A Principled Approach to Data Management

Lessons Learned from Medair's Experience in Lebanon Using Last Mile Mobile Solutions

Joel Kaiser / Rob Fielding

Introduction

Over the past 25 years Medair has developed expertise delivering emergency assistance to disaster and conflict-affected populations in need of safe water and sanitation, hygiene promotion, health and nutrition services, and secure shelter. Since its first cash transfer programme in 2009, Medair has made a concerted effort to realise the benefits of mobile digital technologies in humanitarian programming. The industry trend in this direction has been accelerated by the rapid increase of mobile phone subscriptions in developing countries. With the spread of mobile connectivity, digital technologies are bringing to humanitarian aid workers an unprecedented capacity for data collection and analysis, which can improve service delivery in humanitarian crises (see Tafere *et al*, pp. 42-44). The most effective use of mobile digital technologies to date for Medair has been via Last Mile Mobile Solutions (LMMS).

LMMS is a software system designed by aid workers that enables humanitarian staff to register people in the affected population, and digitally manage a distribution of relief materials or resources to them. To do this, LMMS has replaced paper-based project forms with digital forms on handheld devices, and has in this way fully automated the process of identifying and tracking the quantity of items, such as cash, hygiene kits, or food rations, that are to be distributed per beneficiary based upon project specifications. LMMS accomplishes this by issuing beneficiaries with computer-readable identity cards. Once registered into the system, beneficiaries can be transitioned into projects using the same identity card, thereby avoiding multiple data entries over time. LMMS strengthens the security and control over the inventory of relief items during a distribution and enables improved accountability through photo verification of households or their authorised proxies. It also supports the added benefit of real time analysis and reporting of relief activities involved in the project.

Using LMMS in the Syrian refugee response has enabled Medair field teams in Lebanon to distribute emergency shelter solutions customised to diverse groups of Syrian refugees without compromising accountability or security of relief items.

Benefits of using software for aid delivery in Lebanon

Medair's emergency response team arrived in Lebanon and conducted emergency assessments and crisis mapping for two weeks in the Bekaa Valley in order to locate and identify refugee families living in informal tented settlements. These assessments not only confirmed the vulnerabilities of a growing demographic, but also the rapid rate of data turnover resulting from the on-going displacement of refugees. The multitude of informal refugee settlements, each with unique needs and assets, created a complex and dynamic context in which the accurate and timely collection and management of assessment data became paramount.

Medair field teams realised that static 'snapshots' of individual settlements could not adequately inform the agile humanitarian operation required by the crisis, and therefore trained assessment teams to perform continual, rolling assessments, supported using Open Data Kit (ODK). This form filling software is an open source system that substitutes the traditional clipboard. It allows conducting surveys or questionnaires and collecting quantitative and qualitative data in different languages. In Lebanon, national staff collected data in Arabic for identifying the most vulnerable population and creating a list of beneficiaries and their needs. Subsequently they were able to download the information in both English and Arabic in CSV format back in the office. ODK also enabled the real-time mapping of data using ArcGIS (a geographic information system), and the information produced was shared with other actors in the humanitarian community.

Currently, beneficiary identification and distribution teams cover 173 informal settlements in Medair's areas of operation across West and Central Bekaa with shelter and non-food-items needs. This amounts to aid for approximately 29,000 beneficiaries living in 4,611 tents according to latest data collected and mapped using ArcGIS as part of the Countrywide Inter Agency Mapping Platform Version 3.[99]

This software also allowed Medair to use the information for identifying trends more accurately and gaining a more nuanced understanding of the capacities and needs of newly arrived refugees. This understanding enabled the Medair team in Lebanon to customise their projects for diverse refugee groups using a 'relief items catalogue'. Based on the data gathered at the assessment stage, Medair catalogued all relief items available to beneficiaries factoring different needs, or family size or composition, for example. Although beneficiaries do not get to choose the items from a list, having rapid access to up-to-date information has allowed Medair to tailor the distribution of aid to the actual needs of the most vulnerable populations, and provide a faster and more efficient assistance. This was particularly useful given the very fluid situation in which displaced populations were constantly moving (see Porcaro and Walker, p. 35).

