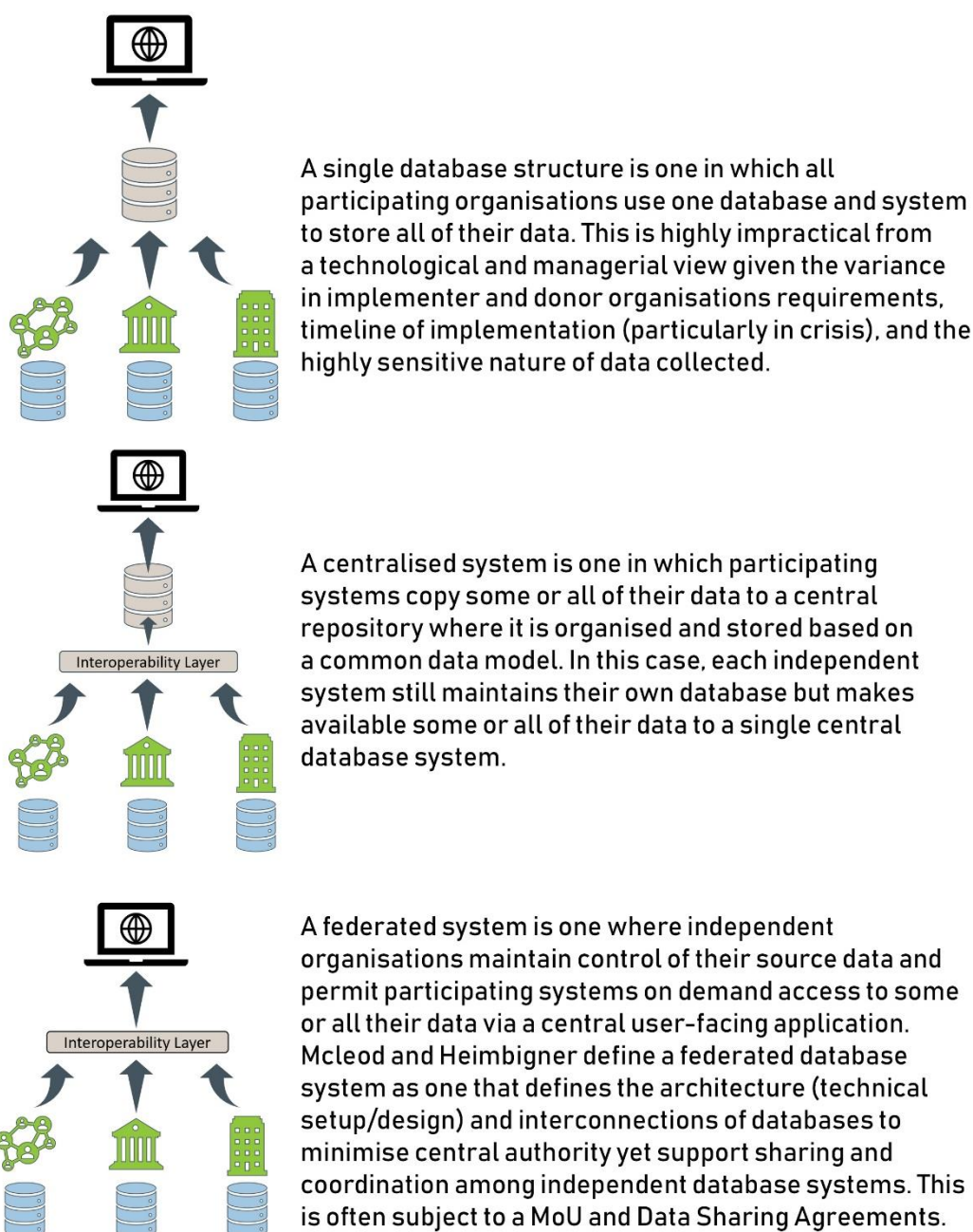


Figure 2 Types of System Architecture

To enable either a federated or centralised system, an interoperability layer is needed. This is a software application or data “translation” algorithm that is designed to standardise (match, relate, deduplicate), and store data in one place for efficient and secure exchange or analysis. As an example, SCOPE (WFP) and BRAVE (IOM) collect different amounts and types of data that are each best served and supported by utilising their own technology platforms and applications, but the resulting data can then be shared to a centralised or federated MIS and used by each participating organisation.

1.4 MIS Interoperability

As noted above, interoperability of MIS facilitates the sharing of reliable identification and registration data. In a crisis, the timely sharing of such data can create efficiency in targeting, efficiency in operations, and efficiency in planning. However, most MIS in the humanitarian and social protection sectors are not designed with interoperability in mind, with increasing collaboration (such as that between IOM and WFP – see box above) happening after the fact. It can be extremely difficult if not impossible to harmonise data

structures and semantics into one single database after separate architectures among disparate organisations have been created in accordance with hyper-specific contextual problems, such as distribution of food aid in refugee camps. Interoperability must therefore be at the forefront of any problem that an MIS is intended to help address.

Interoperability does not just apply to the technical design of the systems, indeed the Cash Learning Partnership (CaLP) recognise that interoperability requires numerous components – “coordinated systems on data standards, use of data, what data can be accessed by who, credentials/ID and transfer mechanisms”.¹⁵³

The most immediate challenge interoperability layers can address is that databases cannot automatically ‘talk’ directly to one another. There needs to be some kind of interface between. One that allows users and/or external systems to access and retrieve data. This is done using an application programming interface or API on the system that hosts the data to be exchanged. Through coding APIs, full or partial data access and management permissions can be granted based on any number of criteria that suits the data sharing needs and security requirements of the implementer. The API can also be considered an interoperability layer when it is designed to serve as the “translation” between different databases containing different types of data often stored in conceptually different ways. For example, different database types (Microsoft, Oracle, Postgres, etc) all have different methods for data creation, population (adding data), and communication. Data cannot simply be dropped from one into another because of programming differences, differences in format, or fundamentals of how the data are collected and stored. For example, one database may by design store an address in one field (ie one cell in Excel), another may break that address into multiple fields of number, street, village/city, state, region, etc.

Designing and implementing interoperability layers can be difficult and time-consuming if data harmonisation questions are not considered at project outset. By using standard definitions of data that allow for shared understanding and meaning within a particular context, like humanitarian response or health services, data transformation –and thus level of effort– within an interoperability layer can be minimized.

1.5 Data sharing agreements

In a context where data of the most vulnerable is being handled and agencies are in competition for resources, there is an evident level of protectionism over the data collected for both protection and commercial reasons. Data sharing agreements can help solve some data access/use concerns, but this solution requires close coordination between involved institutions. Numerous factors come into play in determining these arrangements, including power dynamics, institutional capacity and credibility, information quality and security.¹⁵⁴

In crisis situations, although the overarching theme is to improve the lives of those in need and all institutions are working towards a common good, mediation between organisations to reach adequate compromise and agreement may be fruitless. Sharing data requires a delicate balance of effective coordination and protection of the most vulnerable.¹⁵⁵

1.6 Data

The data collected by each organisation or agency will vary dependent on their needs. There are numerous different types of data, each with different implications for security and usability.

¹⁵³ Cash Learning Partnership (CaLP) and Inter-Agency Research and Analysis Network (IARAN), The Future of Financial Assistance: An Outlook to 2030 (November 2019)

¹⁵⁴ Leite, P. George, T. Sun, C. Jones, T. Lindert, J. Social Registries for Social Assistance and Beyond: Guidance Note and Assessment Tool, Protection & Jobs no.1704 (July 2017)

¹⁵⁵ Weaver, C., Powell, J., & Leson, H. (2019) Ibid.

Biographic data or Personal Identity Information are data that identifies an individual, such as their name, ID number, gender, age or date of birth, place of residence, or place of birth.

