WFP
wfp.org
vam
food security analysis

Conducting Mobile Surveys Responsibly

Marie Enlund, WFP

A Field Book for WFP Staff

The field book outlines the main risks for staff engaged in mobile data collection and helps promote responsible data collection /storage/sharing in the very complex environment in which WFP operates

In collaboration with the International Data Responsibility Group (IDRG) and the Leiden University Centre for Innovation

May 2017

Conducting Mobile Surveys Responsibly - A Field Book for WFP Staff

©May 2017, World Food Programme (WFP), Vulnerability Analysis & Mapping (VAM)

This field book has been prepared by the United Nations World Food Programme (WFP)
for use by staff and its partners. All rights are reserved.
Reproduction is authorized, except for commercial purposes, provided that WFP is acknowledged as the original source.

United Nations World Food Programme
Via Cesare Giulio Viola 68/70, Parco de' Medici 00148, Rome - Italy

Vulnerability Analysis & Mapping (VAM)
Chief: Arif Husain
Tel: + 39 06 6513 2014
e-mail: arif.husain@wfp.org

Acknowledgements: contributions from Jos Berens (Leiden University), JM Bauer, Michela Bonsignore, Perena Sekhri and Angie Lee (WFP).

THE BELGIAN DEVELOPMENT COOPERATION .be

외교부
Ministry of Foreign Affairs

KOICA
Korea International Cooperation Agency

국제질병퇴치기금
Global Disease Eradication Fund | KOREA

Kingdom of the Netherlands

Contents

Introduction and background

1

Mobile data collection for field staff...

Faster

Cheaper

Safer

In 2016, mVAM conducted ***250,000 surveys*** in over ***30 countries***, asking nearly ***4 million questions***.

...also entails privacy and security risks

This field book outlines the main risks for staff engaged in mobile data collection and helps promote responsible data collection/storage/sharing in the very complex WFP environment

SECTION I Introduction and background

Mobile data collection is usually faster and cheaper than face-to-face alternatives. It is also safer for field staff. Thanks to mobile technology, WFP and other humanitarian agencies are now able to gather more information than ever before. WFP has been collecting increasing amounts of information by mobile phone as part of its mobile Vulnerability Analysis and Mapping (mVAM) project: in 2016, mVAM conducted 250,000 surveys in over 30 countries, asking nearly 4 million questions. Mobile technology offers a tremendous opportunity to communicate better with people in humanitarian settings. However, these new capabilities also entail privacy and security risks for people and the communities where mobile surveys are implemented.

Reports of ‘data breaches’ – when data is accessed, copied and/or destroyed by an unauthorized third party – often appear in the news.[i] In December 2016, the media revealed details of the largest breach so far, when data from more than 1 billion Yahoo users was compromised in 2013.[ii] A breach of even a fraction of this size would be entirely unacceptable for a humanitarian organization whose mission it is to protect the world’s most vulnerable people.

Even if sensitive raw data is not leaked, there are still other risks associated with the collection, storage, processing and distribution of digital data on vulnerable people. If the data is flawed or biased, it could misinform operations. If information on the location of WFP’s beneficiaries is shared at too low a level of aggregation in an unstable environment, it might make beneficiaries or WFP staff a target for malicious actors. Uncertainty about the future capabilities and limitations of analytical tools makes it increasingly difficult to assess the sensitivity of datasets in the first place.

WFP first circulated a corporate policy on data privacy and security in 2016. To implement this policy through practical guidance at the field level, the organization has issued this guide for field staff in collaboration with the International Data Responsibility Group.[iii] The field book outlines the main risks for staff engaged in mobile data collection and helps promote responsible data collection/storage/sharing in the very complex environment in which WFP operates.

Key principles and definitions

2

1. Responsible data

2. Lawful and fair data collection and processing

3. Personally Identifiable Information (PII) or personal data

4. Demographically Identifiable Information (DII)

5. Special vulnerabilities

6. Data Controller

SECTION 2 Key principles and definitions

Responsible data – The duty to ensure people's rights to consent, privacy, security and ownership around the information processes of collection, analysis, storage, presentation and reuse of data while respecting the values of transparency and openness.[iv]

Lawful and fair data collection and processing – This is the overarching principle governing the whole data processing cycle, from collection to disposal. It means respect for human rights and do no harm: people should not be exposed to rights violations, harm, or undignified or discriminatory treatment as a consequence of personal data collection and processing. Where applicable, data collection and processing must be done in compliance with local data protection laws and regulations.

Personally Identifiable Information (PII) or personal data – Personal data is any information relating to an individual that identifies them (a direct identifier)[v] or that can be used to identify them (an indirect identifier). While a telephone number[vi] alone may seem harmless because it does not immediately allow for the identification of a person, it can easily be used to trace someone's personal information.

Demographically Identifiable Information (DII) – DII is aggregate data that includes personal information and often refers to subgroups within the population. In addition to a respondent's displacement or refugee status, WFP maintains listings of people's names, which could also be used to identify people's religious or ethnic affiliation. This in turn can identify the location of a concentration of people of a specific religion or ethnicity — a serious consideration in conflict settings.

Data about gender, age and wealth proxies (e.g. housing or toilet type) is also often collected, and although this might not be considered personal data, it can still create risk.[vii]

Special vulnerabilities – These are socio-economic characteristics that may lead to exclusion, harm and/or biased information. For example:

Age: disabilities, debility or particular social norms that may be attached to age could impede people's participation in and/or full understanding of a survey.

