Use of ‘sensitive’ data

Guidance for processing of sensitive data

Table of Contents

Rationale

A majority of Mercy Corps programs and other activities collect some kind of personal information about the individuals we serve and work with and many also collect information on individuals which would be classed as sensitive. The collection of sensitive data is essential for us to carry out our work and serve the program participants and their communities we work in Therefore, as we collect and use sensitive data, it is vitally important that all necessary steps are taken to ensure this data is protected. Failure to protect sensitive data can lead to serious harms to the data subject including but not limited to discrimination and security threats.

Scope

This guidance applies to all processing of sensitive data across the entire agency. It applies to sensitive data collected for programmatic purposes and operational purposes and any other situation where sensitive data is present.This document details the necessary steps whenever sensitive data processing occurs.

What is sensitive data and why is it different from other types of personal data?

Sensitive Data is usually data such as an individual's cultural profile, sexual orientation, health data biometric and genetic data. It is data which, if disclosed, accessed or shared improperly, could result in:

- harm (such as sanctions, discrimination and security threats) to a person, including the source of the information or other identifiable persons or groups;
- a negative impact on an organisation's capacity to carry out its activities or on public perceptions of that organisation.

Example 1:

A programme is working in a community and during the project, several participants reveal that they are HIV positive. This information is accidentally shared with senior members of the community resulting in the potential for significant harm and even physical danger to the programme participants.

Example 2:

An office is planning a celebration and is collecting dietary requirements from team members. Several team members have indicated that they require either Kosher or Hallal meals. A spreadsheet identifying which team members have specific dietary requirements is shared with the whole team. Some team members had not shared their religion as they are conserned about discrimination.

Sensitive data needs to be treated with greater care because collecting and using it is more likely to interfere with the fundamental rights or freedoms of an individual, or cause significant harm including discrimination or physical danger if it is misused.

The General Data Protection Regulation (GDPR) defines a number of data types which are categorised as special category sensitive data and details specific processing conditions for these types of data.However, it is important to note that in some contexts, data which falls outside the standard special category sensitive data may still be sensitive because of the particular context. For the purposes of this guidance note, these types of data will be referred to as contextually sensitive data.

This guidance note is designed to complement the Mercy Corps Responsible Data Policy as well as the Program Management Policy (which also incorporates the agency's MEL Policy) and applies to the collection of sensitive data in all contexts, including but not limited to HQ, programmatic and MEL data.

Definitions of Key Terminology

- **Mercy Corps Operational Data** – Any unit of information, composed of letters, numbers, symbols, images, video and voice recordings, geo-spatial coordinates or location identifiers, mapping or any combination thereof processed by Mercy Corps. This may include but is not limited data on Mercy Corps team members, vendors, donors or partners. Data exists in both digital and physical form.

- **Sensitive Data-**This information is often used as a basis for targeting a particular group or individual. Common examples are race, religion, political opinion, sexual orientation, health or biometric information.

For the purposes of this note, sensitive data will include ‘Special Category sensitive data’ as outlined in the GDPR and ‘Contextually sensitive data’

- **Special category sensitive data-** The GDPR sets out specific requirements for the processing of all special category sensitive data which must be met. The GDPR defines special category sensitive data as:
    - personal data revealing racial or ethnic origin;
    - personal data revealing political opinions;
    - personal data revealing religious or philosophical beliefs;
    - personal data revealing trade union membership;
    - genetic data;
    - biometric data (where used for identification purposes);
    - data concerning health;
    - data concerning a person’s sex life; and
    - data concerning a person’s sexual orientation
- **Contextually sensitive data** - data which does not fall into the categories of sensitive data as defined by the GDPR but which due to the context in which it is processed is sensitive in its nature and which could cause significant harm to the data subject if disclosed.
- **Personal data breach** – A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.
- **Program Data** – Any unit of information, composed of letters, numbers, symbols, images, video and voice recordings, or any combination thereof related to program participants, implementation, and outcomes. Data exists in both digital and physical form.
- **Mercy Corps Responsible Data Policy** – Agency policy intended to set principles for the transparent, secure, and responsible use of personal data across the agency and incorporating those principles into our daily work.
- **Informed Consent** – A process for gathering voluntary permission to collect data of any kind, based upon a clear appreciation and understanding of the facts, implications, and consequences of any engagement from participants. This agreement may be given either by a written or oral

statement or by a clear affirmative action. Agreement must be obtained at the time of Personal Data collection, or as soon as reasonably possible thereafter.

- **Explicit consent** – Explicit consent requires a very clear and specific statement of consent. A record must be kept of when and how consent was obtained and exactly what data subjects were told when consent was obtained. Explicit consent must specify the nature of the special category data; and it should be separate from any other consents you are seeking.