Personal data encompasses both biometric and biographic data. Personal data are any information relating to an individual that identifies, or can be used to identify, the individual.¹⁵⁶

Sensitive Data are Personal Data which, if disclosed, may result in discrimination against or the repression of the individual concerned. This may include data relating to health, race or ethnicity, religious/political/armed group affiliation, or genetic and biometric data.¹⁵⁷



Why it is important to understand: Biometrics

A person's biometrics cannot be changed, meaning that the leak of such data is often irreversible and can be catastrophic (i.e. while a password or account number can be changed after a leak to re-secure data, biometrics like fingerprints cannot be changed, posing challenges for re-registration if key biometric data are compromised). Biometric data can be used for theft, fraud, financial loss or other damages. In January 2018, it was reported that access to the entire digital ID database of India – Aadhaar – including the names, addresses, phone numbers, and photographs, but not fingerprint or iris scan data – was being sold for 500 rupees on a WhatsApp group.¹⁵⁸ In 2015, the United States Office of Personnel Management confirmed that 5.6 million fingerprints were stolen from its database, and noted that “Federal experts believe that, as of now, the ability to misuse fingerprint data is limited. However, this probability could change over time as technology evolves.”¹⁵⁹

1.7 Biometric data

Biometrics is the automated recognition of individuals based on their biological and behavioural characteristics.¹⁶⁰ The term “biometrics” can refer a wide range of forms of collecting biometric data such as fingerprinting (also known as dactyloscopic data), facial recognition, iris scans, DNA and gait. Biometric data can be used for authentication (e.g. use of fingerprints during distribution to determine whether a person is a registered beneficiary of in kind aid) and identification (e.g. use of facial recognition software to determine a person is who they claim to be).

The sensitivity of these data are well known, indeed biometric data are classified by GDPR as special category data due to its high sensitivity and has resultant stringent storage and processing regulations. ICRC also have a comprehensive policy on the processing of biometric personal data.¹⁶¹ Oxfam recognised these risks and imposed a moratorium on the use of biometric data in its programmes for two years and commissioned comprehensive research into the risks. The paper by the Engine Room and Oxfam on the use of Biometrics in the Humanitarian Sector¹⁶² is an excellent resource for the risks associated with the use of biometric data. Whilst not the focus on this research, due to the prevalence of biometric data in humanitarian and social protection systems, a few risks and benefits (system-type agnostic) are outlined below:

¹⁵⁶ WFP Guide to Personal Data Protection

¹⁵⁷ ICRC Handbook on Data Protection in Humanitarian Action

¹⁵⁸ Privacy International <https://privacyinternational.org/long-read/3067/have-biometric-id-system-coming-your-way-key-questions-ask-and-arguments-make>

¹⁵⁹ Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident (23 September 2015), available at: <https://www.opm.gov/news/releases/2015/09/cyber-statement-923>

¹⁶⁰ ICRC Handbook on Data Protection in Humanitarian Action

¹⁶¹ ICRC, Policy on the Processing of Biometric Data (2019)

¹⁶² Rahman, Z et al, Oxfam and The Engine Room, Biometrics in the Humanitarian Sector (2018)

Risks

- Uniqueness and immutability. Biometric data such as fingerprints cannot be modified and are unique. Increased risk of identity theft and reuse long into the future.
- Reusability / further processing. Increased risk of doing so due to immutability and richness of information. Some biometrics such as DNA can be used for a range of purposes, and likely even more so in the future. Ease of sharing and immutability make the data attractive to law enforcement and other actors.
- Reliability/Accuracy. Biometric data are often seen to be infallible, so results trusted, but in reality can return false matches, leading to exclusion. This can be down to errors or factors such as aging, cataracts in the iris, or increasingly depleted fingerprints through labour. Fingerprinting has the highest rate of error.
- Cultural Factors. Individuals may be reluctant to share data for cultural reasons or due to gender dynamics. For instance, women may not be willing to have their face uncovered for facial recognition software.
- Flexibility of use. Some such as facial recognition or iris scan could be done at a distance or without consent.
- Hacking. Due to increased interest in biometrics, there may be an increased incentive for hackers to obtain these unique data.
- Legal basis: Often there are no legal guidelines specific to biometrics, particularly in the countries in which humanitarian and social protection programmes are in operation.
- Cost burden. Human infrastructure, hardware and software, security, training and community sensitisation costs may or may not outweigh the efficiency savings.

Benefits

- Uniqueness and immutability of biometrics also make them a rigorous basis on which to identify someone long-term, potentially reducing the likelihood of leaving someone behind.
- Reusability / further processing. Assuming the individual gives consent, biometrics are attractive as they can be easily repurposed to provide access to services already or likely to use biometrics, such as bank accounts.
- Proportionality/minimisation. As the data are unique to the individual, in theory the agency only need to collect or hold one piece of data.
- Inclusion. Allow for inclusion of those that have no alternative means of identification (although criticised as perception of "giving an identity")
- Personal security. Beneficiaries do not need to carry a card or other personal papers. Their right to the aid is therefore protected, as well as their personal security.
- Fraud Reduction. Enhanced accuracy leading to reduction in double claimants, on one or multiple systems. Systems seen to "pay for themselves"

1.8 Blockchain

A blockchain-based system (or distributed ledger technology (DLT)-based system) is basically a database that is shared across a network of computers. Such systems allow for added layers of security and transparency (or opacity, to encrypt or hide data). However, in the case of social protection and humanitarian MIS, the number of disparate and unaligned data sources which exist in many contexts would pose problems for the establishment of such a system (as is the case with a single MIS). The system would necessitate being created from scratch.

Blockchains are best used when storing records that must remain unchanged (such as vaccine records or financial transaction data), which is not necessarily the case for social protection and humanitarian

programmes. Blockchain systems are also high energy consumption and may require significant IT skills and are perhaps not ideal for developing contexts. Blockchain based systems could be an unnecessarily complex response to the relatively simple issue of disparate datasets.¹⁶³

1.9 Consent

In the face of strong power imbalances, corresponding obligations are needed to ensure protection of fundamental rights. The need to obtain consent can be seen as an essential corresponding obligation of the right to privacy. This right is enshrined in key international legal instruments like the Universal Declaration of Human Rights¹⁶⁴ and the International Covenant on Civil and Political Rights,¹⁶⁵ and has been interpreted by the UN Human Rights Committee to extend to data protection.¹⁶⁶ More recently, in December 2016 the UN General Assembly adopted a resolution affirming the right to privacy in the digital age, which specifically references consent: expressing concern that “individuals often do not provide their free, explicit and informed consent”, and calling upon all States to “develop or maintain legislation, preventive measures and remedies addressing harm from the sale or multiple resale or other corporate sharing of personal data without the individual’s free, explicit and informed consent”.¹⁶⁷

The General Assembly’s own Guidelines for the Regulation of Computerized Personal Data Files require obtaining consent before using data other than for the purpose for which it was collected.¹⁶⁸ However, these guidelines include a “humanitarian clause” which provides for derogation “when the purpose of the file is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance.”¹⁶⁹ Such exceptions, particularly in emergency and/or humanitarian contexts, along with other legal avenues for data processing, are common features of many policies and guidelines.

The requirement of consent (generally with some exceptions) also features strongly in key regional/transnational legal frameworks, such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), Asia-Pacific Economic Cooperation (APEC) Privacy Framework, the Commonwealth of Nations Model Bill on the Protection of Personal Information, the EU General Data Protection Regulation (GDPR), the Council of Europe’s Convention 108,¹⁷⁰ and the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines. NGO, CSO, and UN agency guidelines, such as the ICRC Handbook on Data Protection in Humanitarian Action, the Open Society Foundation’s Complying with the GDPR: Best Practices for Civil Society Organizations, WFP Guide to Personal Data Protection and Privacy, and IOM Data Protection Manual, for example, also note the importance of consent and either require it, or include it as one of a small number of lawful bases for data processing.

In addition to this general convergence regarding the importance of consent, there is also convergence on the definition and interpretation of consent. As in the UN General Assembly’s definition above, many data protection laws require consent that is informed, explicit, and freely given. For example, the GDPR requires consent given to be a “freely given, specific, informed and unambiguous indication”.¹⁷¹ Similarly,

¹⁶³ More detail on the use of Blockchain in the humanitarian sector can be found at <https://jhumanitarianaction.springeropen.com/track/pdf/10.1186/s41018-018-0044-5>

¹⁶⁴ Universal Declaration of Human Rights, GA Res 217 A (III), UN Doc A/810 (10 December 1948), Article 12

¹⁶⁵ International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976), Article 17

¹⁶⁶ UN Human Rights Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 32nd Session (8 April 1988)

¹⁶⁷ UN General Assembly, The right to privacy in the digital age, GA Res 71/199 (19 December 2016)

¹⁶⁸ UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, GA Res 45/95 (adopted 14 December 1990), Part A(3)(b)

¹⁶⁹ Ibid, Part B

¹⁷⁰ Of which 9 of the 55 signatories are non-members of the Council of Europe – the membership of which is broader than that of the European Union

¹⁷¹ GDPR, recital 32

the South African Protection of Personal Information Act¹⁷² defines consent as: “any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information”, and the Malabo Convention states that “Consent of data subject means any manifestation of express, unequivocal, free, specific and informed will by which the data subject or his/her legal, judicial or treaty representative accepts that his/her personal data be subjected to manual or electronic processing.”

