

Ne pas nuire: Comment ne pas nuire lors de la collecte, du partage et de l'analyse des données ?

1. Actions recommandées.....p 1
2. Liste de contrôle.....p 2
3. Questions directrices propres à chaque étape du processus de traitement des données.....p 3 et 4

1. Actions recommandées

- L'équipe DTM procède à une première évaluation globale des risques de l'exercice dans son ensemble et décide comment procéder en fonction des résultats. Cette évaluation sera renouvelée au besoin si la situation évolue ou si de nouvelles informations pertinentes mettent en évidence un risque ou un changement de contexte. L'évaluation des risques sera idéalement réalisée avec le soutien des collègues de la Protection.
- De plus, l'équipe DTM, les experts du contexte, les experts en traduction, les responsables de la Protection et les experts en sécurité prennent conjointement en **considération les conséquences de chaque question lors de la conception du questionnaire DTM**. Avant d'inclure une question dans les questionnaires, ils veillent à ce que cette **question soit sûre et ne mette personne en danger**. *Ils peuvent utiliser la liste de contrôle en page 2 et les questions directrices approfondies en page 3.*
- Concevoir des questions qui ne nuisent pas signifie prendre en considération les risques potentiels pour **toutes les parties prenantes** (enquêteurs, informateur clé, communauté, organisation...) à **toutes les étapes du processus**, y compris lors de la collecte, du stockage, de l'analyse, de la diffusion et de l'utilisation des données. Il est essentiel que la DTM et les partenaires de la Protection prennent en considération les éléments suivants lors de la conception des outils de collecte et d'analyse des données :
 - Le contexte sécuritaire / politique et la dynamique du pouvoir. Est-ce que le fait de poser certaines questions peut mettre en danger un enquêteur, un informateur clé, une communauté ou un accès humanitaire ? Cela peut-il créer des soupçons quant au motif réel de la collecte de données ? Cela peut-il entraîner une stigmatisation des personnes interrogées ou de la communauté ? Cela peut-il les exposer à des représailles, à des interrogatoires ou même à des sanctions par la marginalisation des groupes armés par le reste de la communauté ? Cela peut-il entraîner le refus d'accès du programme d'intervention à la communauté ?
 - La complexité ou le caractère sensible des questions par rapport à la capacité de procéder à un contrôle qualité sur le terrain. Les enquêteurs reçoivent une brève formation préliminaire sur la Protection de l'Enfance, la Violence Basée sur le Genre (VBG) et la Protection, mais ils ne sont pas formés à collecter des données sensibles généralement recueillies lors d'évaluations spécialisées.
 - L'impératif humanitaire. La collecte de données DTM a souvent une couverture géographique bien plus large dans un pays que les partenaires qui peuvent y répondre. Cela signifie que les questions seront posées dans des sites disposant de capacités d'intervention ainsi que dans des sites sans capacités d'intervention. Il est donc important d'évaluer l'équilibre entre les avantages/risques liés au fait de poser chaque question dans des zones dépourvues de capacité d'intervention par rapport à la nécessité d'obtenir des données auprès des zones non couvertes pour plaider en faveur de l'expansion du programme / financement de l'intervention.
 - Divulgaration d'incident. Le DTM ne collecte pas de données sur les incidents de protection, mais demandez-vous si la question pourrait conduire à une divulgation d'un incident de protection : Un mécanisme de référencement est-il en place ? Devriez-vous demander ces informations ? Les enquêteurs ont-ils été formés au processus de l'Action Urgente ? (voir les Urgent Action Process Guidelines for DTM (Directives relatives au processus de l'Action Urgente pour la DTM) à l'adresse : <https://displacement.iom.int/dtm-partners-toolkit/data-sharing-guidelines>).
 - Recenser les questions qui nécessitent une formation supplémentaire pour les enquêteurs DTM, en particulier en ce qui concerne la sensibilité, la terminologie, ou quand il est important que les enquêteurs sachent qu'ils ne doivent pas énumérer les options d'intervention potentielles.

