7 Responsible Data Practices and Data Protection

Table of Contents of the Module

Responsible Data Practices and Data Protection

Ensuring Data protection and responsible data use are top priorities at IFRC and throughout the Movement. With this Module, we hope to provide information and exercises that explore the issues you might face and help you to be better prepared to understand and solve those issues in practice.

As with any content of a general nature, the guidance (and examples) contained in the module are only intended as a starting point. You should do your own due diligence, involving legal counsel where appropriate, to determine what any specific legal obligations (or other relevant considerations) are in your operating context.

Questions this module explores:

- What does responsible data use and data protection mean to humanitarians and why are the concepts important?
- What are the differences between non-personal, personal and sensitive data and why is it important to know the differences?
- What does it take to protect and use data responsibly in practice?

Learning Objectives

- Understand why responsible data use and data protection are important to the implementation of the IFRC's work and how they link to humanitarian principles;
- Develop the confidence and knowledge to identify and distinguish between different kinds of data (e.g. non-personal, personal, sensitive and sensitive group data) and what that means for how it should be used responsibly; and
- Explore legal, ethical, practical and cultural factors impact upon data protection in practice in complex emergency settings.

Module Topics

- Using data responsibly includes protecting it but also requires thinking about broader humanitarian responsibilities like Do No Harm and Impartiality.
- Distinguishing between different kinds of data can make it easier to understand what data needs to be protected. Humanitarians have a duty to protect and responsibly use information that might be used to identify an individual or vulnerable group.
- It is important to work with local communities to identify possible risks to them and then take steps to responsibly use that data.
- Responsible data use and data protection should be considered at each step of a project's workflow and need to be thought through before any new data collection activities commence.
- How data should be protected and used responsibly in any given context depends largely on the IFRC/NS's mandate to operate there. As humanitarians, communities' consent isn't always needed to use data about them, but that data must always be used responsibly.

- Documenting decisions (and how those decisions were reached) about how data has been protected and used is a key part of using data responsibly. Data Protection Impact Assessments, Data Sharing Agreements and Consent Forms can be helpful when doing this.

Recipes

A suggested step by step process to achieve learning objectives

1. How can we incorporate best practices of data protection and responsible data use into our work? With your teams, explore: **People Before Data (handout) (7 - 16)**, **What data do we really need? (7 - 9)**, **What can we do vs. What should we do? (7 - 10)**, and
2. Humanitarians collaborate across organisations. Data sharing is important for humanitarian response. Yet, sharing data must be done carefully and guided by the practices of Data Protection and Responsible Data use. Start by having a short discussion. **Would you Share it? (7 - 12)** Teams can then plan with their existing projects by reviewing this handout and associated checklist: **Data Sharing Agreements (part 1) (7 - 1)** (part 1 and part 2).
3. How does data protection align with our values and principles? The **Humanitarian Values & Data Protection (7 - 7)** (exercise) combined with the **Humanitarian Values & Data Protection (7 - 8)** (handout) can guide teams through these conversations.
4. The **Polio Campaign Monitoring In Syria (7 - 17)**, **PMER Data Simulation (7 - 15)** 'simulates' data workflows for various topics. Teams should use these scenarios in conjunction with the **Strengthening Data Teams and Projects (3)** (Module 3).

Ingredients

Pick and choose ingredients to create your own recipe. Do you have an ingredient we're missing? Send an email to data.literacy@ifrc.org.

Exercises

Short, discrete social learning experiences

- ► What is the Data We Really Need?
- ► What should we do vs What Can we do?
- ► Data Responsibility (scenario)
- ► PMER Data Protection (Scenario)
- ► Polio Monitoring (Scenario)

Session Plans

Longer social learning experiences

- ► Debate Club: Data Protection and Digital Risks
- ► In Your Shoes
- ► Matching Humanitarian Values and Data Protection Principles
- ► Data Protection Nightmares
- ► Wheel of Misfortune

Slide Decks

Presentations to be used and/or adapted:

Provides context for data use and its importance within IFRC

- ► Understanding and Identifying different types of data
- ► Understanding the 'legal basis'

Checklists/Handouts/Materials

For documentation of essential elements of the learning experience

- ► Data Sharing Agreements (Part 1)
- ► Data Sharing Agreements (Part 2)
- ► Matching Principles (Handout)

- Data Hygiene (checklist)
- People before Data (handout)

Next Steps

Relevant modules in the Data Playbook

- (Module 3: Strengthening Data teams and Project) and (Module 4: Getting the Data we need)

Resources

- IFRC Data Protection guidance
- Handbook on Data Protection in Humanitarian Action, 2nd Edition (ICRC)
- IASC Operational Guidance on Data Responsibility in Humanitarian Action
- OCHA Data Responsibility Guidelines
- IFRC Digital Transformation Strategy
- Digital Dilemmas (interactive website)

Credit

James De France, Tom Orrell, Heather Leson, IFRC V1 Sprint and Data Playbook Beta contributors

7 - 1 Data Sharing Agreements (part 1)

In our work, there are many questions about "data sharing" and "data sharing agreements." This handout can be used pre-deployment/ pre-project planning session as part of responsible data use and data protection training. It can also be used in the field as a rapid reference tool and checklist to help staff think through the requirements of data sharing.

Data sharing is the practice of granting other individuals or organisations access to data that you are responsible for. Data sharing could be anything from sending a spreadsheet to a colleague at another humanitarian organisation via email, to providing limited access to Red Cross Red Crescent data to governments. This handout is an explanation for Data Sharing Agreements. See Part 2 for a draft document to fill out as you coordinate.

What are Data Sharing Agreements?

Within the Red Cross Red Crescent's work, 'data sharing agreements' (DSAs) refer to a range of documents that cover the transfer of data within and between the Movement and governmental and non-governmental partners. DSAs need to address a number of considerations; and where they relate to the sharing of personal or sensitive data, need to clearly define how that data will be protected and individuals' rights respected.

At a minimum, DSAs need to establish clarity and a degree of certainty about what data will be shared, how data will be shared, why it is being shared, what it will be used for, who will be sharing and receiving the data, and when and where the sharing will take place, and how to ensure the data is protected and not misused after sharing. Ideally, DSAs should also include agreed terms relating to how intellectual property rights will be upheld, how and where any disputes relating to the agreement will be resolved, and any other relevant considerations.

Within the Red Cross Red Crescent, DSAs should be used any time data is being transferred into, out of, or between the different organisations that comprise the Movement.

What does a Data Sharing Agreement include?

Contents	Explanation
What data is expected to be shared?	⊙ Be as specific as possible about what datasets are going to be shared. Ideally, list them out. ⊙ It is extremely important that you separate out 'personal and sensitive' datasets from 'non-personal' and ensure that you abide by any applicable local data protection and privacy laws, and IFRC guidance on personal data sharing.
Who is sending data and who is receiving it?	⊙ List all the names and contact details for the organisations/people who will be sharing data – both those sending the data and those receiving it. ⊙ If some or all of the data that is being shared belongs to another organisation, make sure that you have permission to share it or also include them in the agreement if they have control over the data.