The Office of the Privacy Commissioner of Canada notes that for consent to truly be *informed*, data subjects must understand any meaningful residual¹⁷³ risks involved, which it defines as “a risk that falls below¹⁷⁴ the balance of probabilities but is more than a minimal or mere possibility”. The definition includes both direct and “foreseeable” risks, such as the risk, after transfer to a third party, of unauthorised use by an employee of that third party, or a breach of the third party’s systems.¹⁷⁵ Defining and assessing the level of these risks in a fragile, conflict-affected context is likely to be difficult. During a data collection exercise – particularly when providing urgent, life-saving support – how can the data collector articulate risks of future processing by an unknown third party (for example, the government established after a protracted conflict and conciliation process) in a manner that can be fully understood and consented to by a person in extreme, immediate need?

The UK Information Commissioner’s Office (ICO) interprets the need for *freely given* consent to require “giving people genuine choice and control over how you use their data” and the ability to “refuse consent without detriment”; it also advises that relying on consent is inappropriate where there is a significant power difference between the parties, or where the consent will act as a “precondition” for accessing services.¹⁷⁶ Putting this into action, the ICO recently concluded that a website that offered free access to news stories if the user accepted cookies, but required the user to pay for a subscription if they rejected cookies, was not obtaining “freely given” consent as there was no free option that did not include data collection and storage that was not necessary for the core purpose of the site (publishing news stories).¹⁷⁷

All of these examples demonstrate the increasing convergence globally on a definition of consent that recognises the need for both clear information on the implications of the consent, and that true consent relies on a freely given choice, which requires alternatives. In short, beneficiaries should not have to forego rights to privacy and data protection to realise other rights, such as the rights to social protection and an adequate standard of living enshrined in the International Covenant on Economic, Social and Cultural Rights.¹⁷⁸

In addition, consent is no substitute for protecting beneficiary rights by ensuring adherence to other core data protection principles like data minimisation, minimum data retention, and data protection and security – under a rights-based approach, consent should not be used as an “excuse” to provide lower levels of protection than is feasible, merely because beneficiaries “consented” to this approach. “Individuals forfeit a good deal of control over their personal data once it has been disclosed. Data

¹⁷² Expected to come into force later this year, with a one year grace period provided for compliance.

¹⁷³ The residual risk is the risk remaining after application of risk mitigation measures.

¹⁷⁴ If there is a likely/probable risk of harm (i.e. *above* the balance of probabilities), the Guidelines unsurprisingly consider data collection inappropriate.

¹⁷⁵ Office of the Privacy Commissioner of Canada, “Guidelines for obtaining meaningful consent” (May 2018), available at: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

¹⁷⁶ ICO, “What is Valid Consent?”, available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/> (accessed 14 February 2020)

¹⁷⁷ ICO letter to WP Company LLC, 11 October 2018, available at: <https://ico.org.uk/media/about-the-ico/disclosure-log/2616227/irq0872554-disclosure.pdf>

¹⁷⁸ UN General Assembly, Report of the Special Rapporteur on extreme poverty and human rights (A/74/493, 11 October 2019), at paragraph 64

controllers therefore bear the bulk of responsibility for ensuring good practice and privacy-preserving outcomes.”¹⁷⁹

Of course, during a humanitarian response, it may not be possible to provide the level of information and the alternatives needed to ensure consent is informed and freely given. In these situations, it will be necessary to rely on an alternative legal basis, such as vital interest or important grounds of public interest.¹⁸⁰ In such cases, if consent is not an appropriate basis for the initial data collection, it is similarly unlikely to be sufficient to form the basis for data transfer to a third party. This is particularly problematic in fragile and conflict-affected states, where:

1. It is unclear who will form the future government, and therefore to whom beneficiaries are providing their consent;
2. Government systems are not yet established, limiting the data collector’s ability to explain, and the beneficiary’s ability to understand and make a decision regarding the risks involved in the data transfer;
3. Timeframes for establishing government systems are unknown, risking reliance on out of date, and therefore inaccurate, data when these systems are developed, violating principles of accuracy and minimum retention periods for data collection;¹⁸¹
4. Potential bias in data collection where the government is a party to combat, as those who are not aligned with the government may be less likely to provide consent, and may therefore be under-represented in the data collected, impacting data accuracy and impartial future service delivery; and
5. The uncertainties around the data that may be needed for unknown future government systems (or use by any other party interested in providing services to beneficiaries) may encourage data over-collection, in violation of data minimisation principles.¹⁸²

To address this uncertainty, there may be a temptation to take advantage of what Zuboff terms “click-wrap contracts” through which a data subject is encouraged to “consent” to extensive terms and conditions around onward data sharing, and to agree that the data collector and/or processor can unilaterally amend the agreement to other use of the data subject’s personal data at any time.¹⁸³ While the advent of digital contracts that can be so easily amended (as compared to paper documents which are generally seen as fixed documents requiring fresh signatures, and an opportunity to review terms, to authorise amendments), this can hardly be seen as informed and freely-given consent.

As with the initial data collection, the transfer of data can be based on another legal basis. However, absent exigent circumstances that require transfer without consent, it may be difficult to justify a transfer on this basis. It also runs the risk of breaching trust between beneficiaries and nascent government systems, or the entities that conducted the initial data collection, if beneficiaries feel that they do not have control over their own data. Ultimately, we need to consider: are we sharing data to save lives in a context where consent is impossible? Or are we doing so for other reasons?

Even where consent can be relied on for the initial data collection, and in a more stable context where government systems are well-established (for example, during disaster response where agencies provide support to an established government that is not embroiled in conflict), concerns about over-collection of data remain. This will be particularly problematic where those collecting data have not first coordinated with the government, to understand what information is needed to effectively support government systems.

¹⁷⁹ ‘Personal Data Protection Guidelines for Africa: A joint initiative of the Internet Society and the Commission of the African Union’ (9 May 2018), page 24

¹⁸⁰ ICRC, Handbook on Data Protection in Humanitarian Action (July 2017), Chapter 3: Legal bases for personal data processing

¹⁸¹ Sepúlveda Carmona, Magdalena. 2018. ‘Is Biometric Technology in Social Protection Programmes Illegal or Arbitrary? An Analysis of Privacy and Data Protection.’ Extension of Social Security (ESS) Working Paper No. 59. Geneva, Switzerland: International Labour Organization (ILO).

¹⁸² Ibid.

¹⁸³ Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019) at pages 48–50.

Strong coordination with government is necessary both to ensure the data collected is useful, while still meeting data minimisation principles, and to fully understand the government's intended use of the data, to adequately inform and gain freely given consent from beneficiaries. This may need to include explaining likely onward sharing by government – for example, to third party service providers contracted by the government, or even with other governments as part of cross-border information sharing agreements.¹⁸⁴

This of course poses significant challenges for goals to increase efficiency and effectiveness in the transition to greater government control over social assistance. However, there are other ways to support governments towards this goal, including in ways that encourage greater accountability to beneficiaries, such as technical assistance on data collection and privacy, the development of Ethics and Privacy Impact Assessments for data collection,¹⁸⁵ and training for beneficiaries on data protection and privacy rights, to support efforts to involve beneficiaries in the co-design of systems that respond better to their needs, data protection or otherwise.¹⁸⁶ Such an approach aligns with movements toward a rights-based approach to data protection, rather than a narrow focus on technical compliance,¹⁸⁷ and the “interest of the international community in embedding data protection more strongly in international human rights law.”¹⁸⁸

1.10 Identity

Identity refers to the way systems identify individuals, creating registers of individuals in defined categories.

Identification is a critical mediator of power, and ID technologies ‘sit at the interface between the power and prerogatives of institutions and the rights and needs of individuals’.¹⁸⁹ Identification is a way of proving that an individual is who they say they are, and that they are entitled to defined rights and benefits.

As systems are increasingly digital and linked, digital identification becomes increasingly central to the relationship between institutions and individuals. A useful definition of a digital identity is from the Pan Canadian Trust Framework: “a trusted digital identity is an electronic representation of a person, used exclusively by that same person to receive valued services and to carry out transactions with trust and confidence”.¹⁹⁰

¹⁸⁴ See, for example, the ‘Personal Data Protection Guidelines for Africa: A joint initiative of the Internet Society and the Commission of the African Union’ (9 May 2018), noting the progress made “towards establishing a Continental Free Trade Area (CFTA) in support of the principles of free movement of persons, goods and services” and the “implications for the corresponding cross-border transfer of personal data, in the context of online transactions (trade), and of individuals living and working in member states other than their country of origin.”