At the distribution stage, Last Mile Mobile Solutions comes into play. LMMS enables digital tracking and control of relief items, and streamlines the distribution process, allowing teams to undertake distributions that would otherwise be too complicated and cumbersome to support. Combinations of relief items, such as vinyl sheeting, plastic sheeting, timber of various sizes, plywood sheets, hand tools, and NFI materials such as fire extinguishers, mattresses, blankets, baby kits and kitchen sets can be distributed within a single settlement.

The initial deployment of LMMS in Lebanon focused on distribution projects including shelter and new refugee arrival non-food-items kits as well as the distribution of fire prevention and mitigation equipment. It is anticipated that both WASH and health projects will also benefit from one centralised beneficiary database and registration system using one centralised multi-sectorial assessment and distribution team, with supporting technical staff for each sector. To avoid duplication where uncertainty arises, the Medair team in Lebanon also benefit from being able to crosscheck beneficiaries' names in the field using the LMMS server. Along with the benefit of having instant access to beneficiaries' previous distribution records and knowing exactly what they have received and when, the team can instantly address complaints and distribution inaccuracies raised by beneficiaries.

Handling sensitive information appropriately

The most sacred tenet in data storage is to correctly recognise (and protect) sensitive information, which for humanitarians amounts to any data that directly links to individuals in an affected population. This data must only exist in a limited domain, since any breach could radically jeopardise the personal security of many people and thereby undermine the principle of 'Do No Harm' (see Porcaro and Walker, p. 36). In this way, aid agencies should approach the topic beginning with the protection principles of the Sphere Handbook, specifically the section on managing sensitive information.[100] The Sphere Handbook recommends that humanitarian agencies have clear policies and procedures in place to guide staff on:

1. How to respond to a security breach.
2. How to refer sensitive information, such as incident reports and trend analyses.
3. How data may and may not be shared.
4. How to collect data, including seeking consent to gather information and providing a rationale for why data is being collected.

The data collected by Medair using ODK and LMMS includes vulnerability and demographic indicators, and is therefore sensitive. Add to this fact the sectarian nature of the conflict in Syria, and the security of beneficiary data becomes of paramount importance. The risk to beneficiaries is most related to the use of

[99] Howe, A. (2014). LMMS *Lessons Learned in the Syria Regional Crisis*. Beirut: Medair.
[100] Schenkenberg van Mierop, E. and Haenni Dale, C. (2011). Protection Principles. In *The Sphere Project: Humanitarian Charter and Minimum Standards in Humanitarian Response*. 3rd ed. Rugby: Practical Action. pp. 29-47.

data for purposes other than those for which they were collected, such as the sharing with or selling of data to third parties, and the inherent security risks of sending and receiving sensitive data via mobile phones.[101] Reports of security breaches at large online companies such as eBay, and even security and anti-virus providers such as Kaspersky and Symantec, offer additional proof that the challenges related to digital data collection and storage are a risk for even the most technologically advanced companies. For humanitarian organisations operating on tight budgets, this challenge can appear insurmountable (see Gilman, p. 9).

The context of the Middle East also presents unique challenges to data management and security. For example, it was originally planned to export monthly list files for cross checking with UNHCR's database to ensure that beneficiary registration information on LMMS was up to date. However, difficulties with the data export process were encountered because the digital tools used to extract the data from the LMMS server did not support Arabic script. Quick workarounds had to be devised in order to fix an otherwise simple checking process.