Gender: household and community power dynamics, socially ascribed roles, and the undue influence of husbands, fathers, family members and community leaders on women and young girls may lead to harm, discrimination or self-censored and/or incorrect answers. The same risks exist for men and young boys in matrilineal societies.

Other diversity factors: language ability, illiteracy, disability, sexual life, political affiliation, ethnicity, and religious and cultural beliefs may adversely affect people's free participation in a survey.

Data Controller – When WFP implements surveys, whether in-house or through an external agency or service provider, WFP is the data controller. The organization is the primary custodian of personal data and determines the purposes and manner in which personal data is processed. WFP's status as the data controller entails obligations that are described in this guide. The position of data controllers is also outlined in the forthcoming European General Data Protection Regulation (GDPR), which although not applicable to all of WFP's operations, can provide direction for resolving particular data responsibility issues.[viii]

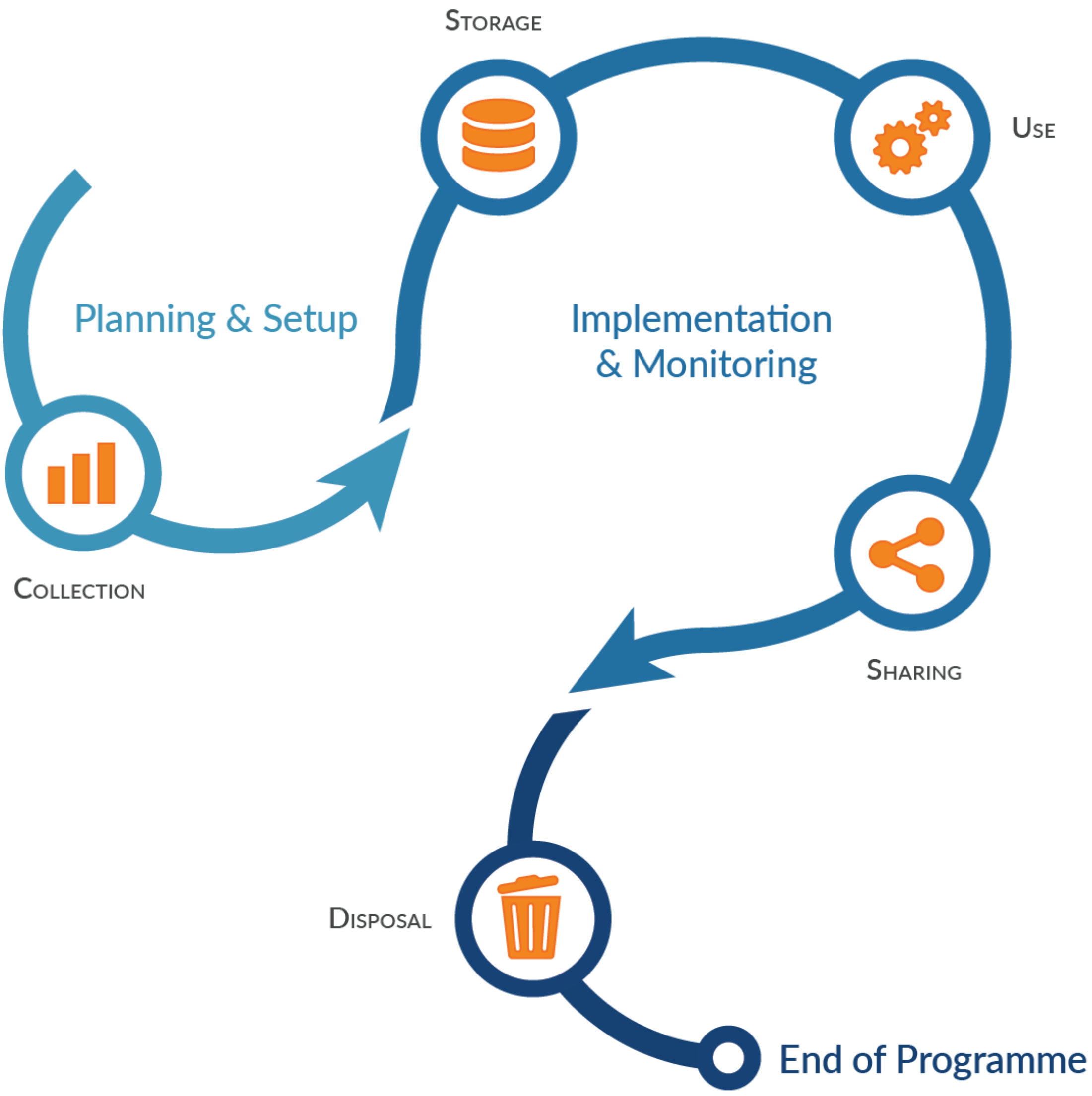
The data responsibility chain

3

At each step of the humanitarian data lifecycle, there are risks to data security that can potentially harm people, communities and even WFP and its partners. The table below lists some of the most likely risks and harms that can occur before, during and after collecting data.

Step	Risk	Potential harm
Before collecting data	• Design of survey is vague and unnecessary PII or DII is collected • Data collection is at odds with regulatory or legal provisions • WFP contracts unprofessional third party service provider(s)	• Conflict with individuals, communities or authorities; loss of trust and credibility • Lawsuits • Poor quality of service by third party providers, harm to WFP's reputation
Data collected	• Consent is not requested before data collection • Lists with personal information (names and numbers) are divulged • Overkill – too much information is collected along with the phone number, allowing people to be identified according to their answers • People in conflict settings could be exposing themselves to risk by taking a phone call (e.g. phone 'bans' in some conflicts) • Phone calls or text messages are monitored and read by parties to a conflict	• Misunderstanding of the purpose of the survey (e.g. WFP operators perceived as 'spies') • People are targeted for phone fraud (e.g. third parties impersonating WFP) • People could believe they would lose assistance if they didn't sign up • Potential for gender-based violence (e.g. unknown male operator calls a married woman or vice versa)
Data analysed	• Geographic concentrations of an ethnic, religious or other minority group are identified • Data is mis-aggregated	• A military actor analyses and uses data to find people or communities to attack • Individuals or communities can be wrongly documented or categorized, leading to discrimination or exclusion
Data stored, shared or disposed of	• Personal data is not stored in a safe, password-protected location and/or is subject to a data breach or malicious attack • Data records are leaked through negligence or theft • Data records are not disposed of at the end of the project	• PII or DII is leaked, used against specific target groups or exploited in different ways

The data responsibility chain and its place within the programme cycle can be illustrated as follows:



Note that the data responsibility chain is only as strong as its weakest link, and it hinges on the ability of an organization to manage risk cases throughout data lifecycle as part of its data preparedness[ix] plans. Proper action can mitigate many of the risks identified above, and the following sections contain a step-by-step guide on how to put safeguards in place.

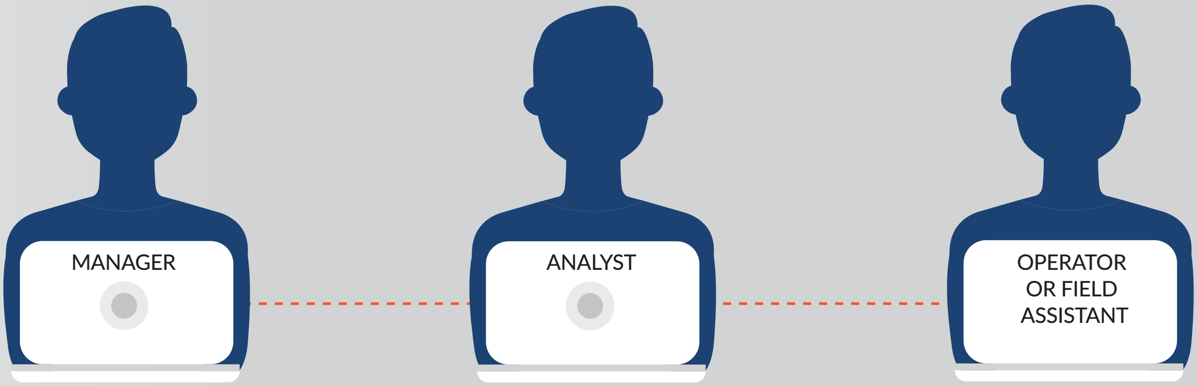
SECTION 3 The data responsibility chain

Lucia Casarin, WFP

BOX 1

Data preparedness, accountabilities and roles to promote responsible data use

Effective responsible data use depends upon a clear sense of the individuals or groups that are accountable or tasked to oversee the implementation and enforcement of the policy. For this reason, any data policy should clearly determine and describe responsibilities and roles. Some policies WFP has examined centralize this function, while others take a more decentralized approach. The general sense is that a decentralized or distributed approach is more effective, allowing a broader community to take part in decision-making, but the ultimate structure and delineation of duty must be based on the particular needs of the organization and feedback from its user community and other stakeholders.



should never ask for PII and should decide when analysis of DII is appropriate. Clears analytical reports. Consistently reviews what data is authorized by whom and for what purpose throughout the project. **Should be accountable for managing the risks of DII analysis. Should conduct randomized data security audits** (e.g. pull out PII logs and check).

should not have access to PII nor ask for PII from a third party provider and **should not attempt to re-identify anonymized data. Should not share DII-based analysis unless manager clears it.**

needs access to PII to call people. **Should never share PII with anyone. Should adhere to Standard Operating Procedures (SOP)** for data security at all times.

SECTION 3 The data responsibility chain

3.1 Before collecting data

Review existing domestic legislation – Especially for WFP's local partners, local legislation may pose challenges when collecting sensitive data. For example, applicable domestic laws may contain provisions that could force WFP's local partners to disclose personal data in their possession to the government. Under such circumstances, WFP should only collect data if it is comfortable with the data being shared with the government.

Ensure your data collection has a specified purpose – Given the sensitivities and risks of collecting, storing and sharing data, personal and demographic data should never be collected indiscriminately. The purpose of data collection and processing must be clear and unambiguous and must be defined prior to data collection.

Data minimization: collect data on a need-to-know basis only – Collected data must be limited to the minimum necessary to achieve the objective in order to avoid unnecessary and potentially harmful intrusion into people's private lives. In particular, information about people's ethnicity, political opinions, religious beliefs or health or sexual orientation/choices should be strictly avoided unless absolutely necessary to the purpose of the survey. This information is not usually collected in WFP's food security surveys.

Conduct a Privacy Impact Assessment – Before undertaking data collection in a country, WFP should conduct a Privacy Impact Assessment (PIA)[x]: this is a systematic analysis of all the factors (including legal, operational and environmental) that may lead to rights violations or abuse. The PIA determines strategies to mitigate these risks, and it can be conducted by a WFP VAM Officer in partnership with government and other key stakeholders. The PIA should identify any groups that are particularly vulnerable given the context in which the data is to be collected. This will allow WFP to maintain a higher protection standard for data that could lead to an individual being identified as a member of a vulnerable group; alternatively, WFP could decide not to collect personal or demographic data at all. The PIA should take into account the special vulnerabilities mentioned in Section 2.