¹⁸⁵ Kroener, I. et al, *Agile ethics: an iterative and flexible approach to assessing ethical, legal and social issues in the agile development of crisis management information systems*, Ethics and Information Technology (Springer), 11 February 2019

¹⁸⁶ UN General Assembly, Report of the Special Rapporteur on extreme poverty and human rights (A/74/493, 11 October 2019)

¹⁸⁷ See, for example, *NJCMcs/De Staat der Nederlanden (NJCM vs the Netherlands)*, also known as the “SyRI case”, in which the court’s ruling was largely based on fundamental human rights as outlined in the European Convention on Human Rights, rather than technical compliance with GDPR.

¹⁸⁸ Kuner, C. ‘International Organizations and the EU General Data Protection Regulation’, *International Organizations Law Review* 16 (2019) 158–191, at 162

¹⁸⁹ Center for Digital Development, Strategy & Research Team. ‘IDENTITY IN A DIGITAL AGE: INFRASTRUCTURE FOR INCLUSIVE DEVELOPMENT’. Washington, DC: USAID, 2017.
https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf.

¹⁹⁰ Pan Canadian Trust Framework – <https://diacc.ca/pan-canadian-trust-framework/>

Digital ID that can be used to access services – state as well as private – is nearly always based on an official or legal ID¹⁹¹. Official ID is the recognition of an individual by an official body, usually the State. Legal ID is defined as the basic attributes of an individual's identity that is officially recognised by a State's laws and/or practices.

States' identity systems can be defined by two categories. Foundational ID systems are intended for general purposes, such as the proof of legal identity and serve as the basis for the creation of functional IDs (e.g. civil registries and 'national ID' systems). Functional ID systems are intended to manage a specific service or transaction (for example, driving license, health record, voter ID). Functional IDs are also often treated as proof of official or legal identity. Voter ID cards or driving licenses are recognised as proving individual identity.

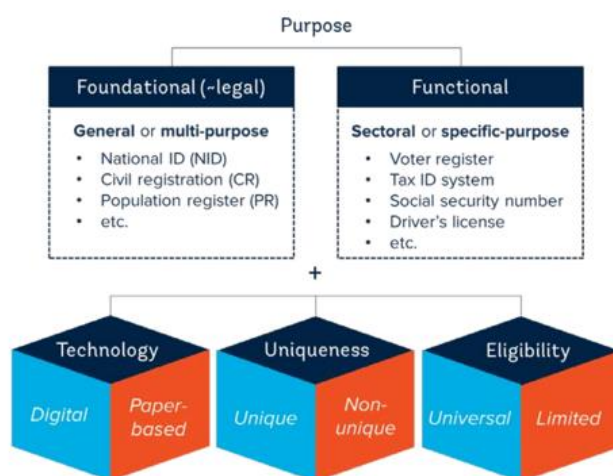


Figure 3 Foundational and Functional Identification. Source: World Bank ID4D Practitioners Guide

A functional ID credential is distinct from a legal identity, such as a birth certificate or identity card recognised under national law, and a foundational ID system, which commonly are intended for general purposes, including as proof of legal identity and a basis for issuing functional IDs (e.g. civil registries and 'national ID' systems). Functional ID systems reflect recognition of entitlement, and as such have different characteristics from foundational ID systems – they may not reflect entire populations, they may contain differing amounts and kinds of data, and there may be different data formats and data sharing practices between systems. There are often high levels of fragmentation within state functional systems, as within humanitarian identification systems. Furthermore, although functional identification systems do not usually grant legal status, they can sometimes serve as foundational credentials for humanitarian beneficiaries, particularly refugees, where refugee certificates serve as the most important credential in obtaining further rights and access to services.

Importantly, foundational and functional identity systems are never standalone systems, but exist as ecosystems that include not just the MIS and their parent institutions but the laws, regulations and political economy of the context in which they exist. See the figure below for an example from a mapping of Kenya's Identity Ecosystem by Caribou Digital¹⁹² of the diversity of MIS systems, and the complexity of relationships in an IE Ecosystem.

Identification credentials that prove the authenticity and uniqueness of the holder are critical to accessing humanitarian and state services, as well as services from the private sector such as mobile phone SIM cards and financial services including bank accounts and credit. Without these credentials, individuals can be excluded from both rights as well as opportunities. In protracted crises, the risk of loss or losing access to credentials is great – people may flee leaving documents behind or state institutions may be eroded or become party to the conflict and use ID issuance as part of conflict and political strategies. In the absence of state credential issuance, or the lack of agreement on the basis of ID issuance, aid agencies play an important role in providing services and the issuing of functional ID credentials.

¹⁹¹ World Bank ID4D Practitioners Guide 2019 - <https://id4d.worldbank.org/guide>

¹⁹² Caribou Digital, 2019, Kenya's Identity Ecosystem - <https://medium.com/caribou-digital/kenyas-identification-ecosystem-7cbc2ee27>

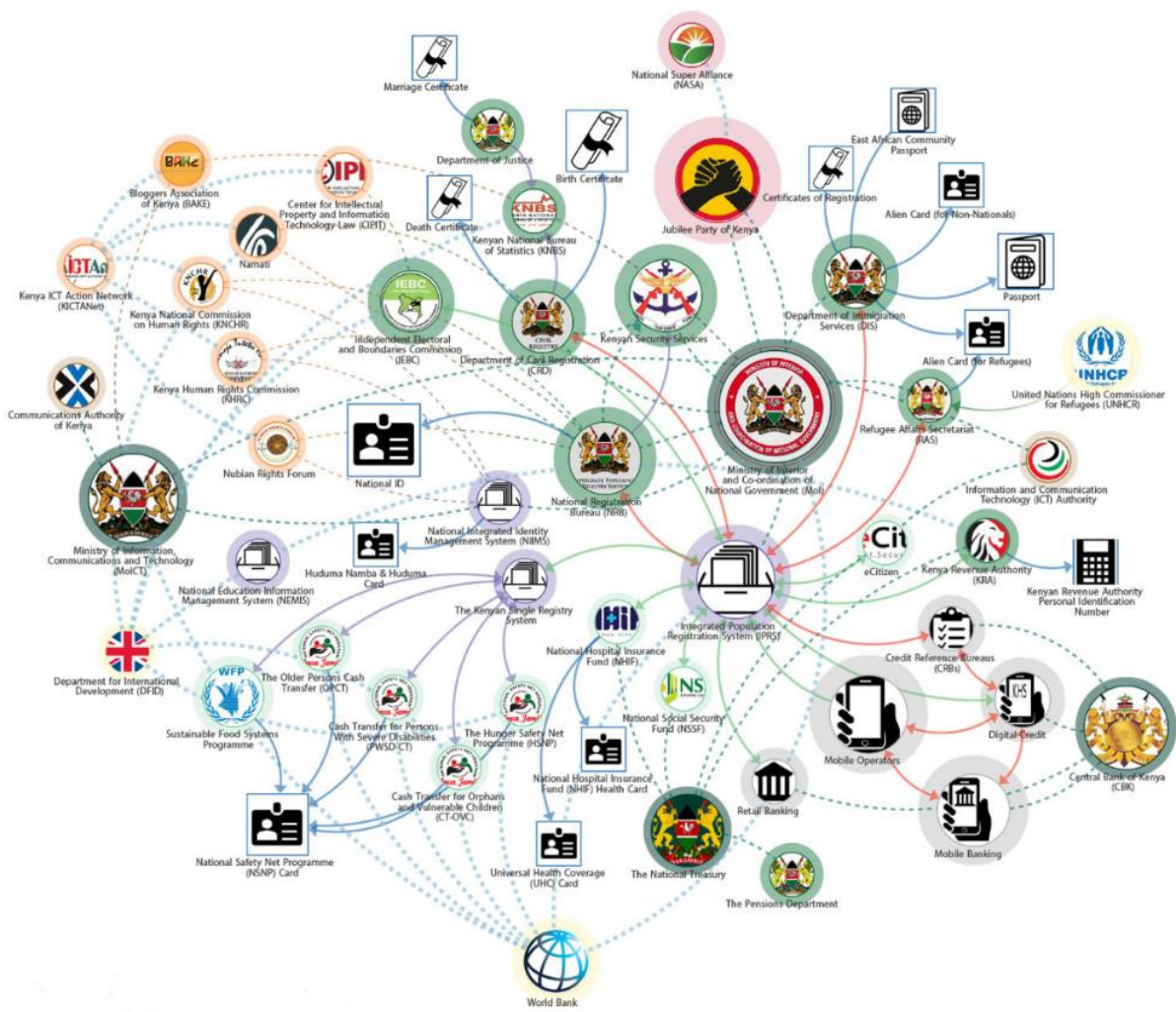


Figure 5 Kenya's Identity Ecosystem

ANNEX 2 – CASELOAD TYPES

This report focuses on the use of MIS in humanitarian contexts including how such system might support a transition to the establishment and / or resumption of a government role in transfer systems. In these contexts, a beneficiary might be described as fitting within various caseload categories. Vulnerability and need are of course more granular than these categories, but the MIS functionality needs to be able to meet the needs of people in these circumstances.