Adapting Cash Learning Partnership (CaLP) principles to data management

To date, there is no widely recognised guidance on data management in humanitarian operations. However, in an effort to operationalise the Sphere guidance on managing sensitive data, the Cash Learning Partnership (CaLP) has published a set of principles and operational standards for the secure use of personal data in cash transfers. Medair chose to use the CaLP principles, despite the programme not involving cash transfers, out of the belief that they present the best guidance on data management to date. The principles were developed to address the risks associated with the collection, storage, use, and disclosure of the personal data of beneficiaries. They were designed to serve as a minimum standard to ensure the protection of beneficiaries' privacy and personal data, which is defined as 'any data that directly or indirectly identifies or can be used to identify a living individual'.[102]

The principles are based on numerous international and national instruments which enshrine data protection principles, and derive guidance from human rights standards related to privacy and data protection. These are strongly linked to individual autonomy and dignity. The principles are necessary, particularly since a CaLP survey indicated that a majority of respondents reported that their organisation lacked internal data management guidelines. The principles also introduce a Privacy Impact Assessment[103] that serves as an excellent means to inform the planning and implementation of data management. The final section of this paper describes Medair's experience interacting with these principles in the management of sensitive beneficiary data in Lebanon.

> The version of the Privacy Impact Assessment (PIA) adapted by CaLP was initially developed by the U.S. Department for Homeland Security (DHS). DHS considers the PIA process 'inherently necessary for all U.S. Federal Government programmes since 2002.' 'The process of a PIA is to demonstrate that programme managers and system owners have consciously incorporated privacy protections throughout the development life cycle of a system or programme. This involves making certain that privacy protections are built into the system from the initiation of the development, not after the fact, when they can be far more costly or could affect the viability of the project.'

Lessons learned: implementation of data management principles

Medair's digitally collected beneficiary data is significantly more secure than using Excel spreadsheets or paper-based beneficiary lists. Of course, Medair is aware that no system is foolproof and that it is only as good as the personnel who implement it (see Byrne, b. pp. 56-58). To this end, Medair has created Standard Operating Procedures (SOPs), which are periodically refined based on theoretical anticipation of the strengths and weaknesses of the process as implemented, and based on trial and error as experienced by teams in the field. This has produced several lessons learned which highlight that a mutually trustworthy relationship with the beneficiaries is critical when employing digital technologies, and that time spent explaining the use of the technology, supported by easily understood leaflets, has garnered this requisite trust among refugee populations (see Porcaro and Walker, p. 33).

[101] Gallagher, I. (2011). Egyptian police use Facebook and Twitter to track down protesters' names before 'rounding them up'. *Mail Online*. Available from: http://www.dailymail.co.uk/news/article-1354096/Egypt-protests-Police-use-Facebook-Twitter-track-protesters.html. [Accessed 10 July 2014].

[102] The Cash Learning Partnership. (No date). Protecting Beneficiary Privacy. p. 5. Available from: http://www.cashlearning.org/downloads/calp-beneficiary-privacy-web.pdf. [Accessed 1 Sept. 2014].

[103] *Ibid*.

Digital technologies may be difficult to understand and trust for some communities, and key for their success is that beneficiaries understand that personal information is not shared outside the agency (see Porcaro and Walker, p. 36). Medair field teams are very clear in delivering this message, and explain the advantages that these technologies have in protecting people's confidentiality. As mentioned before, an added advantage of LMMS is that plastic card IDs substitute the traditional finger printing signature, which can be seen as impersonal and demeaning by some beneficiaries. LMMS allows a more dedicated approach by aid agencies, which in turn helps communities trust the technology behind it (see Tafere *et al*, pp. 42-44).

Cash Learning Partnership principles for data management: Medair's experience

The principles published by CaLP are paraphrased below, along with a summary of Medair's experience of applying them.

1. *Respect that collection of personal data represents a potential threat to beneficiary privacy.*

This principle is fundamental to the training of Medair's data collection teams. The teams are identified to the refugee community as the sole authority for the collection of personal data, which minimises the risk of fraudulent actors seeking personal data in the name of Medair. A lesson learned is to include additional information on the programme leaflet explaining the use of personal data and steps taken to secure it, as well as the redress mechanism refugees have access to in the event they feel their privacy has been compromised.