Understand and engage with local context – If possible, get advice from a protection specialist before starting a survey (this can also be part of the PIA). Some of the best practices are as follows:

- Engage with the community about major risks related to the proposed data collection. This can be done by interviewing members of the community and through a quick literature review on the mobile phone landscape (e.g. mobile phone ownership and usage rate, social and gender norms) in the country.

- Work with a community-based organization (CBO) or NGO in the community that can sensitize people about the activity. It is vital to engage with the community before collecting data. If there are protection risks, WFP needs to inform/sensitize people about said risks. This is usually done with the support of a local CBO, as was the case with mVAM in eastern DRC. In Niger, mVAM partnered with the international NGO ACTED to achieve this aim.

- Explore opportunities with 'self-organizing' groups, whereby respondents set up management committees themselves.

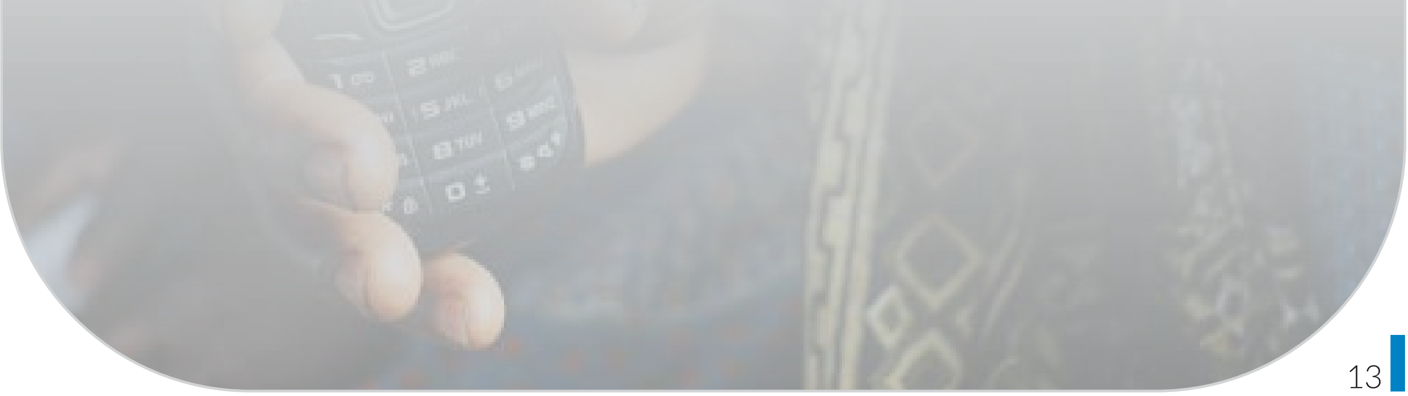
BOX 2

Management committees and mobile data collection

In the mVAM pilot in Mugunga 3 camp in eastern DRC, survey participants self-organized as the activity was set up. A committee of camp residents was constituted, comprising men and women. Committee members liaised with the WFP field office in Goma to report any questions or issues about the data collection that arose while surveys were taking place. Initially, people in the camp had a lot of questions about the purpose of the survey and how/when they would receive the airtime incentive. People wanted to know why WFP was collecting data, and they wanted to be informed of the modalities of the activity. They also needed advice on using the basic phones WFP had provided at the start of the project. WFP soon began receiving calls from the community members who wanted to know more about WFP's food distributions.

As the activity continued, the questions changed. Residents of Mugunga 3 who were preparing to go home wanted to know if they could keep their phones when they left the camp and continue participating in the survey. People also asked whether there was any restriction on using the airtime incentive credit that respondents received after completing each survey.

The committee assisted the elderly in using the phone devices that WFP provided and would help track down respondents who missed a survey round, which contributed to achieving high monthly response rates. The committee was also in touch with the WFP operators and the local camp management leaders.



Choose the right provider – The decision on whether to implement surveys in-house or to outsource them has different implications for data risk.

- **In-house** – When WFP implements surveys in-house, WFP staff collect phone numbers from beneficiaries and manage the lists of contacts (lists of names and phone numbers). It is up to WFP to obtain respondent consent, securely manage phone numbers and collect data in a responsible way. The onus is on WFP to ensure its staff adhere to good data management/privacy practices. WFP is considered the only data controller in cases where WFP has end-to-end responsibility for the protection of respondents' personal data.

- **Outsourcing** – WFP sometimes outsources phone surveys to commercial call centres or providers of SMS or IVR surveys. The third party provider either has an existing list of phone numbers (obtained in various ways, including from old campaigns or through mobile network operators), or WFP provides phone numbers. In the former case, WFP is not responsible for the provider's use and management of the numbers. In the latter, WFP's role is to vet and supervise the third party provider. Note that WFP remains the data controller even when it delegates the use of mobile phone details to a third party provider, and the organization is fully responsible for the protection of people's personal data throughout the entire data lifecycle.

3.2 When collecting data

Seek informed consent from respondents – This is the backbone of the entire data protection system and relates to the principle of lawfulness and fairness: no personal data should ever be collected without the informed consent of the respondent. To enable people to give informed consent, WFP (or the service provider on its behalf) must ensure that people are informed about the following:

- The identity and mandate of WFP and the service provider
- What types of personal data will be collected
- The intended use of the personal data
- With whom the data is expected to be shared (e.g. mobile network operators or other humanitarian actors)
- How to access, update, modify, correct or delete data, where feasible and relevant
- The beneficiary's right to refuse to provide information and the implications of withholding consent, including the effect it may have on the type of assistance that may be rendered, if applicable.