Caseloads are comprised of individuals with characteristics of one or more of the following categories are likely to comprise a substantial proportion of the caseloads managed by humanitarian, development, and state actors in fragile and conflict affected states. While some of these categories lack rigid definitions, others are narrowly defined in international, regional, and domestic law. The various rights related to these categories can have a significant impact on the obligations of those providing support to these groups.

2.1 Asylum seekers, refugees, returnees

Despite its broader use in everyday language, the legal definition of a “refugee”, and the rights associated with this legal status, are determined by international, regional, and domestic law. The 1951 Convention and the 1967 Protocol Relating to the Status of Refugees form the backbone of this definition, limiting the legal status of refugees to those who are: “unable or unwilling to return to their country of origin owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group, or political opinion.”

However, refugee status is determined by the receiving state, in accordance with domestic and/or regional legislation implementing, and caselaw interpreting, these provisions. There is therefore some jurisdictional variation in the implementation of this definition and its associated legal status.¹⁹³ Asylum seekers include both those seeking refugee status (who therefore are entitled to international protection pending status determination), and individuals that cross international borders as part of large groups where individual status determinations are logistically impractical.¹⁹⁴ Returnees are former refugees who have returned to their country of origin.

The Office of the UN High Commissioner for Refugees (UNHCR), a multilateral, intergovernmental institution, and subsidiary organ of the General Assembly, holds the mandate to support refugees, returnees, and asylum seekers, including “providing international protection” and “seeking permanent solutions”.¹⁹⁵ This mandate is strongly entrenched in public international law, including in the Statute of the Office of the High Commissioner for Refugees, General Assembly resolutions, and multilateral treaties (including the 1951 Convention and 1967 Protocol).¹⁹⁶ While asylum seekers, refugees, and returnees clearly form a core part of UNHCR’s mandate, it is increasingly asked to extend its “good offices” to others in humanitarian need, including host communities and internally displaced persons, as discussed below.

Of course, UNHCR’s mandate does not mean it is the exclusive provider of support to asylum seekers, refugees, and returnees. This is even recognised in UNHCR’s mandate, which includes authorisation to “invite the co-operation of the various specialized agencies”.¹⁹⁷ In addition, to accomplish its mandate it is obligated to coordinate with both host and origin states in refugee status determinations (which can only be made by host states), and to facilitate reintegration of returnees.¹⁹⁸ These obligations to coordinate

¹⁹³ Guy S. Goodwin-Gill and Jane McAdam, *The Refugee in International Law* (3rd Edition) ‘Part 1 Refugees, 2 Refugees Defined and Described’ (Oxford University Press, 2015)

¹⁹⁴ UNHCR Division of International Protection, ‘Note on the Mandate of the High Commissioner for Refugees and his Office’ (October 2013), pages 3–4

¹⁹⁵ Statute of the Office of the High Commissioner for Refugees, as revised by GA res. 58/153, 22 December 2003, at paragraph 1

¹⁹⁶ UNHCR Division of International Protection, ‘Note on the Mandate of the High Commissioner for Refugees and his Office’ (October 2013), pages 1–2

¹⁹⁷ UNHCR Statute, paragraph 12

¹⁹⁸ UNHCR Division of International Protection, ‘Note on the Mandate of the High Commissioner for Refugees and his Office’ (October 2013), pages 4–8

with states will have an impact on data sharing, and associated data protection concerns, undertaken by UNHCR.

2.2 Internally displaced persons (IDPs)

The Guiding Principles on Internal Displacement define IDPs as: “persons or groups of persons who have been forced or obliged to flee or to leave their homes or places of habitual residence, in particular as a result of or in order to avoid the effects of armed conflict, situations of generalized violence, violations of human rights or natural or human-made disasters, and who have not crossed an internationally recognized state border.”¹⁹⁹ This definition is wider than that of refugees in terms of the reasons for displacement (albeit limited to those within their country of origin), and importantly does not provide a complete, finite list of criteria, allowing for potential change over time.

The Guiding Principles are not a binding legal instrument themselves – instead, they compile existing legal protections from international, regional, and domestic law, and articulate how these would apply to IDPs, occasionally applying refugee and humanitarian law by analogy.²⁰⁰ As such, the Guiding Principles do not confer a legal status on IDPs. They instead recognise that IDPs remain in their countries of origin and have the same rights as other citizens, but acknowledge and address their special needs and challenges in accessing these rights due to their displacement.

In contrast to UNHCR’s mandate regarding asylum seekers, refugees, and returnees, there is no single UN agency that holds a mandate regarding IDPs. Instead, the Special Rapporteur on the Human Rights of Internally Displaced Persons acts as the focal point for protection, and cooperates with a variety of actors involved in the IDP response, including UNHCR, IOM, WFP, UNDP, UNICEF, WHO, ICRC, INGOs, NGOs, regional, and state authorities, among many others.²⁰¹

2.3 Host communities

The needs of host communities have received less attention compared to those of refugees and IDPs. However, there is increasing awareness that host communities need to be included in programming, to avoid conflict with nearby groups that are receiving greater international support, recognise their likely high levels of need,²⁰² and support durable solutions, particularly for communities hosting refugees and/or IDPs who are unlikely to return to their place of origin.²⁰³

For these reasons, host communities are receiving increased attention. This can be seen, for example, in their inclusion in regional instruments like the African Union Convention for the Protection and Assistance of Internally Displaced Persons in Africa, which expands on the Guiding Principles on IDPs in a number of aspects, including requiring specific consideration of host communities and their needs.²⁰⁴

2.4 Vulnerable people

Beyond the specific groups outlined above, much programming seeks to include vulnerable people or groups in caseloads. However, definitions of vulnerability vary significantly across programmes, based on the specific vulnerabilities the programme seeks to target. Common vulnerable categories used in social assistance schemes worldwide include:²⁰⁵

- Maternal (pregnant and lactating women);

¹⁹⁹ United Nations Guiding Principles on Internal Displacement 1998, Introduction: Scope and Purpose, paragraph 2

²⁰⁰ Ibid. and W. Kalin, Commentary on the Guiding Principles (American Society of International Law, 2000)

²⁰¹ See Mandate of the Special Rapporteur on the human rights of internally displaced persons (A/HRC/RES/23/8, 20 June 2013)

²⁰² With approximately one third of the global refugee population (6.7 million people) in the Least Developed Countries in 2018: see UNHCR (2019), Global trends: Forced displacement in 2018

²⁰³ See UNHCR-NGO Toolkit for Practical Cooperation on Resettlement. Community Outreach – Outreach to Host Communities: Definitions and FAQs (June 2011)

²⁰⁴ African Union Convention for the Protection and Assistance of Internally Displaced Persons in Africa (Kampala Convention), adopted 23 October 2009, entered into force 6 December 2012

²⁰⁵ Goodman et al., ‘Yemen – Linking Humanitarian Cash and Social Protection: Phase I Report’ (DFID BASIC, June 2019), at page 42

- Infants and children;
- Orphans and Child-headed households, and Female-headed households;
- Severe disability or severely disabled (mental and physical, or those with chronic illnesses);
- Elderly persons (such as those above 60, 65 or 70 years old).

Varying programmatic definitions of vulnerability will lead to differing data collection needs across organisations. This poses challenges for greater interoperability across MIS, and risks leading to unnecessary additional data collection in an attempt to meet each organisation's needs, along with the risks associated with holding more personal details on an individual in one place. These risks are discussed further below.