- **De-identification** – Any data processing activities or methods that work to prevent a participant or other person's identity from being revealed directly and/or indirectly. Example types: Anonymization (i.e., removing certain amounts of Personal Data, or applying a range of values across certain sets of Personal Data) and Pseudonymization (i.e., processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject or household of data subjects without the use of additional information such as unique IDs or hashes).

- **Personally Identifiable Information (PII)** – Information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity. This is closely related to **Demographically Identifiable Information (DII)** which can be used to identify a community or distinct group, whether geographic, ethnic, religious, economic, or political.

- **Stored Securely** – Only necessary Mercy Corps team members are able to access the data; steps are taken to prevent theft and misuse of data. Stored Securely – Only necessary Mercy Corps team members are able to access the data; steps are taken to prevent theft and misuse of data. A file is stored securely when:
  - It lives in a platform that has/meets strong security, data protection and privacy standards
  - Access is restricted to required parties only
  - Access is regularly reviewed and adjusted as needed

- Additional requirements are set forth for Mercy Corps' programs in the newly adopted MEL Policy, particularly the Standard 9, requires all programs to ensure safe handling practices, in line with the Responsible Data Policy and donor requirements.

- **Necessary Mercy Corps Team Members** – Team members who require access to the identified information in order to fulfill tasks specific to their job, such as serving the needs of program participants and completing program deliverables

- **Data Subject** - Any individual from and about whom data is collected directly, indirectly or through a third party, and who can be identified, directly or indirectly, in particular by reference to Personal Data.

- **Data Protection** - Safeguarding and preventing unauthorised access, use or distribution of personally identifiable information (PII), demographically identifiable information (DII), and other sensitive data about an individual or a group across the program or project management data cycle, or after the completion of the program or project. Mercy Corps' Responsible Data Policy outlines

data protection requirements, and the agency is also subject to other legal/regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR).

For more definitions related to responsible data, see the Responsible Data Definitions document.

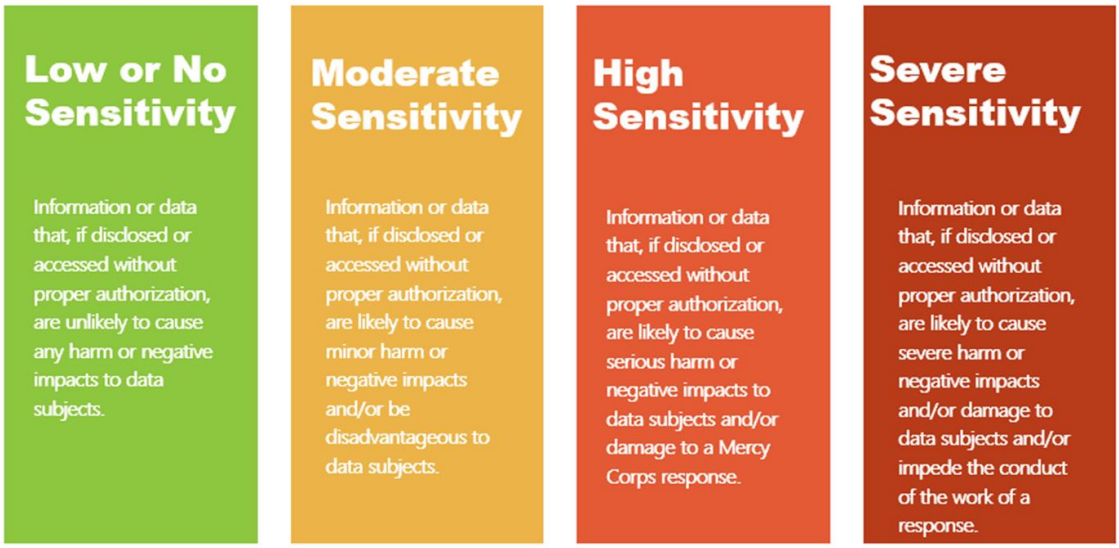
Planning

- Consider which types of data will be collected and document this at the planning stage of the project, in the Privacy Impact Assessment (PIA).
- Where a plan includes the collection and/or documentation and/or storage of any kind of sensitive data, particular consideration should be given to how and why the data is used. Consider whether the collection of this data is necessary to deliver the required outcomes of the programme or project or if an alternative type of data would be sufficient. Only if it is necessary should sensitive data be collected. Please note that collecting sensitive data, if done well, is an expensive process. By elevating the burden of unnecessary data collection, you are allowing teams to save time and resources for other necessary work. If you identify that PII is necessary, do not implement shortcuts. If your resources allocated for collecting and managing sensitive data are not enough to do it well, please reconsider weighing in all the risks that you may cause to the communities you work with.
- Consider which technologies will be used for collection and storage. Technologies used must include appropriate safeguards for the collection of sensitive information.
- Generally speaking, the more sensitive the data, the more safeguards you need to have in place. Sensitive data will usually be of either 'High' or 'Severe' sensitivity (see figure 1). Additionally the more data sets collected, the greater the risk and the more safeguards there should be. Examples of safeguards include but are not limited to:
    - Encryption
    - Pseudonymisation
    - Disassociation
    - Storing paper files in locked cabinets with restricted access
    - Storing files on Mercy Corps servers with protection levels
    - Restricting access to Mercy Corps devices and only to those who must have access in order to complete their job duties
    - Ensuring devices such as laptops are locked when not in use
    - For spatial data randomise or aggregate GPS points

- Be clear about which legal basis for processing sensitive data you will be using and plan accordingly.

- Reporting requirements in grant agreements must abide by Do No Harm principles (e.g., the program is not expected to collect information that may compromise the safety of participants) and clearly outlines commitments and agreements for data sharing platforms, processes with donor, partners and other stakeholders, incorporating requirements for de-identification and anonymisation.
- Program-level data security protocol is part of the MEL Technology Plan (Standard 6) and outlines team member data considerations including permission levels and protocols for MC and non-MC team members.
- Where sensitive data is being collected for Mercy Corps Operational purposes, plan and outline data considerations including permission levels and protocols.
- Think about, and be able to justify, how long you need to keep data (retention period), this will depend on the reasons for collecting it, legal requirements, donor requirements and MC program record retention policies.
- Have a process in place for the destruction of data when retention periods are met.

Figure 1:



Planning for Data Collection

- A Privacy Impact Assessment is completed to identify and manage data privacy risks associated with any new activity, such as new programs, technology, or policies. Where sensitive data is to be collected, this must be reviewed by a competent individual. This would be the Data Protection and Privacy team, your DPO or per the MEL Policy, (Minimum Standard #9 - Data Privacy & Security):
    - Accountable -Country Director, or Director of Programs and Program Manager or Chief of Party

    - Recommended Responsible -Program MEL/Knowledge Management Lead

- Complete a Sensitive Information Assessment (SIA) which is related to the PIA. This should document all additional safeguards being employed for the sensitive data.
- If consent is the legal basis relied upon, Informed Consent requires that data subjects are advised of the following in plain language:
    - What data is being collected and why this is required
    - Who this will be shared with including any external partners and donors
    - Whether the data will be shared internationally
    - How long the data will be kept
- A record should be kept of when and how consent was collected and what the data subject was told. A template of what data subjects will be told to obtain consent should be included in the planning stage.

Data Collection

- Data collection protocol is in place for each instance of data collection which includes:
    - Additional safeguards for the sensitive data
    - Documented instructions for collection, data cleaning, review, and de-identification, as applicable.
    - Instructions for potential data security breaches for all quantitative and qualitative data collected (e.g., lost or stolen devices, compromised logins, etc.)
    - Instructions for the use and protection of hard copy forms during collection
    - Spot checks and monitoring of the extent to which safeguarding and protection protocols are adhered to by the data collection person/s
- All of the above should be linked to the SIA

Data Storage

- Files that contain sensitive information must be restricted to team members that need access to this information to complete necessary deliverables, and the systematic de-identification of sensitive information is conducted before linking to TolaData or sharing with any third party as relevant.The MEL Policy Standard 8 provides additional guidance on MEL data filing and storage best practises
- Data is stored in a location that is compliant with all relevant Mercy Corps policies (e.g., Responsible Data Policy, Acceptable Use).
- Sensitive data must be kept for no longer than is necessary. When retention periods are met data must be securely destroyed or fully anonymised.
- Retention periods must be documented and justified.

- Remember- data may also be stored in mobile data collection systems. All data storage considerations noted above apply to mobile data collection systems as well.

Data Analysis

- There is a protocol for sharing data with consultants, HQ teams, partners, stakeholders, including but not limited to data sharing agreements, approvals by Country MEL, roles and responsibilities, etc.

- Non-Disclosure Agreements (NDA) are signed by all consultants before accessing any datasets owned by Mercy Corps.

Data Submission to Donor, partner or other third party (if relevant)

- Raw data is de -identified and reviewed for compliance with Do No Harm principles prior to submission.

- Sensitive data must not be shared with any third party that was not mentioned as part of the informed consent process.

- Sensitive data must not be shared with any third party unless there is a Data Sharing Agreement in place.

- Only use authorised organisational systems such as Google Drive or Microsoft Sharepoint for sharing documents, not third party sharing platforms.

Frequently Asked Questions

To ensure we comply with diversity requirements, we ask team members to indicate their ethnic status on job application forms – do I need to do anything with that?

Yes, data on racial or ethnic origin is considered to be sensitive personal data so you will need to follow sensitive data guidelines and apply additional safeguards to that data.

What happens if me or a team member has accidentally, unintentionally shared sensitive data? What remedial actions can be taken?

Upon discovering accidental sharing of personal data, the data sharing should cease immediately. This could mean asking the accidental recipient to delete any copies of the data, removing the accidental recipient's access to the data, taking the data offline, or other steps as needed.

Accidental or unintentional sharing of personal data is considered a data breach and you must notify **it-security@mercycorps.org** immediately in line with the Incident Response Plan. As much information as possible should be provided, as soon as possible, about the nature of the data shared.

What should I do when I see a team member intentionally sharing sensitive data with someone who should not have access to this data?

Intentionally sharing sensitive data to an unauthorized person is extremely serious as it can lead to severe harm to the data subject and to the agency. If you see a team member intentionally sharing sensitive information in this way, you should report this immediately to the programme manager, regional director or to your director.

Sharing of sensitive data with those who should not have access is also a data breach, and should be reported to **it-security@mercycorps.org** in line with the Incident Response Plan immediately. As much information as possible should be provided about the nature of the data shared, as soon as possible.

How does the program decide who should/shouldn't have access to sensitive data?

Access to sensitive data should only be granted to individuals who need access in order to carry out their role. Sensitive data should always be masked before it is shared, if possible. Common examples of masking include anonymization or pseudonymisation.

What is disassociated data?

Disassociated data is data which has been completely and irreversibly detached from the data subject so that it is no longer possible to re-associate the data with a data subject. Disassociated data is a type of data anonymization.

Should I enable alerts on electronic dataset if it is accessed by an unauthorised individual?

If it is possible to trigger alerts for unauthorised access, these should always be enabled, however not all electronic platforms have this capability. Check system settings for your platform and if it is possible, enable alerts.

Should team members use personal devices to collect or store sensitive information? If so, what protections should be provided?

Personal devices should not be used to collect or store personal information, including participant information *unless appropriate device management software has been installed* and use of personal devices is captured on the project PIA. Personal devices must never be used for collection of participant data without the express sign off of the programme lead. Personal devices should not be used to collect or store sensitive information.

Can my donor audit how I handle sensitive data?

Yes, many donors require internal and also conduct external data quality audits and data quality assessments. One aspect of these assessments is to assess the MEL system for shocks, invasions and security, especially if the program is collecting sensitive information.

Do I link participant lists to TolaData as evidence?

Participant Lists (e.g., training attendance lists, etc.) can be linked as evidence since that evidence should be housed and stored outside of TolaData, thus only certain people will have access to that evidence, based on the permissions of that external storage facility. Consideration should be given to whether any type of evidence linked to TolaData requires inclusion of Personal Information. It is extremely unlikely that inclusion of sensitive information will be necessary.

How do I know if data collection or storage technology vendors or platforms are compliant with sensitive data requirements?

The existing data collection and storage platforms in the MEL Tech Suite are already compliant with sensitive data requirements, provided they are appropriately configured to use the safeguards and protocols noted in this document. If a platform outside the MEL Tech Suite is to be used, then a Privacy Impact Assessment (PIA) must be completed to assess whether it can be considered compliant with sensitive data requirements. In terms of assessing a technology vendor, and their willingness to be compliant with the Responsible Data Policy and sensitive data requirements, a PIA is again the best tool to determine if their practices will be considered compliant.

How do I tell if data is personal data or sensitive?

If you are processing data which falls into any of the special category sensitive data outlined by the GDPR (see **Special category sensitive data** above), this will always be sensitive data. If there is a context specific reason that data would fall into the category of 'Severe Sensitivity' (see Figure 1 above), this should also be classed as sensitive data.

Related Documents:

Consent

MEL Tool: Informed Consent Template (for Interview Participants)

Informed Consent Guidance for Sharing CARM Data

COVID-19 Remote MERL Guidance

Encryption

Using Ona.io at Mercy Corps: Encrypting Forms & Sensitive Data

Biometrics

Biometrics @ Mercy Corps: Internal Primer

General guides

- Data Responsibility Toolkit – A guide for Cash and Voucher Practitioners - https://www.calpnetwork.org/wp-content/uploads/2021/03/Data-Responsibility-Toolkit_A-guide-for-Cash-and-Voucher-Practitioners.pdf
- ELAN Data Starter Kit for Humanitarian Field Staff: v https://www.calpnetwork.org/wp-content/uploads/2020/06/DataStarterKitforFieldStaffELAN.pdf
- ICRC Handbook on Data Protection in Humanitarian Action: https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

De-identifying information

USDA Guidance for Reviewing Personally Identifiable Information (PII) in Project Evaluations

Poverty Action Lab 'De-identification for data publication'

Generating unique codes for programme participants or other data subjects

Draft guidance from T4D

Assessments

Privacy Impact Assessment (PIA)- template

Privacy Impact Assessment (PIA)- Guidance

Sensitive Information Assessment (SIA)