Communications on mobile devices are not necessarily secure and can be tapped into by potentially malicious third parties with advanced technical skills and resources. For that reason, WFP should be careful not to include sensitive PII in any survey. Questionnaires should not mention specific locations, information of an ethnic or religious nature, or informants' names. Secure tools should be used for messaging and surveys (some examples are provided in Section 4).

BOX 3

Guidance for identifying and selecting third party providers

- Providers need to be scrutinized and vetted. WFP should undertake due diligence on candidate companies and assess their compliance with best practices in terms of data security and privacy.

- For a list of vetted providers, consult the existing Long Term Agreements (LTAs)[xi] on remote data collection services including Computed Assisted Telephone Interviews (CATI), IVR, SMS and web surveys.

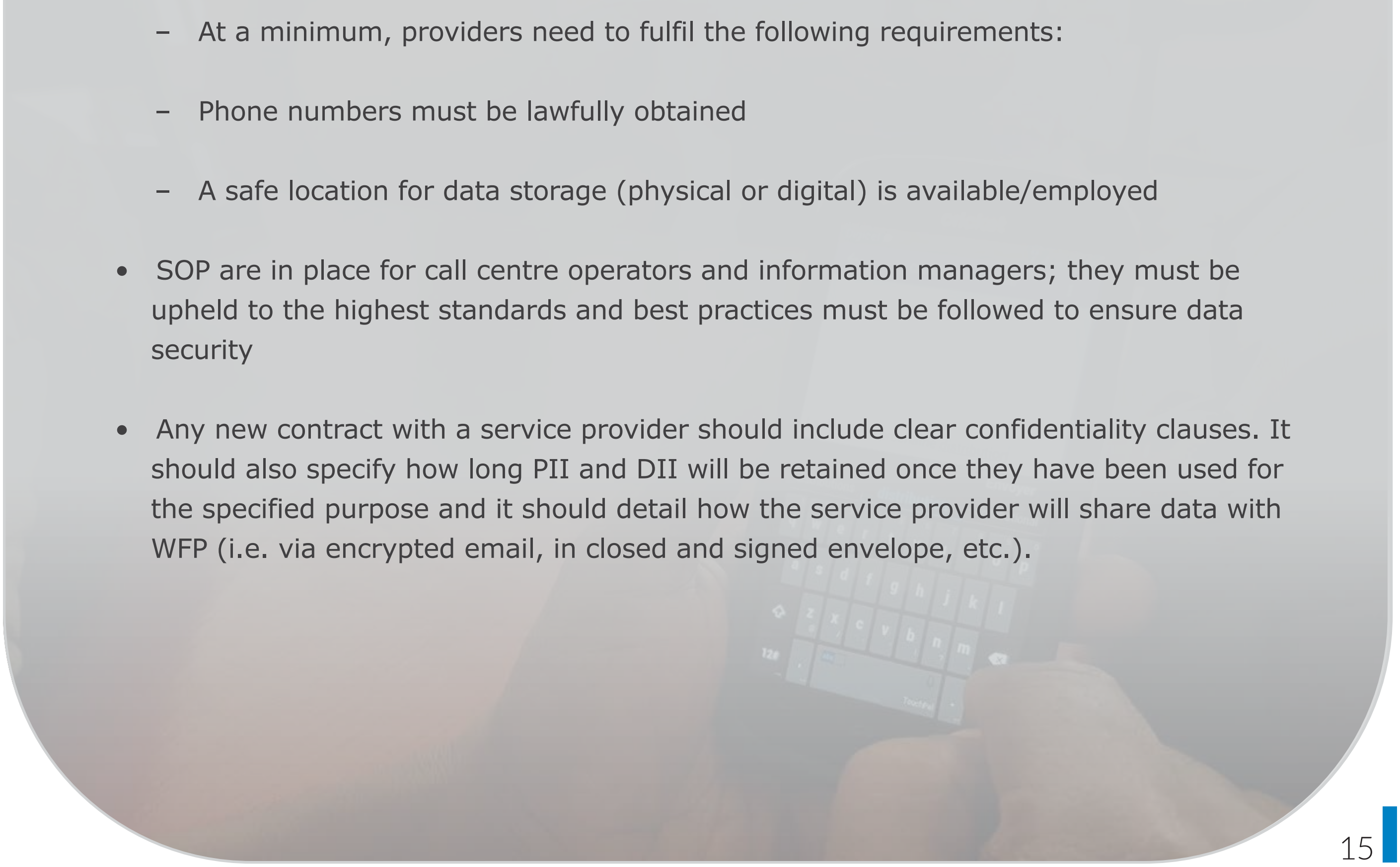
  - At a minimum, providers need to fulfil the following requirements:

  - Phone numbers must be lawfully obtained

  - A safe location for data storage (physical or digital) is available/employed

- SOP are in place for call centre operators and information managers; they must be upheld to the highest standards and best practices must be followed to ensure data security

- Any new contract with a service provider should include clear confidentiality clauses. It should also specify how long PII and DII will be retained once they have been used for the specified purpose and it should detail how the service provider will share data with WFP (i.e. via encrypted email, in closed and signed envelope, etc.).



BOX 4

Challenges related to consent

Consent is not merely a tick box. Fully informed consent includes full disclosure of all potential risks and negative consequences of participation. For a humanitarian organization such as WFP operating in volatile and complex emergency settings, this may not always be feasible or even possible. As a principle, however, some form of mediated or simple consent should be sought even in high risk contexts and especially when WFP is collecting data from economically deprived, marginalized groups and communities with high protection needs, such as displaced people and refugees.

The increasing prominence of crowdsourced data using messaging apps and chatbots poses another challenge related to consent. As WFP tests these new tools and applications, it needs to document learning and share best practices in order to establish strategies and standards to address the responsible data challenges in this digital era.

For more information, see the Responsible Data Forum handbook and guidance from the International Committee of the Red Cross.

Be particularly mindful in conflict settings – In conflict settings, it is important to avoid modalities that leave a large digital footprint which may expose people or WFP to risk. These include SMS and random digit dialling (RDD).[xii] Being cautious with SMS is particularly important because messages remain on phones that security forces or other groups can search – unless respondents delete the messages. Voice calls are better in conflict situations as they do not leave the same trail on a respondent's phone. Additional factors to consider are as follows:

- It is good practice to time calls in the evenings or at an indicated time of preference when people are in the privacy of their homes.
- There are outright cell phone bans in some conflict zones. Using mobile data collection in such settings means putting people in harm's way. Adequate assessment of the situation from a legal and policy perspective is important to avoid this type of error. Remember that sometimes the risks of collecting data in conflict settings are simply too high.
- When the risks outweigh the benefits, think of alternative approaches (e.g. remote sensing, social media monitoring).
- Seek security clearance for your plan by sharing your mobile data collection concept note with the WFP security officer.

3.3 After collecting data

Ensure data integrity – To analyse your data responsibly, the first step is to verify and validate the data. From an analyst's point of view, this is normally addressed during the data cleaning process, but there are other structural factors that are critical to data integrity such as access up in such a way that data is available for the rightrestrictions, interoperability between different data platforms, logging changes made to the data, and backup mechanisms in case of failures.

Information management systems should be set people at the right time, following a 'privacy by design' principle. Managing bias in the data is also an important for data integrity, especially when the results have implications for the allocation of aid resources when certain communities are prioritized over others or when some vulnerable groups could be excluded. Because of disproportionate mobile phone ownership rates and connectivity, some bias in mobile phone survey results is inherent. Literature has shown that results tend to be biased towards wealthier, younger, more literate and male populations from urban areas. WFP accounts for such bias when analysing the data through post-stratification, reweighing and triangulation.[xiii]

Store data in a safe and secure environment – WFP should aim to offer high standards of data security and to be accountable to respondents following data collection. Once data has been collected, it becomes a potential target for malevolent actors seeking to damage the reputation of WFP or to obtain information on targets for attack or other purposes. Data must be stored in a safe and secure location, whether it is physical or digital.[xiv] Inevitably, data will be stored on multiple platforms throughout the data lifecycle as various tools are used for data collection (mobile device, IVR, web, paper);

data storage (mobile device, laptop, centralized database, paper); and data cleaning/analysis (Excel spreadsheets, SQL, data visualization and other reporting platforms). A data security plan should be put in place for each of the platforms used.

Dispose of data once the purpose is met – With the enormous amount of data being generated by WFP through the use of conventional as well as new tools, a distinction must be made between data that can be open and available as a public good and data that should be disposed of when the specific objective of the project has been met. For the former, WFP has already put a best practice system in place with an API-enabled open databank, where food security reports are freely available online together with anonymized aggregate data. For the latter, it is critical that the survey design encompasses a timeline for the data with a clear 'expiry date' so that at the end of the project, the data can be disposed of in a responsible manner.[xv]

Act swiftly when a data breach has occurred – Even with the requisite controls and checks in place, a breach may occur at some point in the data responsibility chain. Privacy breaches and the disclosure of data, whether intentional or unintentional, may have important ethical and operational repercussions. The loss, theft or misuse of personal data may cause harm to the people WFP seeks to assist as well as to WFP personnel. Once a breach of privacy has occurred, it cannot be undone, and it may adversely affect the beneficiaries for the rest of their lives. All incidents of loss or theft must be reported to WFP management and relevant ITC officer(s) immediately.

WFP should also establish a contingency plan in case tools or data sets are confiscated or lost (e.g. ability to wipe out the data remotely and maintain back-up mechanisms). In addition, a case management system for data breaches needs to be in place to register, handle and follow up on incident reports.

Remember accountability – Respondents should be able to contact WFP and/or its service providers to access, verify, correct, update and delete their personal data at any time. Some of the simple mechanisms proposed by WFP's Data Privacy Policy include a) giving beneficiaries the contact details of the WFP sub- and country office focal points; b) providing a feedback desk at the project site; and c) using existing complaints and feedback mechanisms including toll-free hotlines, suggestion boxes and community-based groups.

Summary

Before collecting data

1. Review existing domestic legislation
2. Ensure your data collection has a specified purpose
3. **Data minimization:** collect data on a need-to-know basis only
4. Conduct a Privacy Impact Assessment
5. Understand and engage with local context
6. Choose the right provider

When collecting data

1. Seek informed consent from respondents
2. Be particularly mindful in conflict settings

After collecting data

1. Ensure data integrity
2. Store data in a safe and secure environment
3. Dispose of data once the purpose is met
4. Act swiftly when a data breach has occurred
5. Remember accountability

Tools and methods that WFP Field Officers can use **to mitigate risk**

4

1. Keep respondent lists confidential and do not share phone numbers

2. Use encrypted transfer methods

3. Use secure storage

4. Ensure third party providers abide by their obligations

5. Take extra precautions when sharing or reporting on geolocation

6. Monitoring, evaluation and reiteration

7. Working with the government

8. Alternative approaches

SECTION 4 Tools and methods that WFP Field Officers can use to mitigate risk

Keep respondent lists confidential and do not share phone numbers – WFP's own databases should be kept under lock and key (when on paper) or in a password-protected encrypted file. When phone numbers are held, they should be converted into an anonymous ID – a randomly generated alphanumeric code that makes it impossible to retrace the original number – before data is shared.[xvi] When WFP works with a third party, the provider should be instructed not to share their phone numbers or names of respondents with WFP.

Use encrypted transfer methods – Email is not a secure data transfer tool. Should you need to transfer phone number lists, please use the 'WFP Box' file sharing system rather than the Outlook email system. If for whatever reason you need to use an alternative method, make sure your messaging or email traffic is encrypted by using a secure tool (e.g. Signal Whisper or other email encryption and cloud storage tool).

Use secure storage – WFP has upgraded Pollit and Verboice software to allow the local storage of phone numbers. This makes our systems less vulnerable to hacking than if the data was stored on a public cloud. This is 'security by design'. Another best practice is two-factor authentication (2FA), which is a security process for user authentication through two methods, one of which is usually a password and the other an email/call/SMS verification (an example is Google 2-step verification).[xvii] Many organizations have started using 2FA to protect sensitive data and confirm the identity of the person trying to access the system.

Ensure third party providers abide by their obligations – Third party providers should keep the phone numbers and should not be required to share them with the office. A provision requiring the third party providers to remove this information from the data they eventually send to WFP may be included in the agreement governing collaborations between WFP and third party providers, particularly in highly sensitive contexts. Adherence to this should be verified by WFP through random audits as well as checks by an external party.

Take extra precautions when sharing or reporting on geolocation – The accuracy of GPS locations (e.g. cell phone towers) should be degraded by only providing coordinates to two decimal places. When sharing geolocation data, make sure to use end-to-end encryption transfer methods. In conflict settings, be cautious about providing geolocated information. Information on the whereabouts of respondents is some of the most sensitive data in these settings.[xviii] WFP often works with key informants in besieged and hard-to-reach areas. When reporting results, do not mention the specific location of the informant because this information could put the person at risk.

Monitoring, evaluation and reiteration – Documenting security breaches and sharing lessons learned is key to raising awareness and mainstreaming best practices on data security. In the event of a data breach, WFP must take adequate containment and recovery measures, such as notifying management (Country Director or the appropriate Chief/Director), reporting the incident and redressing the data breach as part of a comprehensive after-action report process involving all relevant actors. Note that a data breach is grounds to end a contract with a third party provider.

SECTION 4 Tools and methods that WFP Field Officers can use to mitigate risk

Working with the government – WFP works closely with local authorities. We suggest that only anonymized data is shared with the government partners with whom WFP collaborates, and only if respondents have consented to this when they opted in.

Alternative approaches – Remember, we don't need to know everything! In the most sensitive environments, information that would allow an individual or a group to be identified should not be collected in the first place. Alternative approaches involve using encrypted chat apps[xix] that offer more security than SMS. Most commercial call centres use software that prevents an operator from seeing the actual number dialled.

Lucia Casarin, WFP

Conclusion:
WFP for responsible open data

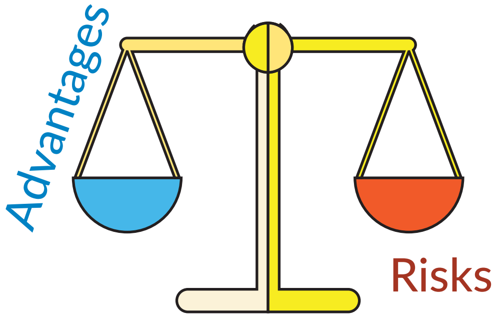
5

Mobile surveys can greatly benefit WFP's operations, especially in hard-to-reach areas. However, this potential can only be leveraged in an ethical and sustainable way if it is done in adherence to a strong data responsibility process. If the process described in this document is consistently applied to WFP's mobile survey projects using the tools and methods laid out in Section 4, and if it is regularly updated to reflect the latest developments in the field of data responsibility, it will ensure an optimal balance between the advantages of leveraging digital data and the potential risks associated with doing so.

There are no shortcuts to responsible open data and the responsibility lies with everyone in the humanitarian data lifecycle. Data responsibility is a process that requires re-evaluating risks regularly to reflect changes in context or data use. Documents such as this one must also be reviewed regularly to keep abreast with the latest insights in this rapidly developing field.

This field book should therefore be considered a living document. If you notice mistakes, or if you find that practices suggested in this book do not work well in a particular situation, please do not hesitate to contact us at the addresses provided below.

Mobile surveys can greatly benefit WFP's operations
...in adherence to a strong data responsibility process!



Optimal balance between the advantages of leveraging digital data
and the potential risks associated with doing so.

Annex

Recommended reading

Electronic Cash Transfer Learning Action Network (eLAN). Data Management and Protection Starter Kit

Gordon, Grant, 2016. Monitoring Conflict to Reduce Violence: Evidence from a Satellite Intervention in Darfur

GSMA, 2014. Guidelines on the protection of privacy in the use of mobile phone data for responding to the Ebola outbreak

Harvard Humanitarian Initiative, 2016. Data Preparedness: Connecting Data, decision-making and humanitarian response

Harvard Humanitarian Initiative, 2017. The Signal Code: A Human Rights Approach to Information During Crisis

International Committee for the Red Cross. Humanitarian Futures for Messaging Apps

International Organization for Migration, 2010. Data Protection Manual

McDonald, Sean, 2016. Ebola: A Big Data Disaster – Privacy, Property and the Law of Disaster Experimentation

OCHA, Leiden University and NYU GovLab, 2016. Mapping Responsible Data Approaches

Oxfam, 2015. Responsible Program Data Policy

Responsible Data Forum, 2016. The Handbook of the Modern Development Specialist

UN Global Pulse, 2016. Privacy Advisory Group Meeting Report 2015-2016

UN OCHA, 2016. Think Brief - Building Data Responsibility into Humanitarian Action

WFP, 2016. Guide to Personal Data Protection and Privacy

[i] Over 6,000 data breaches have taken place since 2005.

[ii] See, for example, "Yahoo hack: 1bn accounts compromised by biggest data breach in history".

[iii] The International Data Responsibility Group (IDRG) is a global network of experts and organizations working on the principles and standards for guiding the Data Revolution in the context of humanitarian action, sustainable development and peace and justice. Its members seek to build an authoritative knowledge base that enables responsible experimentation on the release, processing and use of data and the minimization of risks. The IDRG is designed as a networked platform, with a coordinating secretariat in The Hague. Research and affiliated partners meet every year to host the Annual International Data Responsibility Conference.

[iv] Source: Responsible Data Forum working definition, September 2014.

[v] This is inspired by Europe's General Data Protection GDPR art. 4 under 1: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

[vi] A telephone number, if triangulated with a few other non-strictly personal information points (e.g. identity of the provider, geographical coverage of the provider, user's birthplace), might also lead malicious hackers to retrieve people's identity indirectly. Mobile numbers should be considered as personal information and treated in accordance with WFP's personal data protection standards. WFP usually records people's names and phone numbers in the lists that operators use to place phone calls. The listings identify whether respondents live in an internally displaced persons (IDP) or refugee camp and sometimes they contain the camp's name and location. While WFP doesn't collect people's physical addresses, its listings will mention a place of residence (e.g. a camp, a neighbourhood, a village). The listings will likely also mention if someone is a refugee, an IDP or a returnee (i.e. someone who used to live in a camp). This could be used to identify individuals by inference – by combining a number of information points that together mean the respondent can only be person X. Another threat is that once a malevolent actor has access to an individual through their telephone number, they could contact the individual to extract more information or extort mobile money or airtime by posing as an operator, or through other means of social engineering.

[vii] Taylor, Linnet, Luciano Floridi, and Bart van der Sloot, 2017. "Group Privacy".

[viii] See the GDPR portal.

[ix] For more on data preparedness, see this Harvard Humanitarian Initiative report.

[x] For more on PIA, see the Electronic Cash Transfer Learning Action Network's (eLAN) Data Management and Protection Starter Kit, available at http://elan.cashlearning.org/

[xi] LTAs can be located in the database managed by HQ Procurement. For further enquiries, contact HQ.Procurement@wfp.org

[xii] Random digit dialling is a sampling technique for telephone surveys whereby survey participants are selected by generating telephone numbers at random. Employed by call centres or third party providers who do not have a list of phone numbers, this technique has the advantage of including unlisted numbers that would be missed if the numbers were selected from a phone book.

[xiii] Additional documents detailing how bias is accounted for can be found in some of the country pages of the mVAM site.

[xiv] As a minimum, the following specifications are recommended:

- **SERVER:**
    - Processor: Inter(R) Xeon(R) CPU – 4 (or 6) Processors
    - Memory: 16 (or 32) GB RAM
- **DATABASE:**
    - Microsoft SQL Server
    - MongoDB

[xv] There is no single established norm for how long data should be kept as this depends on the country and the context. Some guidance on personal data detention can be found on pp. 82–83 of the WFP *Guide to Personal Data Protection and Privacy*: "WFP should not hold personal data for longer than is necessary to fulfil the specified legitimate purpose for which the data was collected...Extension is allowed when in the interest of beneficiaries...Anonymized/less sensitive data can be stored for longer if useful".

[xvi] mVAM guidance on anonymization is available here.

[xvii] For a list of websites and web services supporting 2FA, visit this site.

[xviii] For more on this subject (though not specifically related to conflict settings), see 'Building Data Responsibility Into Humanitarian Action' by NYU GovLab, Leiden University Centre for Innovation and UN OCHA, p. 3: "(...) the most critical type of data produced by the ecosystem is information about the time and place-specific activities of affected populations, i.e. 'spatiotemporal metadata'."

[xix] A list of secure messaging apps is available here.

Kusum Hachhethu, WFP

Contact us

For comments, questions and suggestions on this field book, please contact the following colleagues who were involved in drafting the document:

Jos Berens, *Project Officer Data Responsibility*, Leiden University Centre for Innovation (j.b.berens@fgga.leidenuniv.nl)

Jean-Martin Bauer, *Senior Food Security Analyst*, WFP (jean-martin.bauer@wfp.org)

Angie Lee, *Food Security Analyst*, WFP (angie.lee@wfp.org)

vam.wfp.org @WFPVAM and @mobile VAM

WFP
wfp.org

vam
food security analysis