Contents	Explanation
When will the data sharing start and when will it end?	- Specify the start and end dates for the data sharing. Specify what will happen to the data at the end of the agreement – will it be returned to the data provider, deleted, archived, etc. - If you are not sure when the data sharing will end, add a clause into your agreement agreeing to review the timeline at an appropriate juncture (e.g. you could agree to review in a month, or three months, or a year, depending on the nature of your needs at the time).
If personal data is involved, what measures are needed to ensure that it continues to be protected during and after transfer (access is provided)?	- Review the proposed data sharing plan with all of the data protection principles in mind: i.e. legal basis, minimization, purpose limitation, data security, transparency, proportionality and data subject rights.
Why is the data being shared?	- Make sure to clearly list out the reasons why data is being shared. - If personal or sensitive data is being shared, ensure that you document all the legitimate legal bases upon which that data is being shared.
How is the data being shared?	- The DSA should specify how data will be transferred; for instance, by email, by granting remote access to a server, via the cloud, etc. - Where possible, the agreement should specify the standards and formats that apply to the data being shared.
Where is the data being shared from and where is it going to?	- It is important to clarify where data is being transferred from and to because this could affect the laws that cover the data sharing. For example, under the European Union General Data Protection Regulation (GDPR), there are special rules that must be followed when making international data transfers. Each organisation and/or region/country may have their own legal obligations around data protection. - The agreement should set out which country’s laws (jurisdiction) apply to the agreement and ensure that the DSA complies with those requirements. This might require legal guidance. - This will require a review of any applicable national or regional data protection and privacy laws.

Contents	Explanation
Other Considerations	⊙ Who will own the intellectual property rights over any outputs produced from the shared data? ⊙ Who will cover the costs associated with the transfer, processing or analysis of the data? ⊙ How will any Red Cross Red Crescent logos and emblems relating to the data be used? ⊙ What will happen to the agreement in the event of some unforeseen circumstance cutting it short (force majeure)? ⊙ How will you and the other parties to the agreement agree to compensate each other and protect yourselves financially in the event of a financial loss (indemnification)? If you are operating in a high-stress emergency setting and you need to share data quickly with a trusted partner such as a colleague at another humanitarian agency in exceptional circumstances, remember to consider the following things: ⊙ You can share non-personal data unless there is a good reason not to – DO NOT share any data externally that might put individuals or communities at risk, jeopardise the delivery of humanitarian programmes or operations, or bring the Movement into disrepute. ⊙ If you need to share personal data: — Think about what precise data you need to share to meet your urgent need and what the best way of sharing it might be; — Agree how the data will be used, who else it should or should not be re-shared with and what steps will be taken to protect it; — Set a time limit for how the data that is being shared will be used and agree on what you'll do with the data once it's been used. Agree a time and way in which you will formalise your data sharing; — Consider whether conducting a Data Protection Impact Assessment (DPIA) is appropriate; and — Ensure that you document your data sharing decisions and enter into a data sharing agreement as soon as possible. All sharing of personal or sensitive data must be documented and recorded.

Credit

Tom Orrell, consultant IFRC Data Playbook

7 - 2 Data Sharing Agreements (part 2)

In our work, there are many questions about "data sharing" and "data sharing agreements." This handout can be used pre-deployment/pre-project planning session as part of responsible data use and data protection training. It can also be used in the field as a rapid reference tool and checklist to help staff think through the requirements of data sharing. Data sharing is the practice of granting other individuals or organisations access to data that you are responsible for. Data sharing could be anything from sending a spreadsheet to a colleague at another humanitarian organisation via email, to providing limited access to Red Cross Red Crescent data to governments. This Handout can be used with part 1 (explanations).

Coordinate your Data Sharing Agreement:

Contents	Description
Who is sending data and who is receiving it?	
When will the data sharing start and when will it end?	
What data is being shared?	
Why is the data being shared?	
How is the data being shared?	
Where is the data being shared from and where is it going to?	
Other Considerations ⊙ Who will own the intellectual property rights over any outputs produced from the shared data? ⊙ If personal data is involved, what measures are needed to ensure that it continues to be protected during and after transfer (access is provided)? Review with all of the data protection principles in mind: i.e. legal basis, minimization, purpose limitation, data security, transparency, proportionality and data subject rights. ⊙ Who will cover the costs associated with the transfer, processing or analysis of the data? ⊙ How will any Red Cross Red Crescent logos and emblems relating to the data be used? ⊙ What will happen to the agreement in the event of some unforeseen circumstance cutting it short (force majeure)? ⊙ How will you and the other parties to the agreement agree to compensate each other and protect yourselves financially in the event of a financial loss (indemnification)?	

Credit

Tom Orrell, consultant IFRC Data Playbook

7 - 3 Debate Club - Data Protection and Digital Risks

Organisations and individuals have many questions and concerns about data protection, responsible data, and digital risk. In this interactive session, we will host an "informal debate club." The purpose is to openly discuss (with humour and role playing) some of these questions and concerns. The output is a list of questions/policies and practices that need more explanation/shared understanding.

Each of the participants will work in small groups to write up some informal 'statements' that could be debated on high level topics. An example statement is 'AI's benefits outweigh any risk of bias.' Each group/individual will make statements about 'agreeing' or 'disagreeing' with the statements. It is encouraged to debate different viewpoints to prompt discussions and highlight nuances of the topics. Participants should be encouraged to discuss the topic in a spirited role playing manner. This session is for all audiences to explore concerns around responsible data use, Data Protection and Digital risks. Invite subject-matter experts to be available for the introduction and for the 'after discussion' during this session. Some examples might include a cybersecurity officer, lawyer, communications officer, or policy colleague.

- **People:** 5 to 30 people
- **Time:** 60 Minutes
- **Difficulty:** Easy
- **Virtual Materials:** virtual meeting platform, shared document/writing space
- **In Person Materials:** flipcharts/noteboards, sticky notes, markers

Exercise

Session guidelines: Advise participants that there will be no recording or directly identifying quotes from the conversations. The goal is to create an open conversation space.

Part 1: Setting the scene

- Welcome people to the session
- Introduce guest subject-matter experts.
- Begin the session with a brief introduction to the topics (some definitions and workplace policies/practices) and provide some examples to get people thinking about the context of the work.
- Depending on group size and team – ask people to share 1 thing about what worries them about data and digital risks
- Explain the exercise (Parts 2 – 4)
- Demonstrate how the 'debate' portion would work. Discuss with two people to represent the flow of a 'debate.'

Some Examples:

- AI's benefits outweigh any risk of bias
- The government protects all vulnerable citizens so we should share citizens' personal data with the government
- We must share HIV data of beneficiaries with local government health organisations
- When a delegation/donor pays for a program, they should be entitled to all of the client data (including personal data).
- We should pay ransom in case of a ransomware cyber attack

- As long as we get consent, we will not have any data protection issues.

Each 'presenter' will state whether they agree or disagree with the statement. Encourage colourful responses.

- Optional: For a virtual event, you could also have a series of prepared statements to get people thinking and collaborating on statements explaining why they may agree and disagree with the statement. Ask participants to put initials on the line and then ask them to explain.

Part 2: Breakout groups

In breakout groups of 2 - 4 people, introduce yourselves. Create up to 5 'statements' related to the session theme - "What are some examples around responsible data, data protection and digital risks? " Statements should inspire debate: controversial and creative. Take notes in the collaborative document or on sticky notes. Also, capture any questions to be addressed in the future. We will use these in the plenary 'DEBATE'. Pick your top 2 statements to bring to the 'debate club.'

Part 3: Debate in Plenary

Each team will take turns sharing their 'statement.' One of the team mates should present the 'agree' or 'disagree' statement viewpoint. Open the discussion to have people share their viewpoints. Capture notes, insights and questions.

Depending on the time of the session and size of the group, do 3 - 4 rounds of statements.

Part 4: Coordinate questions and insights

Ask participants - What were some of the outstanding questions they identified? Any insights? Capture these in your collaborative document or on a flip chart.

Extra Credit

Use this exercise to foster team discussion before sharing your organisation's Data Protection/Responsible Data Policies and Practices.

Resources

- IFRC Data Protection Guidance
- InterAgency Standing Committee Guidance on Data Responsibility
- Facilitation guidance (Aspiration, Spectrogram exercise)

Credit

Aspiration, IFRC Data and Digital Week participants

7 - 4 Understanding and identifying different kinds of data

Consider the data you are using for any project. Is it **non-personal**, **personal**, **sensitive** or **group sensitive** data?

Identify the **categories** the data you are using. Then, you can make a plan to protect and use the data **responsibly**.

Personal data

Personal data is any data that can be used to identify an individual, whether on its own or when combined with any other data.

Examples:

- ► Individuals' names, addresses, dates of birth, social security numbers can all potentially be personal data if they can be used to identify an individual.
- ► Personal data can include things like someone's GPS coordinates (location), their IP address, or internet browser cookies.

Personal data

Context matters:

- ► Remember, context matters. For example, some names that might be very common in one country – and thus likely to not be personal data on their own – might be considered personal data if they appear in countries where they are rare – and thus more likely to result in an individual being identifiable.

Aggregating (combining) datasets:

- ► Some data THAT might be non-personal on its own, can become personal if combined with another data point.
  - ⊙ **Example:** the GPS data from an IFRC vehicle in the field on its own is probably not personal data, but if combined with data from a register of approved IFRC drivers, it could become personal data as it is likely that the vehicle's driver could be identified as an individual if both data points were available to the same person.

Non-personal data

Non-personal data is simply data that cannot be used to identify any particular individual or vulnerable group.

Non-personal data is not usually subject to strict legal requirements for data protection. However, **this data may still be confidential or otherwise sensitive** and MAY still need to be securely stored, regularly maintained and updated, and used responsibly.

Example: Non-Personal Data

- Logistical data such as inventories of medical supplies or the number of IFRC vehicles registered in a particular country.

Sensitive data

Sensitive data is personal data that, if disclosed, could be used to discriminate against someone or cause them harm (mental or physical).

- Sensitive data is **context specific** and data that is not sensitive in one country, might be sensitive in another depending on local social and cultural norms.
- In many countries, sensitive data requires a very high degree of protection and/ or should not be collected, used or shared unless absolutely necessary.

Example:

- Individuals' medical records, HIV-status, biometric data or DNA, religious or political beliefs, ethnic background and nationality, or sexual orientation and gender identity.
- A name, for instance, is not typically considered sensitive. However, in some places, certain last names may reveal religion or ethnicity.

Sensitive group data

Sensitive group data is data that can’t be used to identify individuals, but can be used to **identify vulnerable groups**, either on its own or when combined with any other data.

Sensitive group data is **context specific** but very important to protect in emergency settings. Ideally, any sensitive group data that is collected or used should be subject to the same rules as sensitive data.

Example:

► Aerial photograph showing the location of an uncontacted indiginous tribe. While no individual is identifiable, the image clearly depicts a community that is vulnerable in numerous ways and if it were to fall into the wrong hands, could lead to harm coming to the community.

Thank you

Credit: Thomas Orrell, James de France, Heather Leson

7 - 5 Understanding the ‘legal basis’ when collecting and using data

What is a 'legal basis' for data collection?

If you plan to collect any personal or sensitive data it is important to think about whether you are permitted to do so.

There are a limited number of reasons for which personal and sensitive data can be collected and used. (sometimes referred to as a 'legitimate basis.')

What are the generally accepted legal bases for data collection?

Legal bases for data collection and data use include:

- Fully informed and freely given consent
- Public interest
- Legitimate interest
- Vital interest
- Contract
- Legal obligation

Fully informed and freely given consent

Fully informed and freely given consent is the approach that gives individuals the most rights and power to decide whether data about them is used and shared.

In humanitarian settings, consent may not be the appropriate legal basis, as individuals may feel that they have no choice but to provide their data (thus, it is not freely given). Moreover, relying on consent as the only legal basis can come with additional administrative challenges, especially in emergency settings. It should also be noted that consent may be withdrawn by individuals at any time.

Consent is best suited to the collection of non-essential data, and in non-emergency settings.

See examples in the Practical Guidance for Data Protection in Cash and Voucher Assistance.

Fully informed and freely given consent (continued)

For consent to be ‘fully informed,’ the data collector needs to clearly communicate the following to the individual that data is being collected from/about: how and why their data will be processed, how that data will be protected, if it will be shared, how long it will be kept, any consequences of not providing the data, and how to address any concerns he/she might have.

In order for consent to process personal data to be ‘freely given,’ the person collecting the data needs to be reasonably certain that the individual providing the information has not been coerced or forced to give up their information; that they truly have a choice to provide the information without negative consequences.

Public interest

Personal or sensitive data can sometimes be collected and used on the basis that such processing is in the 'public interest.'

Example: public health emergency

► Government might ask (not require) a National Society to support data collection for the emergency. In many countries, what is considered as in the public interest must be based on existing law. However, there is a trend toward viewing humanitarian action as in the public interest. It is best to review your national legal requirements when seeking to rely on this basis.

Legitimate interest

Legitimate interest is an activity that supports the underlying mandate(s) of the organisation. For example, fundraising is needed to provide support for ongoing operations. It is in the organisation’s legitimate interest to collect donors’ personal data in order to receive donations and to enable future communications with those donors. When using legitimate interest as a legal basis, you must evaluate whether the rights of the data subject might outweigh the interests of the organisation. Another example might be the collection of personal data during an audit of a project in order to determine whether it was successful and if/how improvement could be made.

Contractual performance

Personal and sensitive data is often collected in order to fulfil an agreement.

Example:

- ▶ Staff might be required to provide details about their address, families and next of kin, nationality and financial details when joining the movement as employees.
  - ⊙ It is necessary to collect certain data to ensure that staff receive their salary payments, thus fulfilling one of IFRC's contractual obligations to a staff member.
  - ⊙ Other data about family members may be necessary to properly calculate benefits that are due as part of the employment contract.

Legal obligation

Sometimes a legal obligation requires that certain data be collected and processed.

Example:

- ► For staff moving to a new country to take up their duties, the IFRC must collect certain data and provide it to the government in order to ensure that the proper residency permit (or visa) may be obtained. A government has imposed this obligation in order to obtain the permit.

Vital interest

Sometimes it might be absolutely necessary to collect personal data to help someone. Collecting and using personal data on the basis of vital interest is typically considered appropriate where there is a relatively immediate threat, either physical or mental.

Example:

▶ if someone is severely injured, you could collect all necessary data (such as health data) to help that person on the basis of protecting his/her vital interests. Once that emergency situation has passed, and the person is physically and mentally stable, you might then rely on other legal bases for your personal data processing.

How do I know which legal basis to use?

- It is not easy to know what the right legal basis to use is. You must always evaluate situations individually to determine which is right.
- Remember, if people are in need of help, consent may not be used if the assistance is conditioned upon receiving data. That is not freely given.
- Also, regardless of which legal basis is relied upon, at least the following information should always be provided to data subjects in an understandable and accessible form:
    - why the information is being collected;
    - what it will be used for;
    - who it will be shared with;
    - how long it will be retained;
    - whom they can contact with questions.
- If in any doubt, you should ask your legal department.

Questions for discussion

- ► What are some of the challenges that you think might arise in trying to collect and use data on the basis of 'fully informed and freely given consent' in an emergency context? When would it be appropriate for the IFRC or a National Society to use consent? When might it be inappropriate?
- ► What additional responsibilities do you think that the IFRC network needs to take into account when collecting and using data on a basis other than consent?
- ► If you had to collect personal or sensitive data on the basis of either legitimate or public interest, what kinds of information would you strive to provide to the individuals from whom you are collecting that data?

Thank You!

Credit: Thomas Orrell, James de France, Heather Leson

7 - 6 In Their Shoes

Using ‘consent’ as a basis for data collection and use in a humanitarian setting requires a series of judgement calls. In an ideal world, IFRC staff and volunteers would be able to get each and every individual’s personal data that they need on the basis of fully informed and freely given consent. In reality, the urgency and complexity of emergency settings make it extremely difficult to do so. While the IFRC and National Societies are often authorised to use personal or sensitive data without necessarily having obtained individuals’ consent, when they do so, they still need to think about the ways in which that data should be used responsibly and in line with data protection best practices.

This scenario-based role-playing exercise is designed to surface some of the complexities that the collection and use of data on the basis of consent gives rise to. It also touches upon the duties to be open and transparent about data that the IFRC collects and uses, as well as the responsibilities that the IFRC has to be an ethical and responsible data steward. The exercise is targeted at an intermediate and advanced audience that already has an understanding of the bases upon which data can be collected and used, and the ways in which humanitarian values and data protection principles overlap.

- **People:** 5 to 20 people
- **Time:** 60 – 90 Minutes
- **Difficulty:** Intermediate
- **Virtual Materials:** virtual meeting platform, shared document/writing space
- **In Person Materials:** flipcharts/noteboards, sticky notes, markers

Exercise: Role Playing

A National Society is preparing to meet a large group of people who had to evacuate their lands and homes due to severe flooding. The international community and host country have recognised the crisis and have issued mandates - both internationally and within the host country - to support the communities that have been affected. Staff are being mobilised to establish meeting posts at which they will undertake a rapid assessment of families that are arriving and register them for support (support envisioned: food, shelter, basic cash assistance via a voucher, psychosocial and medical.). The people arriving are deeply traumatised, having lost their homes and livelihoods as well as family members and friends. They are often destitute, exhausted and in a state of shock.

Roles:

- National Society response coordinator – responsible for planning and establishing the meeting points, including the processes for data collection
- Data collector – on the ground staff member or volunteer who will be collecting data
- Deeply traumatised adult who is seeking assistance
- Deeply traumatised minor traveling alone seeking assistance
- Any others that are needed?

Part 1: planning - group discussion

- What processes should the response coordinator put in place to collect data – how should this be done?
- What data needs to be collected?
- How should the data collector approach data collection in practice?

Part 2: data collection - simulation

- Simulate an initial interaction between the data collector and affected communities. What kinds of questions would be asked? What would the responses likely look like?
- If the data collector tried to gain 'fully informed and freely given consent' from the communities, what would this entail? What would a conversation likely look like?
- What other basis might be more appropriate in this instance to collect data?
- What additional considerations are there when interviewing the unaccompanied minor?

Part 3: data use - group discussion

- Once the data has been collected, given the vulnerability of the communities, what responsibilities does the National Society have to use it responsibly and keep it secure?
- What information should be provided to the affected communities about how their data will be used? When would be the best time to provide them with this information given their state of shock and trauma?
- Looking back over the scenario now, would consent be an appropriate basis to collect data in this instance? If so, why? If not, why not?

Extra Credit

Present your organisation's Data Protection Policy and discuss next steps and examples of applying the lessons in your work. See the IFRC Data Protection guidance

Credit

Tom Orrell, James De France, Heather Leson

7 - 7 Humanitarian Values & Data Protection

Responsible data use and data protection can often be difficult topics to raise with participants who are not familiar with data and what some of the potential risks of digital technologies are. This exercise requires just a basic understanding of humanitarian values and what personal data is. The objective of the exercise is to connect humanitarian principles to data work and introduce key concepts of responsible data use and data protection from a values perspective instead of a legalistic one. Participants can build confidence in their ability to understand the terms and concepts within data protection.

- **People:** 2 to 12 people
- **Time:** 30 – 60 Minutes
- **Difficulty:** Easy
- **Virtual Materials:** virtual meeting platform, shared document/writing space
- **In Person Materials:** flipcharts/noteboards, sticky notes, markers

Exercise

Part 1: Explore

In small groups (ideally pairs), discuss:

1. What do you think it means to ‘protect information’ as a humanitarian?
2. What does it mean to use data ‘responsibly’?

Take notes on any insights or questions on a shared document.

Part 2: Review

Discuss responses as a whole group asking each group to share 1 highlight from their conversation.

Part 3: Discuss

Share the Matching Principles (Handout). In small groups, discuss the following questions:

- How does our independence impact how we collect, use and share data?
- Should we be open and transparent about what information we collect from communities and how it is used?
- Should we collect as much data about the communities we serve as we can or do we need to collect as little as possible? How do we find a balance?
- Take notes on any insights or questions on a shared document.

Part 4: Reflect

In plenary, ask for reflections and questions. Share further details about the organisation Data Protection policy.

Extra Credit

This exercise could also include a scenario for part 2. A scenario-based learning component can link the concepts to real-world situations that participants face where they need to think about what it would mean to use data responsibly and protect it.

Examples:

- A local NGO partner shares data with a National Society but refuses to disclose how the data was collected, raising doubts about its quality. What challenges does this scenario raise? How would you handle the situation?
- You have collected data from a village about their medical needs. You got their consent when collecting the data to only use it to help your own logistical activities. You now want to share that data with local health authorities. Can you share this data? What information should you disclose to the community about your plans?
- You're collecting data in a very fragile conflict zone. Local communities are reluctant to provide you with information because they are worried about the repercussions if it fell into the wrong hands. What steps can you take to ensure that their concerns are taken into account?

Facilitators: you may want to initially divide groups into pairs to first discuss the scenario between themselves before then encouraging a group discussion on the key themes. This exercise is likely to take about 30-45 minutes per scenario to run depending on the number of participants involved.

Considerations:

As you review the exercises and the Extra Credit activities, consider that: 1) all data processing should comply with data protection principles (i.e: having one or more legal bases, accurate and minimized data, transparent communication about the processing, data only used for compatible purposes, ensuring data security, and respecting data subject rights), and 2) our actions, while assisting a government, must remain aligned with the fundamental principles, in particular here independence and neutrality. Our objective must be to serve a humanitarian purpose, not only for the aid of, or direction by, a governmental entity.

Credit

Tom Orrell, Arturo Garcia, Dirk Slater, Heather Leson, Melissa el Hamouch, James De France

7 - 8 Humanitarian Values & Data Protection

Humanitarian action is rooted in human empathy and solidarity. It's purpose is to protect life and provide relief to the most vulnerable. Within the humanitarian community, the highest held value is the idea that humanitarians should *'do no harm'* in their actions. Increasingly, this also applies to how humanitarian organisations use digital tools and data.

What does it mean, though, to 'do no harm' when collecting, analysing, using or sharing communities' and individuals' data? A good place to start is to think, and discuss, more deeply about how humanitarian values and principles, and data protection principles overlap and reinforce each other. In this way, it is possible to start to find answers to questions like what it means to 'protect' use data 'responsibly.' This handout will link Red Cross Red Crescent Movement Fundamental Principles with an overview of some key data protection principles.

