Guideline for DTM Coordinators
Identifying Sensitive Data and Inter-Organizational Data Sharing Pathways

Section 1 Guideline

Introduction

This guideline is to be used in conjunction with the Data Access Request Form for all organizations requesting sensitive, non-personal data from DTM. The purpose of the guideline is to facilitate inter-organizational data sharing while minimizing the risk of doing harm, by ensuring that:

- Sensitive data/information that should not be shared publicly have been identified and documented.
- A data-sharing process for safely sharing sensitive data from DTM to a 3rd party has been discussed and agreed.

This guideline relates to requests for data/information from DTM that fall under the IOM "Confidential" data classification category, as outlined in the table below.

Table A: IOM Data Classification Categories

IOM Data Classification Categories	Information Type / Disclosure Protocol
Public	Data that can be made publicly available because disclosure is associated with little or minimal risk to individuals, communities and/or organizations. This includes data that is aggregated (such as national aggregates of unaccompanied children numbers) and non-sensitive site-level data.
Confidential	Also known as "protected" by other agencies, confidential data are moderately sensitive, and cannot be shared publicly because disclosure could cause minor distress for an individual, put an individual or community at risk of a protection incident, or negatively impact upon an organization's capacity to carry out its activities. This includes (but is not limited to) protection data per site (such as # of unaccompanied children per site).
Secret	Also known as "restricted, personal, or confidential" by other agencies, this is composed of highly sensitive information that may cause serious distress or increase risk to an individuals' safety, or violate an individual's privacy. This includes personal data that could identify an individual (either on their own or if combined with other data sets), and protection incident/referral/case management information.

Identifying Sensitive Data

In order to determine the sensitivity level of a dataset/information type, it is recommended that the DTM Coordinator and a sectoral expert (either from within IOM or the requesting organization) perform a risk-assessment on the potential impact that disclosure of each

dataset/information type may have on individuals, vulnerable groups, communities, and stakeholders if obtained by the public or an unintended source before the data collection process, and repeated on a regular basis.

Borrowing from to the Protection Information Management (PIM) initiative[1], this risk assessment must be carried out at country level and repeated periodically, because data sensitivity is:

1. Contextual: What may not constitute sensitive data and information in one context, may be sensitive in another.

2. Temporal: Data may not be sensitive now, but may become sensitive in the future due to changes in context, such as shifts in conflict dynamics, or shifts in national Government policies (such as those affecting humanitarian access, and impacting upon the rights and/or safety of specific populations or vulnerable groups).

3. Relational: One dataset on its own may not be sensitive, however it could become sensitive if analyzed in combination with other dataset(s). (*for example "feelings of safety" questions per location may not be sensitive in a context, however if crossed analyzed with "presence of armed actors – military", the results may indicate that Government soldiers are responsible for decreasing the "feelings of safety", which would be sensitive to publish*).

Designing Inter-Organizational Data Sharing Pathway

When determining the data-sharing process for sensitive data, the degree of data protection must be considered based on the risk of sharing sensitive data vs the benefits of sharing the data (or the risk of not sharing the data). For IOM's "Confidential" data, it is recommended that the DTM Coordinator consider whether the data requester has a legitimate humanitarian need and defined purpose for the sensitive data.

When determining the method of sharing the sensitive data to a 3rd party organization, the DTM Coordinator must consider:

- Technology (online password protected platforms, vs password protected files sent in an email, including a plan to regularly change passwords)
- Identification of the focal point to receive the data at the 3rd party organization, and agreed processes for being notified of turnover/replacements
- Whether there are datasets that must be shared more urgently than others, and whether/how this can be accomplished given the capacity of the team (*for example: In Nigeria, UNICEF has provided a list of field staff focal points to DTM. When DTM identifies an unaccompanied child, the local UNICEF focal point is contacted within 48 hours).*

[1] PIM Initiative, http://pim.guide/

Section 2: Table To Be Filled in With Requesting Organization

Table B: Identification of Sensitive Indicators and Sharing Pathways

	Low Urgency *(to be shared when data is cleaned)*	**Medium Urgency*** *(to be shared before full dataset is cleaned)*
Timeline	• *[eg. Monthly]*	• *[eg. Within x days]*
Sensitive Datasets/information	• *Dataset/information* •	• *Dataset/information* •
Data destination	*[Insert 3rd Party Focal Point Title]*	*[Insert 3rd Party Focal Point(s)]*
Method for data sharing	*[Password-protected web portal] or [Password-protected excel sheets of raw data emailed to focal point]*	*[Password protected document/email]* *[Telephone call]*

**Information that must be shared with high-urgency falls within the urgent action process of referring a victim/survivor of a protection incident to a service provider within a referral pathway. The referral process mandates the sharing of personal information which is classified as "Secret" by IOM, and is therefore outside the scope of this guideline.*

Table C: Focal Points

Each organization should have a primary and secondary focal point. In the case of staff turnover, each organization is responsible for designating a new focal point, communicating the new Focal Point's contact details in writing to their counterpart, and doing a complete handover on the inter-organizational collaboration history and ongoing data sharing agreements. A new focal point does not necessitate a revision to this guideline.

IOM DTM	***[Requesting Organization]***
Primary Focal Point Name: Title: Mob: E-mail:	*Primary Focal Point* Name: Title: Mob: E-mail:
Secondary Focal Point Name: Title: Mob: E-mail:	*Secondary Focal Point* Name: Title: Mob: E-mail: