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

EXTERNAL BRIEFING NOTE

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

IMPLEMENTING PARTNERS

DAI Caribou Digital

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.

The views expressed in this document are entirely those of the authors and do not necessarily represent the UK Department for International Development'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

CONTENTS

LIST OF ABBREVIATIONS

API	Application Programming Interface
DCED	Donor Committee for Enterprise Development
DFID	Department for International Development
DPIA	Data Protection Impact Assessment
EU	European Union
FCAS	Fragile and Conflict Affected States
GDPR	General Data Protection Regulation
IATI	Independent Aid Transparency Initiative
IOM	United Nations International Organisation for Migration
ISPA	Interagency Social Protection Assessments
M4P	Markets for the Poor
MIS	Management Information System
NGO	Non-Governmental Organisation
SPIAC-B	Social Protection Inter-Agency Cooperation Board
UN	United Nations
UNHCR	United Nations High Commissioner for Refugees
VfM	Value for Money

1 BACKGROUND

This briefing note highlights the key observations and recommendations emerging from a longer study, which 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 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 is 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.

2 KEY OBSERVATIONS

- There is **potential value in leveraging shared data for increased coordination** amongst social protection and humanitarian actors. Those interviewed emphasised that they believed this would lead to reduced duplication of efforts, and potentially cost savings, as well as increased effectiveness due to greater insights into coverage and effectiveness, potentially allowing for better allocation of scarce resources. The majority of those interviewed noted that the promise of de-duplication and resultant cost-saving can be attractive for client donors, making interoperable MIS and/or the use of biometrics an attractive sell for implementers.
    - The majority of interviewees claimed that the principal driver for increased interoperability is efficiency. "Efficiency" was commonly translated as reduced costs and was often conflated with the broader concept of "value for money" (VfM) by many key informants. Other key VfM elements, such as effectiveness and equity, were mentioned by other key stakeholders, although with notably less frequency.

[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.

- **There is a trend towards consolidation of larger systems** in humanitarian contexts, even as the technology is still developing. Such systems are commonly viewed as proprietary, with implementing agencies offering donors a unique proposition when considering financing options. This has created a one-upmanship culture in a quest to prove who can appear the most innovative (as a way to promote the organisation and its services) and therefore dominate the market.
- There is a commonly held **assumption that centralised humanitarian transfers systems may form the basis of longer-term or government-led social protection systems**. However, these assumptions should be challenged for often not adequately protecting rights to privacy and data protection, with potential consequential effects on other fundamental rights of beneficiaries. The need to safeguard the broad range of fundamental rights that are impacted by privacy and data protection violations is referred to in this report as "**protection**".
- **Technology and data processing have uses and consequences that at present are poorly understood by many humanitarian practitioners, project managers and policy advisers**. This includes a lack of understanding of organisation and grantee approaches to data protection. Very few of those interviewed were able to articulate either their own organisations' or their grantees' approach to data protection. For most, there is a pattern of delegating understanding and responsibility to grantees, or to – often remotely based – more senior leadership within the organisation. This underscores the importance of ensuring staff at all levels are aware of and understand such policies. If they exist but are not known and applied, they will not be effective.
    - In many national and international NGOs there was a high level of insecure data collection, processing, and storage practices such as the use of platforms in insecure ways, including unencrypted Excel and Google Sheets and the sharing of personally identifiable information without permission.[3]
- **Relevant experiences and lessons** from the use of personal data for health, social, political, commercial, security, and military purposes **are not commonly translated and applied**. 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 by subjecting beneficiaries to significant, unnecessary risk.
- **The inadvertent and deliberate leaking and sharing of personal and anonymised data is 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. Even the most secure cryptographic technologies are at risk with contemporary computing advances. Recommendations to address this, such as implementing data minimisation measures, are discussed below.

3 RECOMMENDATIONS AND WAYS FORWARD

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.

3.1 Integration and interoperability

[3] Sending personal data via email is almost never recommended as general best practice, as emails can be intercepted and hacked and are not encrypted (except for ProtonMail). Password protecting an excel document, for instance, is not sufficient to protect data, particularly in contexts where digital hygiene and cybersecurity awareness are low.

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 any given 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 on types of MIS). Examples of standards for data exchange include the Humanitarian Exchange Language (HXL)[4], 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'[5] – 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).

3.2 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.[6]

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:

- 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).

3.3 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 countries

[4] https://hxlstandard.org/, currently used by organisations such as UNHCR, IOM

[5] 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

[6] Digital Dignity in Practice: Existing Digital Dignity Standards, Pursuing Digital Dignity and Current Gaps in Digital Dignity

where robust domestic legal and regulatory frameworks are absent) 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 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.

3.4 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)[7] and Interagency Social Protection Assessments (ISPA[8]). 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.

3.5 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

[7] https://socialprotection.org/institutions/social-protection-inter-agency-cooperation-board-spiac-b

[8] https://ispatools.org/

penalty). This could come and/or from a voluntary scheme which sets a standard and encourages aid agencies to meet it.

3.6 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 Data Protection Impact Assessments (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. To achieve critical mass this needs joint agreement and adoption by EC, US, UK and WB at a minimum, with other donors financing such systems adding weight to this approach (e.g. DFAT, Germany, Netherlands). Agreement of the WB to this is particularly relevant given its support to developing national systems in transition countries (including for example in Yemen, South Sudan), and its clients including host governments and (increasingly in the light of IDA18 and the Famine Action Mechanism, FAM) UN agencies. The EC, US and UK all fund NGOs registered in their sovereign jurisdiction and enforcement of data protection standards by these organisations worldwide would lead to near universal adoption. As a starting point, the World Bank ID4D programme's 'Principles on Identification for Development[9]' – 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 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.[10]

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.[11] When addressing any conflict between domestic and international law, an approach that focuses on the fundamental rights underlying the need for

[9] The World Banks 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.

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

[11] Kuner, C. 'International Organizations and the EU General Data Protection Regulation', International Organizations Law Review 16 (2019) 158-191, at 165

data protection, rather than a narrow focus on technical compatibility between the potentially conflicting legal systems, is desirable.[12]

3.7 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 standards[13], and the Donor Committee for Enterprise Development (DCED) standard for Making Market systems work for the Poor (M4P)[14].

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.

3.8 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 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.

3.9 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, 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

[12] See, for example, *NJCM cs/ 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.

[13] https://spherestandards.org/

[14] https://www.enterprise-development.org/

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 choose to utilise biometric data, they must ensure that their choice of biometric data is appropriate and that essential safeguards are in place.

3.10 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.[15] 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.

3.11 Risk management

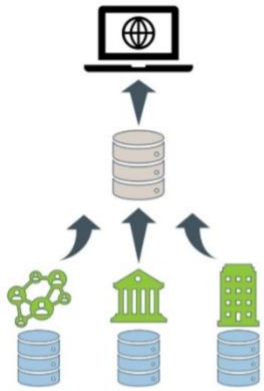
[15] See, for example, ICRC, Handbook on Data Protection in Humanitarian Action (July 2017), Chapter 3: Legal bases for personal data processing

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.

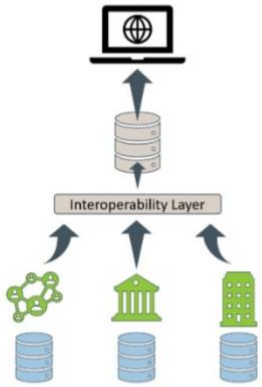
4 ANNEX: TYPES OF MIS

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).

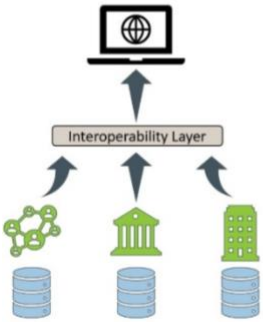
Throughout this report, we refer to different types of system architecture, in order to identify how fragmentation, one "super" single system, and different forms of interoperability (centralised vs federated) may impact upon the effectiveness of humanitarian aid and social protection programming. The graphic below defines these different types - single database, federated[16], and centralised.



A single database structure is one in which all participating organisations use one database and system to store all of their data. This is highly impractical from a technological and managerial view given the variance in implementer and donor organisations requirements, timeline of implementation (particularly in crisis), and the highly sensitive nature of data collected.



A centralised system is one in which participating systems copy some or all of their data to a central repository where it is organised and stored based on a common data model. In this case, each independent system still maintains their own database but makes available some or all of their data to a single central database system.



A federated system is one where independent organisations maintain control of their source data and permit participating systems on demand access to some or all their data via a central user-facing application. Mcleod and Heimbigner define a federated database system as one that defines the architecture (technical setup/design) and interconnections of databases to minimise central authority yet support sharing and coordination among independent database systems. This is often subject to a MoU and Data Sharing Agreements.

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

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)

Published by the Department for International Development