Movement Fundamental Principles:

- Humanity – the need to act to prevent and alleviate human suffering
- Impartiality – non-discrimination of anyone
- Neutrality – taking no sides in conflict
- Independence – being autonomous and resisting any interference
- Voluntary Service – a desire to help others, not prompted by a desire for self-gain
- Unity – there can only be one RCRC society in any one country
- Universality – IFRC is worldwide and carries a collective responsibility to all

Data Protection Principles:

- Don't collect personal data you don't need – only collect data that could identify an individual ("personal data") if you really need it
- Keep your datasets up-to-date and in good shape, just like any other asset – personal data collected should be accurate, complete and kept up-to-date
- Be clear, and document, why you are collecting data – the reasons personal data have been collected need to be clearly stated and only personal data needed for those reasons should be collected
- Only use personal data for specific reasons/activities that you have already planned – personal data collected for a particular purpose, should only be used for that purpose
- Make sure your datasets are safe and in your control – personal data should be protected from unauthorised access, destruction, use, modification or disclosure/publication
- Be open about the data you have and what you're doing with it – information about what personal data is collected and how it is used should be available to the data subjects
- Respect individuals' right to decide how data about them is presented and used – people have the right to ask what information about them has been collected, what it's being used for and have the right to have it changed, and sometimes removed (if the data was collected with their consent)
- The IFRC is accountable to the communities it serves, this includes how it uses their data – those collecting and using personal data need to be accountable to the people whose data they are using and compliant with any applicable international or local laws

References

IFRC Data Protection Policy

7 - 9 What data do we really need?

This exercise explores the principles that guide responsible data use and data protection with a scenario-based approach. Two key concepts explored in the scenario are: *'data minimisation'* and *'privacy by design'*.

What is the 'need' throughout the data lifecycle? What data needs to be collectioned, what information needs to be provided to data subjects (and their communities), who needs to have access to the data, what needs to be done to secure it, does it need to be shared, and how long does it need to be kept before being deleted.

- **People:** 4 to 20 people
- **Time:** 60 Minutes
- **Difficulty:** intermediate
- **Virtual Materials:** virtual meeting platform, shared document/writing space
- **In Person Materials:** flipcharts/noteboards, sticky notes, markers

EXERCISE

Part 1: Explore

In plenary, Introduce the data lifecycle and summarize the objective of the scenario: discuss 'what is the data we really need?'

Part 2: Review

Scenarios are most effective in small discussion groups. In groups, participants should introduce themselves, assign a note-taker. Review the scenario:

Regular/ Ongoing Data collection

Your NS runs a local health clinic. In order to better predict the needs of the community, plan for resources needed and to gauge satisfaction with the services, you regularly collect data from individuals that visit the clinic. You explained the reasons for the data collection to families in the community. You also informed them that if they did not want to provide some of the information, they could still access the healthcare services. Thus, consent was the legal basis relied upon for data collection, at least with respect to patients that did not have medical emergencies.

- What data would you need to collect in the above scenario (understanding that we are not medical or procurement experts)?
- Once you've assessed the needs, what should you do with the data that was collected?

Just before you start collecting data, you get a call from colleagues who inform you that there is a planned cash intervention in the works targeting the same community. They want you to ask a few more questions so that they do not have to come back to the families in the future.

- What additional information would be needed for the cash intervention?

- What additional information, if any, should you provide to the individuals about the data you want to collect regarding the cash programme?

A local NGO learns about your work and wants access to your data to inform its own interventions.

- Do you need to share the data?
- What information needs to be shared if you decide to?
- What additional information (or choices) should you provide to individuals before sharing?

A new IT staff member notifies you that the database of personal data is available for access by anyone in the NS, and further is hosted in an unprotected cloud server.

- Who needs access to the data?
- What should be done to ensure it is securely stored?

In a positive turn of events, the local government has completed a new hospital and has secured funding to provide long-term healthcare to the community. Your NS can close the clinic and focus on other initiatives.

- What data needs to be kept?
- How long and in what form should it be kept?
- Can we use that data for other purposes?

Part 3: Discuss

In plenary, ask for reflections and questions. Share further details about the organisation Data Protection policy. See the IFRC Data Protection policy.

Extra Credit

This is a short exercise to discuss the high level concepts. If the team has more time, have participants share examples directly from their work related to the two concepts 'data minimisation' and 'privacy by design'.

Credit

Tom Orrell, James De France

7 - 10 What *can* we do vs. What *should* we do?

Part of understanding what responsible data use and data protection mean in a humanitarian setting is being able to recognise the difference between ethical dilemmas (responsible data good practices) and legal issues (data protection). This exercise is designed to break these concepts down into more relatable content by reframing data protection requirements vs. ethical dilemmas as 'what CAN we do' (data protection requirements) vs. 'what SHOULD we do' (responsible data practices).

This exercise is primarily targeted at participants who have limited knowledge and understanding of responsible data and data protection and want to expand their knowledge. At the end of the exercise, participants should be able to identify the differences between data protection requirements and responsible data good practices, and what that means for how they should approach particular situations.

- **People:** 4 to 16 people
- **Time:** 60 Minutes
- **Difficulty:** Easy
- **Virtual Materials:** virtual meeting platform, shared document/writing space
- **In Person Materials:** flipcharts/noteboards, sticky notes, markers

Exercise

Part 1:

In small groups (ideally pairs), discuss: what do data protection and responsible data use mean to you? How does this apply to our work?

Take notes on any insights or questions on a shared document.

Part 2:

Review the scenarios and discuss: "What ***can*** we do? vs. What ***should*** we do? Each group should try to do 2 scenarios.

Scenario 1: A friend working at a partner organisation asks you for some data your colleagues recently collected about HIV cases in a particular locality. They plan to offer additional medical/psychosocial support to the community and need to know where to focus their activities.

Can you share the data? Would sharing comply with data protection requirements? If so, should you share the data? Why or why not? If you decide to share, what considerations should be made before providing the information? What if there was a particular danger of violence or stigma against HIV positive individuals in the community? What if your friend worked in the government? And, even if we remove the identifying data, are there still risks of sharing?

- Where would you turn to find out what you could do?
- What should we do? Even if the rules permit it, are there other reasons to not share?
- What shouldn't we do? And why?

Scenario 2: You recently collected some data from a local community in an emergency that contains names, addresses and other identifiable information. Your tablet/laptop was running out of battery so you made a quick back-up on a flash drive without protecting the data in any way (no password or encryption). You get back to the office and you realise you've lost the flash drive. What do you do? What steps could you take before going to collect data to ensure that even if you lost your back-up drive, the data would still be safe?

- What can we do?
- What should we do?
- What shouldn't we do?

Scenario 3: Your office is approached by a large tech company that offers to help you manage your office's data for free during an emergency. Should you accept this offer?

(Options: Tech company #1 has a long and well-reputed history of contributing to humanitarian emergencies and doing charitable work; tech company #2 has large contracts with governments and other companies that could be seen as not respecting privacy or other human rights.)

- What can we do?
- What should we do?
- What shouldn't we do?

Part 4:

Discuss results in plenary. Ask what other ethical dilemmas they should consider.

Extra credit

Review your organisation's Data Protection Policy with participants. Invite your IT focal point or Security officer to share about digital and data risks after the scenario exercise. This might provide real context to your National Societies' work.

Resource

Digital Dilemmas

IFRC Data Protection Policy

Credit

Tom Orrell, Heather Leson

7 - 11 Data Protection nightmares

Which one of these scenarios might keep you up at night?

- **People: 4** to 12 people
- **Time:** 60 Minutes
- **Difficulty:** Easy
- **Virtual Materials:** virtual meeting platform, shared document/writing space
- **In Person Materials:** flipcharts/noteboards, sticky notes, markers

Instruction:

Break people into small groups and get them to consider if any of the following might keep them up at night. After they have identified potential nightmares, bring them back to the large group to talk about the data protection policies in their organisations.

Exercise

Part 1: Explore

Break people into small groups and get them to consider if any of the following might keep them up at night:

1. We didn't get consent
2. We don't have adequate data storage procedures
3. Every now and then one of our laptop/devices goes missing
4. We failed to backup our critical data
5. We missed the bias in our data
6. We might have unauthorized data access
7. We are not clear about which data might be sensitive
8. We've been sharing/posting Personal Data (Identifiable information) and didn't realise it
9. People have opted out of having their data used, but we used it anyways
10. Our data policies aren't robust enough

Ask: Are there any other scenarios that might keep you up at night?

Part 2: Discuss

After they have identified potential nightmares, bring them back to the large group to talk about the data protection policies in their organisations. Share the Data Protection policy of your organisation. Address any outstanding questions that might need resolution with your team. This can also be used with Digital Transformation planning to identify organisational and team needs. See - digital.ifrc.org.

Credit

Dirk Slater

7 - 12 Would you Share it?

Responsible data sharing can be tricky to operationalise. While sharing information is vitally important to emergency and humanitarian work, there is often hesitancy and uncertainty about what should or shouldn't be shared, keeping in mind data protection needs. This exercise is designed to help participants better understand the basics of data protection and data sharing and how they intersect. The session was inspired by work being undertaken by a National Society to train Emergency Response Unit (ERU) staff pre-deployment.

The first part of the exercise hopes to equip participants with a more grounded understanding of responsible data use, data protection and data sharing by building on individuals' own perceptions of what information about themselves they would or wouldn’t be comfortable sharing. The second phase raises scenario-based group discussions which replicate real-world humanitarian examples in which data sharing questions arise. These scenarios can either be sourced from the participants themselves as part of the exercise, or introduced by the facilitator if there is a specific issue that needs to be addressed.

- **People:** 4 to 12 people
- **Time:** 60 Minutes
- **Difficulty:** Intermediate
- **Virtual Materials:** virtual meeting platform, shared document/writing space
- **In Person Materials:** flipcharts/noteboards, sticky notes, markers

Exercise

Part 1: Would You Share It? 30mins

Divide participants into small groups of no more than four and ask them to discuss and respond to each of the statements (below). Each individual should respond to the statements and answers should be based on individual preferences. This part should take about 10 minutes to complete. The content could be placed in a table or diagram (depending whether the event is virtual or in person.) Participants are encouraged to share examples from their personal life and work examples. Take notes on any insights or questions on a shared document. For the purposes of this exercise, please focus on personal data (i.e. data that alone or with other data can be used to identify a natural person).

Statement:	Answers:
It is useful to share this kind of data:	
I want to share this kind of data:	
I don’t want to (or won’t) share this kind of data:	
I don’t want to (or won’t) share this kind of data:	
I have no choice but to share this data:	

Once the full group reconvenes, ask participants to review each other's answers and ask them to comment on similarities/differences. You may want to ask participants how their answers could change if they lived in a conflict or disaster setting. This part of the exercise will likely take about 20 minutes.

Part 2: Scenario-Based Learning (45-60 mins)

For this part of the session, there are prepared scenarios (below). Or, you can create your own organisation specific scenario. It is recommended to do this well in advance with a teammate.

Example Scenario 1: Branch Data

As part of a previous relief effort, your NS branch collected data on beneficiaries that sought medical care for an infectious disease. The collected data is stored in an Excel file containing the following fields: ID number (which is not an official ID, but a number assigned by your NS branch), medical condition, age, region and village, number of children in household, education and phone number (if the individual had one). You have been asked by the local government health department to provide the data on the individuals. What type of data would you share or not share? Why? What are the benefits (or risks) of sharing this data?

Example Scenario 2: Cash and Voucher Assistance data

In the aftermath of an earthquake a National Society tries to identify the people that have lost their homes as they may qualify for cash or voucher assistance. An association in the most affected village offers to share a list of persons currently without shelter due to the earthquake. What information would you ask the association in the village to share with you? What kinds of issues do you think might arise - e.g. how the association itself collected the data, how trustworthy it will be, etc? What steps could you take to mitigate these challenges?

The session should start with the group defining a typical list of data types that might be shared during the scenario. Also, they should make a list of what kinds of data should not be shared. This provides a way to ensure that people have a shared journey as they walk through the scenarios. (Note: Not all questions may be applicable or you may be lacking some information.) Take notes on any insights or questions on a shared document.

Question	Response
Who needs the data? What is their role? What is the purpose of sharing?	
Where does the data come from? Who has access to it? Is it possible to openly publish the data?	

Question	Response
Who can share the data?	
Is there a record of data sharing in the system and/or for the organisation?	
Is there a data sharing agreement/MoU in place with the party that the data was shared with?	
If personal data is being shared, what additional things do you need to consider? Can you aggregate, pseudonymize or anonymize the data? Can/should you remove certain fields?	
Is there a terms of service and license for the data?	
What capabilities for import, export and exchange of data are required and in which format?	

Extra credit

Optional: Creating a new scenario: Teams may create their own scenario for this exercise. It is recommended to do this well in advance of the session with teammates.

- Get people talking about real-world data sharing issues. The method uses scenarios as examples: either real-world or illustrative. The interactive component provides the means to visualise the steps and actions to 'simulate' decision-making. Provide them with an example. Often, it might be best to have someone from the team prepare this in advance of the session.
- OR/ Drive a conversation around the 'implementation steps' and 'requirements' to share data.

Credit

Dirk Slater, Heather Leson, Arturo Garcia, Melissa el Hamouch, Tom Orrell, James De France

7 - 13 Data Hygiene Checklist

These are categories of data to consider when assessing data protection needs.

Data Categories	Notes
Basic identity information such as name, location (address, community, etc.) and ID numbers	
Web data such as location, IP address, cookie data and RFID tags	
Health and genetic data	
Biometric data	
Racial or ethnic data	
Political opinions	
Sexual orientation	

The second part of this analysis is to match the categories of data to the formal terms below:

Data categories	Dataset	Notes
Non-personal data	E.G. logistical data such as number of vehicles a national society has	
	Etc	
Personal data	E.G. Names and addresses of families receiving support in the community	
	Etc	
Sensitive data	E.G. Biometric data, health data, racial or ethnic data	
	Etc	
Sensitive group data	E.G. Photographs/satellite images from which vulnerable groups of people might be identified - e.g. refugee camps, indigenous peoples' villages	

7 - 14 Wheel of Data Misfortune

The Wheel of Data Misfortune might help spark discussion while highlighting data protection and data literacy issues. Use this as an interactive introduction to the organisation Data Protection policy.

- **People:** 2 to 24 people
- **Time:** 30 Minutes
- **Difficulty:** Medium

Making the wheel

Time to make: Not more than 2 hours

Supplies

- 8 colours of large poster board paper
- Scissors
- Stick glue
- Bracket for spinning

Measurements: 50 × 50cm

17 sections, about 3-4 per quarter

Identify

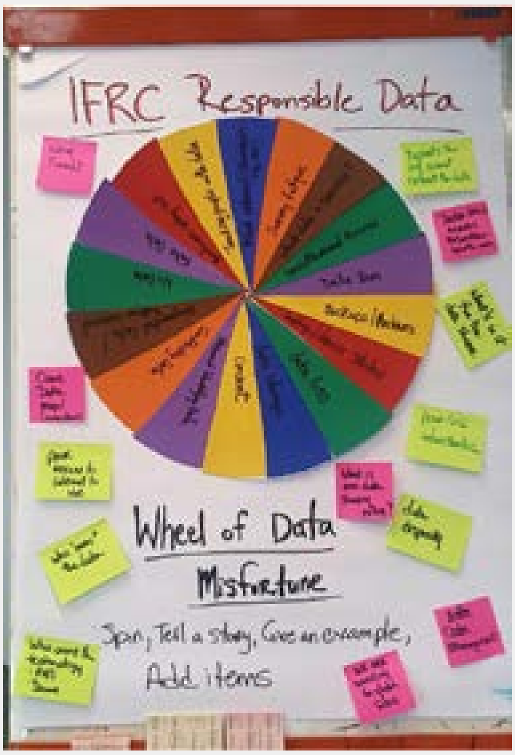
Identify 17 Categories. The 17 below are highlighted as examples, feel free to choose and remix given the context of your participants

1 Consent
2 Data storage
3 Data loss
4 laptop/device stolen
5 Backups
6 Data bias
7 Archive plan
8 Unauthorized data access
9 Understanding which data is sensitive
10 Survey fatigue
11 Are there external standards (e.g. IATI) that we should be adopting?
12 Personal Data (Identifiable information)
13 Tracking people with data
14 Affected person opting out/objecting to data use
15 Bad/Fake data
16 No data
17 Government data request

Exercise

- Have all the categories selected
- In the Session open up the discussion by having someone spin the wheel to determine the topic. Ask if people have a story or question on it. (Do a few rounds to get the conversation started, then turn it over to other key topics that they think are missing or are top priorities from gaps to opportunities.)

After the session, leave it in the hallway (or on a digital version) with some notes asking people to anonymously share their data stories or responsible data issues that they think are a priority.



Resources:

- How to Build a Wheel of Fortune Wheel (with Pictures) – wikiHow
- How To Make Pinwheels – Paper Source
- How We Made Wheel of Fortune From Cardboard – PLAYTIVITIES

Credit

Heather Leson

7 - 15 PMER Data Simulation

In this session, we will use an example emergency to guide conversations on risks, roles, decisions, gaps and evidence needs for our work. This should be used with Strengthening Data Teams and Projects (3) (Module 3).

Scenario: Mass deportation of migrant workers from Randowsa

The country Randowsa is reliant on regular and irregular migrant workers. The Randowsa Government has policies in place to prevent irregular migration and workers from working without necessary documentation.

Due to recent political instability, the Randowsa Government is enforcing their policies around irregular migrant workers, which has prompted fear of arrest or deportation amongst migrant workers. Over the past seven days more than 400,000 people have left the country in fear – many voluntarily, some deported, and companies are being fined large amounts if found to have employed irregular workers. Many of the migrants have crossed the border into Dakandka. There is a growing camp forming and RCRC is ramping up activities to support the complex mandates.

PMER has been engaged to support the various sectors' efforts on survey design with the NS as well as planning the mobile data collection process. You are leading a mobile data collection project involving multiple National Societies. Data processing takes place in the country as well as by remote help via Surge Information Management Support (SIMS teams) in National Societies as well as a 3rd party processor (a research group). Regular health, shelter, wash, and PSEA surveys are conducted to collect comprehensive information with key informant interviews. Each of the surveys is different and run by different National Societies. You recently completed a review of all the various surveys. The report has generated a lot of interest. Most partners are concerned with the worsening situation although some are sceptical of the numbers. The government is especially critical of the numbers.

Exercise

Each team of 3 to 4 people has 30 minutes to make decisions and tackle the key questions.

Key Questions

- What are some of the risks, gaps and needs? How will you safeguard the data workflows to protect the most vulnerable?
- What are some of the steps, roles, and decisions in this initiative?
- What is the minimal data set that can be shared and with who? Why?

Your Decision Points

You received a request for the data for the last round from the following partners. Should we be sharing the data with this actor? And at what stage of the process would you do so? How will you manage/share the data with outside providers?

1. The IFRC PMER unit wants to look at the data to see if they could make a compelling graphic from the data to accompany a press release that will be made about the worsening situation. They requested the full data set.
2. The Office of the Governor and the worst affected regions identified in the latest round of the survey say they would like to take action and need the data.
3. The project officer from the donors would like to see the data.
4. One of the key informants/community members who took part in the survey and feels your report did not accurately capture the problem in their area.

Credit

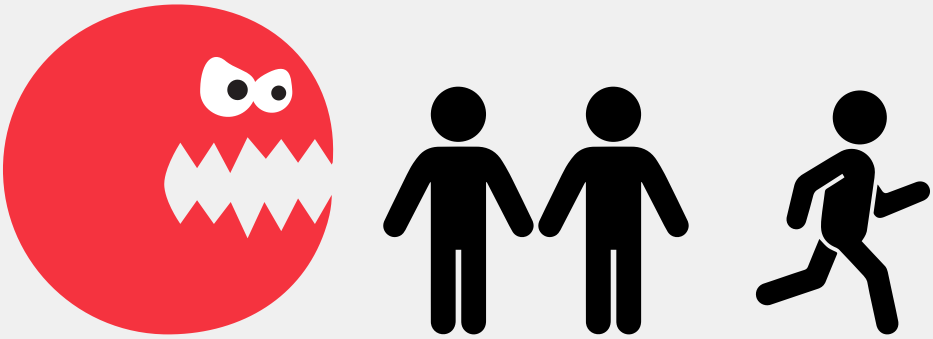
IFRC Migration team, Heather Leson, Miki Tsukamoto

7 - 16 People Before Data (handout)

Credit

Jennifer Chan

The Past



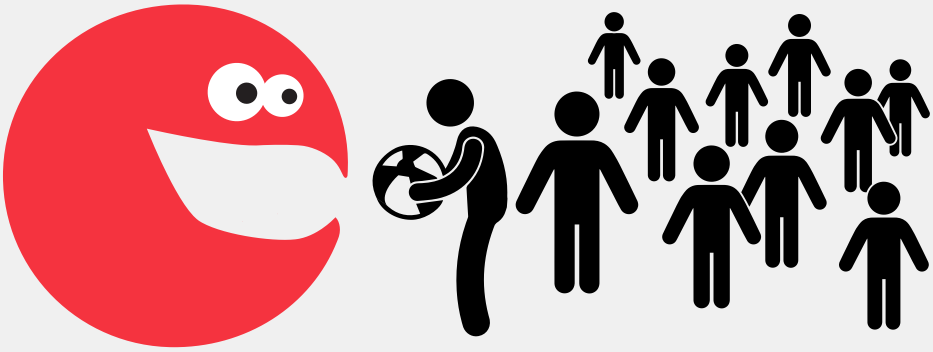
Data Collection

Maybe now

Data Metrics

People and Data learn to talk

The Future



Data Metrics

People harness data for a purpose and meaning

7 - 17 Polio Campaign Monitoring In Syria

Scenario

Qatar Red Crescent Society works as a third-party monitor for a polio campaign in Syria. It is supported by the World Health Organisation (WHO).

As you review the scenario set out below, please consider the following questions regarding what data protection (notably, information provision) and data responsibility measures should be considered throughout the campaign.

- What are some of the risks, gaps and needs to support the campaign? How will you safeguard the data workflows to protect the most vulnerable?
- What are some of the steps, roles, and decisions in this campaign?
- What is the minimal data set that can be shared and with whom? Why, and what issues should be considered before sharing?
- Should we rely on consent for data collection, and if so how will it be acquired?
- How should the data be stored and, if necessary, transmitted?
- Any other data protection or responsible data concerns?

The team's workflow is as follows:

1. Prepare data collection forms on paper. (Note: Be sure to clearly define which data can and should be collected. Adhere to applicable data protection guidance (laws and/or policies.)
2. Input data fields into the data collection platform (DHIS2).
3. A monitor collects data from centres and communities.
4. A supervisor, responsible for leading a team of monitors in a defined reporting area, provides updates to the district supervisor.
5. The district supervisor may then provide aggregated reports on the campaign.
6. Reporters analyse the collected data and extract pre-defined reports to show vaccination indicators which are then shared with the WHO and immunization Task force.

Third-party monitoring is working on three main stages during the campaign:

1. Pre- Campaign (visits centres and check in centres, vaccine and vaccination team preparedness).
2. Intra-Campaign (during the campaign, monitors check the vaccination progress in centres and make visits to homes and marketplaces to monitor vaccine coverage).
3. Post-Campaign (after the campaign, monitors make visits to homes and marketplaces to collect data about the coverage of the campaign).

We usually visit vaccine centres one or two days before the campaign to check the centre's and team's preparation, and make sure that everything is going according to plan.

Also, we pick random people from markets and ask them if they know anything about the campaign and the vaccine and where they heard about them.

Background

In March 2016, in pre-campaign stage, an independent body for the besieged area of Homs, analysed the data and found something wrong with the vaccine vials. We sent pictures of the vials to WHO, and they decided to close the campaign until they have a new vaccine.

The importance of the pre-campaign stage isn't just to check the vaccine and vaccination team, it's also about gathering information from a targeted place, to measure people's knowledge about the campaign and vaccine.

In August 2017 pre-campaign indicators showed a decrease of knowledge about the campaign. 40% of people didn't know about the campaign that was supposed to start the next day! Therefore the campaign was postponed for another week.

Credit

Hesham Othman Hassan and Nami Ghadri, Qatar Red Crescent Society

7 - 18 Data Monologues

A “Data monologue” is a summary of a ‘data project lesson’ or ‘data fail.’ People provide the scenario, issues, mitigation steps and results.

RESPONSIBLE DATA IS:

“Data responsibility in humanitarian action is the safe, ethical and effective management of personal and non-personal data for operational response.”

Data Protection:

Data protection means a set of principles and practices put in place to ensure that any personal data collected and used by, or on behalf of, the Federation is accurate and relevant, and that the personal data is not misused, lost, corrupted, or improperly accessed and shared. (IFRC Policy on the Protection of Personal Data)

Protecting the Personal Data of individuals is an integral part of protecting their life, integrity, and dignity. This is why Personal Data protection is of fundamental importance for Humanitarian Organisations. (Brussels Privacy Hub/ICRC Handbook on Data Protection, ICRC, 2017)

Session Goals

The following is a 1 hour to 1.5-hour session to help you and your team talk about Responsible Data Use and Data Protection Guidelines. Goals for this session:

- Build advocates and expertise to support responsible data use in humanitarian response.
- Build a common language around responsible data use.
- Foster data protection and responsible data literacy for the RCRC
- Introduce Data Protection Policies, get input for training needs
- Introduce the Handbook on Data Protection in International Humanitarian Action (2nd edition, ICRC/Brussels Privacy Hub Publication)

- ► **People:** 12 to 24 people
- ► **Time:** 90 Minutes
- ► **Difficulty:** Easy
- ► **Virtual Materials:** virtual meeting platform, shared document/writing space
- ► **In Person materials:** Flipcharts/noteboards, sticky notes, markers
- ► **Preparation:** Ask 3 to 4 people to help guide the session. Explain the goals, formats and outputs for the meeting. Assign them to different areas of the space.

- Arrange chairs or desks in circle or in small groups/Use virtual session breakouts
- Place welcome signs on the door/ have a shared documentation space
- Each group will need:
- Assigned facilitator
- Dedicated note taker (s)
- Example scenarios in print and digital formats
- Welcome everyone as they join. Ask people to put away their laptops and phones. Start and stop on time.

Sharing in a Healthy Manner

- It would be advisable to encourage a safe place using "Chatham House rules" – focus on the topic and lessons rather than the people/organisation/division.
- "a rule or principle according to which information disclosed during a meeting may be reported by those present, but the source of that information may not be explicitly or implicitly identified"

Provide participants with the following summary: The session objective is to share with and update participants about the increasing attention given to responsible data practices, including the ICRC Handbook on Data Protection in Humanitarian Action, the IFRC Data Protection policy, IATI, and related topics.

Background for the session: easier and faster data processing of increasing quantities of personal data have given rise to ethical concerns about balancing transparency and open access to information with issues of confidentiality and the possible intrusion into the private sphere of individuals. Organizationally, this requires attention to responsible data practices, data protection planning and overall data literacy, transparency and confidentiality. Thus, organisations like IFRC, ICRC, CRS, Oxfam have either published or are working on data policies. This session will share key lessons and considerations on this topic.

What is a Data monologue?

- A "Data monologue" is a summary of a 'data project lesson' or 'data fail.' People provide the scenario, issues, mitigation steps and results.
- The group will share some data-driven project stories, select the best example of a complex issue, then prepare a "pitch" to illustrate some fundamental questions/observations.
- The "Data Monologues" can include names of individuals or organisations removed. Chatham house rules apply (meaning – we will ask people not to share until permission granted). Participants will describe the problem, the risks, any mitigation measures taken, the results and what could be improved.

Part 1: Data monologues: Small group discussion (20 minutes)

- Breakout into groups of 4 to 5 people
- Share data stories for 20 minutes
- Each person shares an example of issues/scenarios they encountered.
- Try to use personal/ organisational examples, rather than third-party examples.

Part 2: Data monologues (40 minutes)

- Pick one of the examples to share in plenary including what happened, results and mitigation.
- The group facilitator documents the core questions/concepts on flipcharts.
- Return to plenary

- The “pitch” of the Data Monologue should be like a ‘Pecha Kucha’ or ‘ignite’ talk: summary, lessons, and next steps. A monologue should not be longer than five minutes. There will be 4 – 5 pitches.

Part 3: Adding Data Protection & Responsible Data Use (15 minutes)

- During the discussions, participants will inevitably discuss issues of consent, data breach, data sharing, data storage, data protection, and more.
- Prepare slides to illustrate these key terms.
- Provide resources to read more about implementation data protection and responsible data use into humanitarian work.

Part 4 Wrap-up (10 minutes)

- Finish with a quick go-round asking participants to share a single ‘aha’ or learning from the monologues before ending.

Post-Event:

- Collate the critical questions from the groups.
- The example “Data Monologues” should only be used again if permitted.
- Send thank you notes to the helpers and participants.

Resources

Heather Leson and PMER Network, IFRC Data Protection Policy, IASC Operational Guidance on Data Responsibility