ANNEX 3 – RISK TABLE

Risks and Benefits of MIS in Crises

| | Political | | Protection | | Legal and Ethical | | Commercial | | Operational | |
|--|--|----------|---|----------|---|----------|---|----------|--|----------|
| | Concerning the implications of political economy realities. For instance, host community perceptions, trust in government, government involvement in conflict (potential contribution to conflict resolution and stability), and perception of data accuracy. | | The tension between protection and inclusion including obligations to beneficiaries (security, consent, preferences, etc), proportionality (in data collection and sharing) and accountability. | | Ethical frameworks, legislation and regulation that guide and govern MIS | | Implications of different types of provisions and interoperability measures on fiduciary responsibility, value for money, set up and maintenance and so on. | | Effectiveness of different types of systems with regards to response, targeting and sustainability. | |
| | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits |
| ALL (implications which are system type-agnostic) | Political misuse of data. Whether data is leaked or status is recognisable through carrying a card or data sharing with entities such as banks, if individuals are known to be receiving aid they may face discrimination or persecution. Individual security may also be a factor for groups at risk of persecution by government. <i>Mitigating Action: Proportionate data collection; comprehensive data protection and data security protocol; limit data sharing with other entities (such as banks). e.g. collecting only what is needed for particular services; not collecting data which may be able to identify sensitive information such as ethnicity.</i> | | Personal security is a particular concern in a conflict environment. The risks associated with host government or international security agency access to the data - whether permissioned, leaked, extorted, or hacked - may put the personal security of certain groups at stake. <i>Mitigating actions: Proportionate data collection: e.g. collecting only what is needed for particular services; not collecting data which may be able to identify sensitive information such as ethnicity. Comprehensive data protection and data security protocols.</i> | | Often no legal requirements in the countries we work. Where they do exist, laws policies and frameworks often do not cover digital capture, use and storage of personal data. Inadequate regulation and governance increase risks for users. <i>Mitigating Actions: Donors should support government to develop data protection policies. In the short-term, agencies should have their own policies and/or adhere to global standards.</i> | | Lack of data on value for money of both implications of types of MIS and of the use of biometrics. | | System management can be an increased burden on any organization. Each type of system has more or less of an operational burden. | |

| | Political | | Protection | | Legal and Ethical | | Commercial | | Operational | |
|--|-----------|----------|--|----------|---|----------|---|----------|-------------|----------|
| | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits |
| | | | <p>Consent: It is challenging to obtain genuine informed consent in a humanitarian agency. Each type of system presents similar concerns: whether the responsibility to collect consent is one agency's (single system) or many, the risks with this process in the humanitarian sector are significant.</p> <p><i>Mitigating Actions: Protocols in the sector as a whole require alignment and better definition.</i></p> | | <p>International standards do not apply to all (e.g. the UN) and thus are insufficient to plug the gap in a lack of national regulation.</p> <p><i>Mitigating Actions: Consensus on data protection is needed, such as the application of international regulations. In the meantime, organisations should adhere to their own comprehensive data standards or chose to follow those such as GDPR</i></p> | | <p>Reputational damages need to be considered for any type of MIS. Data breaches may have implications for the agency and donor, particularly in cases where third parties are involved.</p> <p><i>Mitigating Actions: Particular care should be taken to limit involvement of third parties with negative press or poor data protection histories.</i></p> | | | |

| | Political | | Protection | | Legal and Ethical | | Commercial | | Operational | |
|--|-----------|----------|--|----------|---|----------|------------|----------|-------------|----------|
| | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits |
| | | | <p>Unauthorised use or further processing. Data may be obtained - whether legally or illicitly - and used for purposes other than the intended. This includes use for political propaganda and commercial targeting as well as "good" purposes for which there is no explicit permission, such as tracking of migration or vulnerability analysis. This is a risk to any type of system. <i>Mitigating actions: Data sharing agreements outlining the purposes for data sharing and parameters within which the data may be used. These agreements are reflected in consent processes.</i></p> | | <p>Digital Dignity: many MIS do not afford individuals control over their digital identity and their own data. <i>Mitigating Actions: agencies should look at the way data is governed against humanitarian principles.</i></p> | | | | | |
| | | | <p>Big data: Large datasets allow for the generation of sensitive data when processed for data analytics in a humanitarian situation. Generating data that can lead to surveillance - digital footprints, breaching anonymity through reverse engineering. <i>Mitigating Action: Proportionate data collection; comprehensive data protection and data security protocol; limit data sharing</i></p> | | | | | | | |

| | Political | | Protection | | Legal and Ethical | | Commercial | | Operational | |
|--------|---|----------|--|--|-------------------|----------|---|---|--|----------|
| | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits |
| Single | Data ownership and access turned over to the managing agency, so agencies lose their ownership of data collected. This has implications for the political economy of aid as one agency now controls all beneficiary data. | | Data ownership and access turned over to the managing agency, so agencies lose their ownership of data collected. This has implications for consent given by beneficiaries. | Fairness. Any interoperability or centralisation allows for increased accuracy of targeting and reduced double dipping. This may increase fairness in sharing of resources. However, this requires alignment of eligibility criteria as well as systems. | | | Very high cost to build, manage and implement, particularly where the system is built retrospectively from existing datasets and separate MIS | Fiduciary responsibility passed on to the central system holder - a benefit for smaller NGOs or organisations who may have less capacity. | Implementation time is significant due to efforts required to build one single system and upload all data. | |
| | Political | | Protection | | Legal and Ethical | | Commercial | | Operational | |
| | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits |
| | | | Government pressure: Dependent on where it is housed and the operating agency, the organisation may legally (or at least pressured) be required by gov to share data, despite consent from beneficiaries (not UN agencies). Most pressure for single and centralised MIS where ownership rests in a single place. <i>Mitigating Actions: Data access and sharing protocols should</i> | Ease of case sharing. With all data in one place, as long as data is stored consistently, agencies with access can see all data separate organisations have collected on one household, allowing them to have a full picture of needs. | | | | | Proportionality: data imported will all need to have the same information. For new data this means aligning what needs to be collected in order to aid different types of analysis. For old data, this is a near-impossible task and may require additional data collection. | |

| | | | | | | | | | |
|-----------|----------|--|--|-------------------|----------|------------|----------|--|---|
| | | <i>be clearly defined in line with government policies (where relevant), international standards and beneficiary consent.</i> | | | | | | | |
| Political | | Protection | | Legal and Ethical | | Commercial | | Operational | |
| Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits |
| | | Data Sharing. A single agency has control over who accesses the data. They could therefore approve access by third parties, such as an external Data Processors, Data Controllers, technology providers and other humanitarian organisations. | Accountability for data protection lies in one place, which allows for easier monitoring and enforcement, providing the agency has robust policies | | | | | System management will be a significant factor in implementing a single system. This includes database maintenance, security of one large database, and ensuring all agencies are properly uploaded and keeping data up to date. | Information management is made easier with all data in one place. Facilitates targeting and planning. |
| | | Privacy/Security: Full responsibility is with the system holder. Stakes very high in event of a breach since all data are stored in one location. Breach includes hacking by entities such as national or international security forces. <i>Mitigating Action: The system</i> | | | | | | Sustainability: easiest to transfer data to government as data is under ownership of the single system holder. <i>Mitigating Actions: Agency should have consent for this transfer from beneficiaries, or be under data protection regulations which oversee</i> | |

| | | | | | | | | | | |
|-----------|-----------|----------|--|--|-------------------|----------|--|--|--|--|
| | | | owner must follow all standard cyber security procedures that apply to the level of data privacy required for the data stored. The owner must ensure software is up to date, designed securely, and ensure users have complicated passwords. | | | | | | | |
| | Political | | Protection | | Legal and Ethical | | Commercial | | Operational | |
| | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits |
| Federated | | | Data sharing: the source agency owns and ultimately controls the data and shares it under an MoU. It may operate in conjunction with a variety of private sector institutions and NGOs serving as enrolment centres, thereby increasing the number of parties that have access to at least some of an individual's data. Based on MoU, at any time the source agency can terminate | Data ownership is with the source agency with no need for shared data stewardship. | | | Staff resources are required of each source system to oversee and maintain required data access. Support required to ensure any changes in data in the source location are reflected. Resources needed from each agency to review and approve data requests. | Create efficiencies: Federated systems may create efficiencies which lead to cost-saving for each organisation involved, without cost implications of single or centralised systems. | Data updates and corrections: Data reside within each agency, so each agency is responsible for communicating and possibly updating the data extract processes to reflect changes, corrections or updates. Accuracy of data in centralised system depends on effectiveness of this process | Implementation generally easier and quicker, though still required time for process determination and interoperability layer design and build. |

| | | | | | | | | | |
|-----------|----------|---|--|-------------------|----------|------------|----------|---|--|
| | | | access to the data but should also properly de-identify individuals before sharing if this is grave concern. <i>Mitigating Actions: The MoU should spell out any permissioned sharing and cleaning/de-identifying of these data.</i> | | | | | | |
| Political | | Protection | | Legal and Ethical | | Commercial | | Operational | |
| Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits |
| | | Accountability for data protection lies within each agency, as well as central system holder. <i>Requires equal levels of commitment from each organisation and agreement on policies.</i> | Privacy/Security: Primary responsibility is with the source system agencies. Secure process needed for handling of data queries. Data are diffused, allowing for tailored protection based on sensitivity of each source system's data, and reducing the amount of data that could be accessed through a breach. | | | | | Data Quality is dependent on processes implemented at each agency. | Information management of data between agencies is made easier as agencies can share data on a much more fluid basis. Facilitates planning and targeting, and alignment between agencies for better operational efficiency, providing processes to do so are in place. |
| | | | Proportionality: each agency or organisation can collect the data they require, and share only what is necessary. | | | | | Effectiveness and efficiency in registration may be compromised as data collected needs | Effectiveness and efficiency in registration may be improved as |

| | | | | | | | | | | |
|--|--|--|--|---|--|--|--|--|---|---|
| | | | | | | | | | to be aligned so it can be translated by the central MIS. This means there may be more questions to be asked, reducing efficiency. | data collected digitally can be immediately referenced with existing data in the MIS. |
| | | | | Ease of case sharing. Where consented to, a federated system can improve protection. For instance, separate agencies may share details of vulnerable children, allowing another quickly respond. | | | | | System management burden can be decreased. There must be an entity to maintain the interoperability layer and connections between agencies. This is a software process and reduces the need for a larger team to manage a database and software platform. | Data handling at implementation closeout is simplified because the data is stored in only one place, on the source agency's database. The interoperability layer must be modified to remove references to the data to be removed. This is often easier than removing and cleaning data from a database. |
| | | | | Fairness. Any interoperability or centralisation allows for increased accuracy of targeting and reduced double dipping. This may increase fairness in sharing of resources. However, this requires alignment of eligibility criteria as well as systems | | | | | | |

| | Political | | Protection | | Legal and Ethical | | Commercial | | Operational | |
|-------------|-----------|----------|--|--|-------------------|----------|--|----------|--|--|
| | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits |
| Centralised | | | <p>Data ownership is with the source agency with shared data stewardship with the centralized data warehouse agency/entity. The agency may share with a variety of private sector institutions and NGOs. <i>Mitigating Actions: Responsibility for this data stewardship should be spelled out in memoranda of understanding (MOU). Should apply rigorous data protection protocols to all partners.</i></p> | <p>Fairness. Any interoperability or centralisation allows for increased accuracy of targeting and reduced double dipping. This may increase fairness in sharing of resources. However, this requires alignment of eligibility criteria as well as systems</p> | | | <p>Staff resources are required of each source system to oversee and maintain required data access. Support required to ensure any changes in data in the source location are reflected. Resources needed to support the centralized data base system.</p> | | <p>Data updates and corrections: a process is required including when data is to be updated.</p> | <p>Data Quality can be more easily assured as data is validated as part of the load process and cleaned regularly.</p> |

| Political | | Protection | | Legal and Ethical | | Commercial | | Operational | |
|-----------|----------|--|--|-------------------|----------|--|----------|--|--|
| Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits |
| | | Privacy/Security: Primary responsibility is with the centralized data system agency/entity, so stakes may be higher in event of a breach since all data are stored in one location. <i>Mitigating Actions: Responsibility for this data stewardship should be spelled out in memoranda of understanding (MOU); Records should be de-identified.</i> | Privacy/Security: Primary responsibility is with the centralized data system agency/entity as the data steward, but is dictated by source system agencies via memoranda of understanding. Makes it easier to account for data integrity. | | | Costs are increased to the centralised system holder due to ongoing maintenance and operational costs of a large coordinated database. | | Implementation can take some time due to the need to build a centralised data warehouse. Equal time needed for process determination as federated. | Information management of data between agencies is made easier as agencies can share data. Facilitates planning and targeting, and alignment of these between agencies for better operational efficiency, providing processes to do so are in place. |
| | | Government pressure: Dependent on where it is housed and the operating agency, the organisation may legally (or at least pressured) be required by gov to share data, despite consent from beneficiaries (not UN agencies). Most pressure for | Proportionality: each agency or organisation can collect the data they require, and share only what is necessary. | | | | | Effectiveness and efficiency in registration may be compromised as data collected needs to be aligned so it can be translated by the central MIS. This means there may be more questions to be asked, reducing efficiency. During use of the data, this "translation" would already be taken care of by the interoperability layer, so that if a | Effectiveness and efficiency in registration may be improved as data collected digitally can be immediately referenced with existing data in the MIS. |

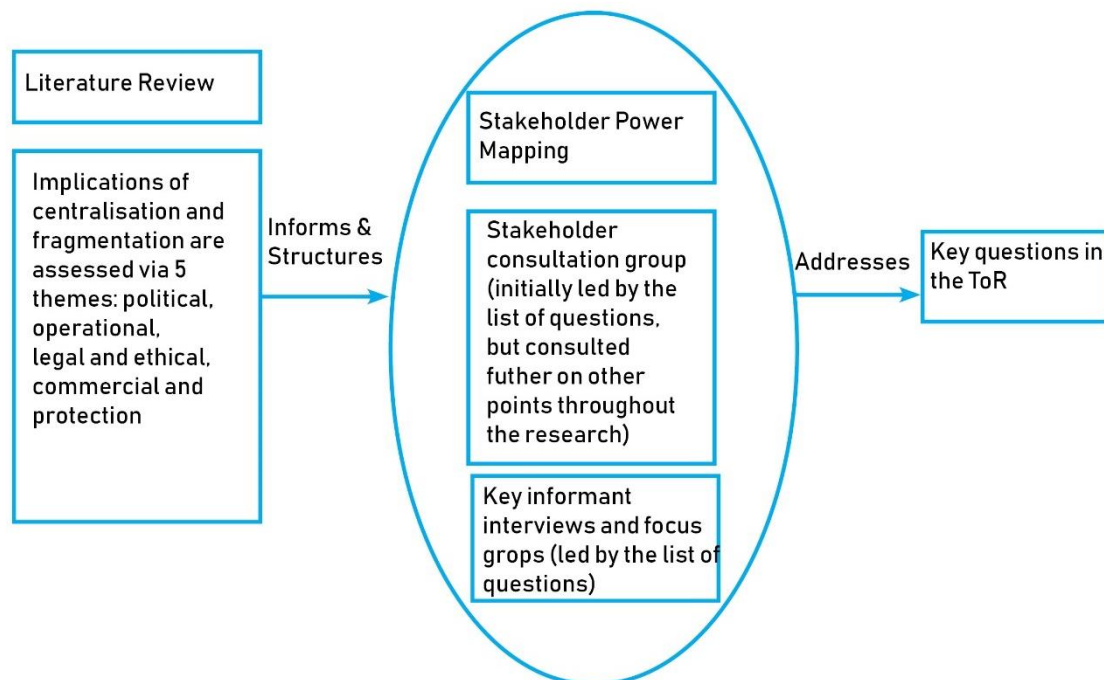
| | | | | | | | | | |
|--|--|--|--|--|--|--|--|---|--|
| | | <p>single and centralised MIS where ownership rests in a single place.</p> <p><i>Mitigating Actions: Data access and sharing protocols should be clearly defined in line with government policies (where relevant), international standards and beneficiary consent.</i></p> | | | | | | <p>user is already registered somewhere, they can reference them, but only IF there has been a method devised (and coded in the software) to properly de-duplicate efficiently.</p> | |
| | | <p>Accountability for data protection passed on in centralised systems. Organisations may feel it is the central data holder's responsibility. May not be clear lines of responsibility but both agencies are ultimately accountable for protecting the data from unauthorised access or use on their systems.</p> <p><i>Mitigating Actions: Responsibility for data</i></p> | | | | | | <p>Data handling at implementation closeout is more complex because the data is stored in more than one place. Data in its entirety or piecemeal will have to be removed from the central database based on sensitivity, data sharing agreements, and MOUs.</p> | |