2. *Protect by design by ensuring that privacy and protection of beneficiary data are designed into the programme rather than as 'add-ons'.*

This has been highlighted as an area of improvement. For example, there was no specific SOP to address a beneficiary who opted out of providing data for LMMS, and an *ad hoc* work-around had to be created. Undertaking a Privacy Impact Assessment (PIA) would have identified holes in SOPs such as this. However, the SOPs did successfully address database backup, encryption, protection and partition; so for example, those collecting data never have access to full beneficiary records, while multiple verifications protect database backups.

3. *Understand data flows within the programme as well as among organisations in order to mitigate the risks.*

Data Sharing Agreements (DSA) among Medair and third parties, which have been in place from the onset of the programme, define expectations concerning confidentiality of the shared data. However, the difficulty of enforcing such agreements remains and as such, trust among partners becomes critically important.

4. *Ensure the quality and accuracy of the personal data by keeping it up to date and relevant, and ensure that the amount of data is not excessive in relation to its use.*

Medair discovered that very frequent spot checks are necessary to account for both errors by data collection staff and beneficiaries providing incorrect data. By building data triangulation into the process through, for example, comparison with refugee registration papers, these spot checks can be facilitated efficiently. However, a lesson learned was to find a better process for identifying beneficiaries who have moved outside the programme area, since this oversight will ultimately undermine the programme's exit strategy.

5. *Obtain consent or inform beneficiaries as to the use of their data.*

All beneficiaries are informed about the programme and asked for their consent to use and share their personal data. A lesson learned indicated the need for improved monitoring to ensure data collection teams are taking the required time to receive informed consent, since some may proceed through the questioning too rapidly for beneficiaries to comprehend the implications of their participation.

6. *Security standards should be in place for each stage of collection, use, and transfer of data.*

Medair maintains a security focal point who is in sole possession of the database password (with failsafes in place). All data is password-protected and encrypted. As stated earlier, DSAs regulate the use of data for third parties, though monitoring and enforcement of data usage by third parties is not practiced.

7. *Disposal of beneficiary data should be part of an exit strategy; data should not be held longer than required without a clear rationale.*

A review indicated a need for a more robust exit strategy beyond destruction of hardware. Personal data held in the cloud has not been addressed and indeed, the footprint of this data is not clearly understood.

8. *An accountability mechanism should enable beneficiaries to address concerns or complaints about the use of their personal data.*

Although Medair operates a hotline for beneficiary complaints, a review found that beneficiaries were not specifically informed that they have a right to follow up on the use of their data, and that this hotline is one such method. LMMS does enable Medair to track information that has been shared, and with whom. Another lesson learned was to establish an SOP for reporting data loss.

Conclusion

Medair believes that the benefits of digital tools such as LMMS outweigh the risks so long as a principled approach to data management is adopted. The benefits in increased efficiency and effectiveness with digital data entry are tangible: on average a competent and efficient data-entry assistant is able to complete 6 to 8 household registrations per hour using LMMS, or approximately one household registration every 7.5 to 10 minutes.[104] This figure is comparable to paper-recorded data collection, until the lengthy data entry component is factored in and the number of errors that often occur when data is typed into Excel spreadsheets or handwritten onto paper forms. This saving of time directly translates into financial savings in the form of reduced workloads and the need for fewer staff. Such evidence in support of the increased use of digital data collection tools suggests that greater emphasis should be paid to developing consensus and training in data management principles. This would help to ensure that humanitarian agencies located in developing countries, often operating with few resources, are also able to realise the benefits of digital technologies.

[104] Howe, A. (2014). *LMMS Lessons Learned in the Syria Regional Crisis.* Beirut: Medair.

European Interagency Security Forum (EISF)

EISF is an independent network of Security Focal Points who currently represent 66 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice.

EISF was created to establish a more prominent role for security risk management in international humanitarian operations. It facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to become a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Agency for Development and Cooperation (SDC), the Department for International Development (DFID) and member contributions.

www.eisf.eu

Disclaimer

EISF is a member-led grouping and has no separate legal status under the laws of England and Wales or any other jurisdiction, and references to 'EISF' in this disclaimer shall mean the member agencies, observers and secretariat of EISF.

While EISF endeavours to ensure that the information in this document is correct, EISF does not warrant its accuracy and completeness. The information in this document is provided 'as is', without any conditions, warranties or other terms of any kind, and reliance upon any material or other information contained in this document shall be entirely at your own risk. Accordingly, to the maximum extent permitted by applicable law, EISF excludes all representations, warranties, conditions and other terms which, but for this legal notice, might have effect in relation to the information in this document. EISF shall not be liable for any kind of loss or damage whatsoever to you or a third party arising from reliance on the information contained in this document.

Editors

Raquel Vazquez Llorente and Imogen Wall.

The editors welcome comments and further submissions for future publications or the web-based project. If you are interested in contributing, please email eisf-research@eisf.eu. Imogen Wall can be contacted at imogenwall@hotmail.com.

Acknowledgments

The editors would like to thank Lisa Reilly, EISF Coordinator, for her input and advice, and especially for her comments on the initial drafts. We would also like to extend our gratitude to Tess Dury, for her research support at the initial stages of the project, Brian Shorten for sharing his expertise with us, and Crofton Black for his early guidance and, as always, his continuous support.

Suggested citation

Vazquez Llorente R. and Wall, I. (eds.) (2014) *Communications technology and humanitarian delivery: challenges and opportunities for security risk management*. European Interagency Security Forum (EISF).

Cover photo: Mary Kiperus, community health worker, uses a mobile phone for reporting to the local nurse. Leparua village, Isiolo County, Kenya. February, 2014. © Christian Aid/Elizabeth Dalziel.

Available at
www.eisf.eu

Other EISF Publications

If you are interested in contributing to upcoming research projects or want to suggest topics for future research please contact **eisf-research@eisf.eu**.

Briefing Papers

Security Risk Management and Religion: Faith and Secularism in Humanitarian Assistance
August 2014
Hodgson, L. et al. Edited by Vazquez, R.

Security Management and Capacity Development: International Agencies Working with Local Partners
December 2012
Singh, I. and EISF Secretariat

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012 – *Sp. and Fr. versions available*
Persaud, C. Edited by Zumkehr, H. J. – EISF Secretariat

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011 *Fr. version available*
Glaser, M. Supported by the EISF Secretariat (eds.)

Abduction Management
May 2010
Buth, P. Supported by the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Buth, P. Supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Ayre, R. Supported by the EISF Secretariat (eds.)

Reports

The Future of Humanitarian Security in Fragile Contexts
March 2014
Armstrong, J. Supported by the EISF Secretariat

The Cost of Security Risk Management for NGOs
February 2013
Finucane, C. Edited by Zumkehr, H. J. – EISF Secretariat

Risk Thresholds in Humanitarian Assistance
October 2010
Kingston, M. and Behn O.

Joint NGO Safety and Security Training
January 2010
Kingston, M. Supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Finucane, C. Edited by Kingston, M.

Articles

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing them
March 2012
Van Brabant, K.

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Van Brabant, K.

Whose risk is it anyway? Linking Operational Risk Thresholds and Organisational Risk Management
June 2010, (in Humanitarian Exchange 47)
Behn, O. and Kingston, M.

Risk Transfer through Hardening Mentalities?
November 2009
Behn, O. and Kingston, M.

Guides

Security Audits
September 2013 – *Sp. and Fr. versions available*
Finucane C. Edited by French, E. and Vazquez, R. (Sp. and Fr.) – EISF Secretariat

Managing The Message: Communication and Media Management in a Crisis
September 2013
Davidson, S., and French, E., EISF Secretariat (eds.)

Family First: Liaison and Support During a Crisis
February 2013 *Fr. version available*
Davidson, S. Edited by French, E. – EISF Secretariat

Office Closure
February 2013
Safer Edge. Edited by French, E. and Reilly, L.
– EISF Secretariat

Forthcoming publications

Office Opening Guide