| | | | | | | | | | | |
|------------|---|----------|---|--|-------------------|----------|--|----------|---|--|
| | | | <i>protection is the responsibility of all and should be spelled out in memoranda of understanding (MOU) and in line with relevant data protection policies.</i> | | | | | | | |
| | | | Data sharing: the centralised data system controls who has access to the data. Third parties can only access data if given permission. It is important that whoever controls the host database be trustworthy or independent party if possible. | Ease of case sharing. Where consented to, a centralised system can improve protection. For instance, separate agencies may share details of vulnerable children, allowing another quickly respond. | | | | | | |
| | Political | | Protection | | Legal and Ethical | | Commercial | | Operational | |
| | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits | Risks | Benefits |
| Fragmented | Political economy of aid: protectionism of agencies over their MIS and their own data can perpetuate the number of separate and disconnected MIS. | | Data sharing: Increased instances of data sharing and storage create further points of entry for hacking or leakage. Small organisations less likely to have the resources to have rigorous processes in place. | Data sharing: Despite the risk of using multiple systems, if one system gets hacked, it does not necessarily mean that others will as well. | | | Numerous systems could lead to confusion among beneficiaries or inflated time taken to receive goods and services. | | Double-Dipping. Depending on the amount of overlap in assistance, disparate MIS may lead to double dipping and thus doubling of efforts of agencies, resulting in inefficiencies. | Data handling at implementation closeout is simplified because the data is stored in only one place. |

| | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|
| | | | Proportionality: When systems are fragmented, data may be over-collected, lost and reproduced. Affected populations are often surveyed multiple times, triggering questions regarding the ethics of beneficiary data collection | Proportionality: each agency or organisation can collect the data they require, and share only what is necessary or agreed upon. | | | | Costs are onto each agency, some of whom may struggle under the burden (such as small NGOs) | | Information management is more challenging as information is in separate locations and not always shared between agencies. Little opportunity to recognise trends for more effective planning and response. | |
| | | | | | | | | | | Effectiveness and efficiency in registration compromised as fragmented systems can be frustrating and costly as they need to go to multiple locations to apply for different benefits and services | |
| | | | | | | | | Double-Dipping. Depending on the amount of overlap in assistance, disparate MIS may lead to double dipping and thus reduced value for money and increased costs. | | Sustainability: Fragmented systems would render this transfer challenging, due to disparate datasets, the lengthy process of data translation, and the numerous data sharing agreements which would be required. | |

Sources - The Engine Room and Oxfam Report; ICRC Handbook on Humanitarian Data Protection; Centralized vs. Federated: State Approaches to P-20W Data Systems, October 2012 (National Center for Education Statistics)

ANNEX 4 – ANALYTICAL FRAMEWORK



| TOR Questions | Detailed questions (including interview questions) | Theme* <i>* every theme may be applicable to each question, dependent on our findings.</i> | Method (KII, beneficiary interviews and focus groups consultation group, stakeholder power mapping) |
|---|--|--|---|
| 1. What are the implications of having separate and disconnected MIS for identification and registration among humanitarian and social assistance responders? | What MIS systems are currently in use (in Yemen / S Sudan / in crises globally)? | <ul style="list-style-type: none"> Operational | <ul style="list-style-type: none"> Stakeholder mapping Desk Research KII |
| | Has your organisation ever attempted to collaborate (or coordinate) with other organisations in the development and/or implementation of an MIS? If so, why have you done this and what has been the experience? | <ul style="list-style-type: none"> Political Operational | <ul style="list-style-type: none"> KII (global/ country) Stakeholder mapping |
| | What identity-related data do these systems collect, what is it used for, and how often is it updated? | <ul style="list-style-type: none"> Legal and ethical Operational Protection | <ul style="list-style-type: none"> KII |
| | How many individuals are registered and what is the maximum capacity of the system? | <ul style="list-style-type: none"> Operational | <ul style="list-style-type: none"> KII |

| | | | |
|--|--|--|--|
| | With regards to storing and sharing individual information, what level of consent is asked for and how? Do beneficiaries feel they have a real choice as to whether to share their personal data? What issues do beneficiaries who refuse to share their data face? Can they withdraw their consent? | <ul style="list-style-type: none"> • Protection • Legal and Ethical | <ul style="list-style-type: none"> • KII • Beneficiary interviews and focus groups |
| | How is this data collected, and from which sources? By whom and how often? | <ul style="list-style-type: none"> • Operational | <ul style="list-style-type: none"> • KII • Beneficiary interviews and focus groups |
| | Is this data collection proportionate to the use at country programme level? What does it mean for potential recipients in terms of amount of data collected? | <ul style="list-style-type: none"> • Protection • Legal and Ethical | <ul style="list-style-type: none"> • KII |
| | What data does your organisation share, with whom and for what purpose? Under which conditions? And what type of agreements? | <ul style="list-style-type: none"> • Legal and Ethical | <ul style="list-style-type: none"> • KII • Stakeholder mapping |
| | What are the barriers to sharing data (e.g. legal/ technical, etc.)? | <ul style="list-style-type: none"> • Legal • Operational | <ul style="list-style-type: none"> • KII |
| | What are the costs / challenges / benefits of separate MIS for ID and Registration? | <ul style="list-style-type: none"> • All | <ul style="list-style-type: none"> • KII • Beneficiary interviews and focus groups |
| | What would be the costs / challenges / benefits of linking MIS for ID and Registration? | <ul style="list-style-type: none"> • All | <ul style="list-style-type: none"> • KII |
| | What are the implications for organisations (e.g. efficiency, accountability, targeting) of linking MIS for ID and Registration? | <ul style="list-style-type: none"> • All | <ul style="list-style-type: none"> • KII • Beneficiary interviews and focus groups |
| | What are the costs, challenges and benefits to individuals of separate MIS for ID and Registration? | <ul style="list-style-type: none"> • All | <ul style="list-style-type: none"> • KII • Beneficiary interviews and focus groups |
| | What are the current or potential linkages between your MIS and government social protection MIS (incl plural)? | <ul style="list-style-type: none"> • Political • Operational | <ul style="list-style-type: none"> • KII • Stakeholder mapping |
| | What are the linkages between your MIS and humanitarian cash assistance? | <ul style="list-style-type: none"> • Political • Operational | <ul style="list-style-type: none"> • KII • Stakeholder mapping |
| | What are the strengths / weaknesses of your MIS for cash assistance ? | <ul style="list-style-type: none"> • Protection • Commercial | <ul style="list-style-type: none"> • KII |
| | What are the challenges and benefits of separate and disconnected MIS systems? What would be the benefits of further linkages between humanitarian and social protection cash assistance? | <ul style="list-style-type: none"> • All | <ul style="list-style-type: none"> • KII |
| 2. Does the use of different MIS for identification and registration in crises enable or challenge potential linkages between humanitarian cash assistance and social protection, and how? | How could further linkages between humanitarian and social protection cash assistance be developed? What would they look like? | <ul style="list-style-type: none"> • Operational • Commercial • Legal and Ethical | <ul style="list-style-type: none"> • KII |

| | | | |
|---|--|--|--|
| 3. Can different models of linking MIS improve the effectiveness of crisis response in protracted and recurrent crises? | What different models are there for linking humanitarian / and humanitarian and social protection MIS? | <ul style="list-style-type: none"> • Operational • Commercial • Legal and Ethical | <ul style="list-style-type: none"> • KII • Desk research |
| | What examples are there of humanitarian MIS aligned with/connected with/supporting a national system? What are the governance / regulatory dimensions of these models? | <ul style="list-style-type: none"> • Operational • Legal and Ethical | <ul style="list-style-type: none"> • KII • Desk research |
| | What would the implication of these models be for organisations (e.g. efficiency, accountability, targeting)? | <ul style="list-style-type: none"> • All | <ul style="list-style-type: none"> • KII |
| | What would the implication of these models be for individuals (e.g. access to benefits, control over data, privacy)? | <ul style="list-style-type: none"> • Operational • Protection • Legal and Ethical | <ul style="list-style-type: none"> • KII • Beneficiary interviews and focus groups |
| | | | |

The Department for International Development:
leading the UK government's fight against world poverty.

Department for International Development
22 Whitehall
London
SW1A 2EG
UK

and at:

Abercrombie House
Eaglesham Road East
Kilbride
Glasgow
G75 8EA
UK

Tel: +44 (0)20 7023 0000

Fax: +44 (0)20 7023 0016

Website: www.dfid.gov.uk

Facebook: www.facebook.com/ukdfid

Twitter: @DFID_UK

Email: enquiry@dfid.gov.uk

Public enquiry point: 0845 3004100 or +44 1355 84 3132 (if you are calling from abroad)

© Crown copyright 2020

Copyright in the typographical arrangement and design rests with the Crown. This publication (excluding the logo) may be reproduced free of charge in any format or medium, provided that it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright with the title and source of the publication specified.

Published by the Department for International Development