- Les données DTM sont partagées avec les partenaires, soit publiquement, soit dans le cadre d'accords de partage de données. Il est donc crucial de prendre en considération les conséquences que peuvent avoir les données partagées pour la population, les organisations et le personnel également lors de la conception des outils de collecte de données. Pour chaque question incluse dans le questionnaire, nous devons évaluer les avantages et les risques, dans le contexte actuel et futur potentiel. Les collègues de la Protection peuvent apporter un soutien précieux dans cet exercice, et la DTM travaillera idéalement en étroite collaboration avec eux.
- Pendant la mise en œuvre, il est important que les enquêteurs puissent informer la DTM lorsqu'ils n'ont pas pu poser une question, sans que cela n'entraîne de conséquences négatives pour la sécurité de leur emploi. Un feedback concernant de tels cas déclenchera une modification du questionnaire et sera signalé aux partenaires ayant initialement demandé ces informations. Cela améliorera la qualité et la fiabilité des données.
- Pendant et après la collecte, l'analyse et le partage des données, la DTM et les partenaires doivent également observer les conséquences (bénéfiques, risques...) du partage de données. Ces informations serviront à réviser le questionnaire et les modalités de partage des données et, dans certains cas, elles peuvent déclencher une nouvelle évaluation des risques de l'ensemble de l'exercice.

2. Liste de contrôle : Concevoir des questions DTM de façon à NE PAS NUIRE

Orienter les questions et les actions à utiliser par la DTM et les partenaires lors de la conception d'un exercice DTM, afin d'évaluer les risques et de décider comment procéder. Cette liste de contrôle doit être utilisée conjointement avec le **Interagency Sensitive data sharing guideline**, et le **Framework for Data Sharing in Practice**, tous deux disponibles dans le dossier de la Boîte à outils DTM et partenaires dédié au partage de données¹.

1. Prenez en considération l'UTILISATION de l'ensemble de données :
 - ✓ Quelle action humanitaire sera menée sur la base de ces données ?
 - ✓ Quelles sont les conséquences probables sur la sécurité, la dignité et le bien-être du bénéficiaire si nous collectons et utilisons cet ensemble de données ?
 - ✓ Quel est l'impact probable sur la sécurité, la dignité et le bien-être du bénéficiaire si nous ne collectons pas et n'utilisons pas cet ensemble de données ?
 - ✓ Quelle est la probabilité que l'ensemble de données soit utilisé aux fins répertoriées ?
2. Prenez en considération les conséquences potentiellement néfastes de la collecte, du stockage, de l'analyse et du partage de cet ensemble de données :
 - **Au moment de la collecte**
 - **À l'avenir**
 - ✓ À quel danger (accru) ou risque (plus élevé) cette question peut-elle exposer ces groupes / personnes, à différentes étapes du processus ?
 - ✓ Quelle est la probabilité de ce danger (accru) ou de ce risque (plus élevé) ?

¹ Directives : <https://dtm.iom.int/dtm-partners-toolkit/data-sharing-guidelines> et modèles <https://dtm.iom.int/dtm-partners-toolkit/dtm-data-sharing-forms>. Pour une évaluation conjointe des avantages et des risques, reportez-vous au *Cadre PIM-OCHA pour le partage des données dans la pratique* : <http://pim.guide/wp-content/uploads/2018/05/Framework-for-Data-Sharing-in-Practice.pdf>

Vous pouvez remplir le tableau, en indiquant **SI et COMMENT** des acteurs spécifiques sont exposés à un risque (accru) à cause d'une question

Qui est exposé à un risque accru ?	En raison de la collecte de données	En raison du stockage des données	En raison de l'analyse des données	En raison du partage de données ou de rapports (actuellement)	En raison du partage de données ou de rapports (à l'avenir)
Enquêteurs					
Informateurs clés		NE PAS collecter ces données si l'utilisation prévue ne justifie pas le risque probable			
Communauté déplacée					
Communauté d'accueil					
Organisation					
Autres					

3. Questions directrices propres à chaque étape du processus de traitement des données

La collecte de l'ensemble de données peut-elle nuire ?

- ✓ Quelle est la probabilité que le fait de poser cette question expose les enquêteurs, les informateurs clés, la population déplacée, la communauté d'accueil ou d'autres personnes à un danger (accru)/risque (plus élevé) ? Quels sont ces risques / dangers ?
- ✓ Dans quelle mesure est-il probable que poser cette question expose l'organisation et sa capacité à mener ses activités à un danger (accru) / risque (plus élevé) ? Quels sont ces risques / dangers ?
- ✓ Existe-t-il des services accessibles et sûrs pour soutenir les membres de la communauté si la question déclenche un partage d'informations sur des incidents de violence et d'abus ? Les enquêteurs peuvent-ils en référer à ces services ?

Le partage de l'ensemble de données peut-il nuire ?

Prenez en considération les conséquences potentiellement néfastes du **partage** de cet ensemble de données : Ces données peuvent-elles être **analysées puis utilisées** d'une manière qui nuise / mette en danger les enquêteurs, les informateurs clés, les communautés, les individus au sein des communautés (communauté d'accueil ou communauté déplacée) ou l'organisation si...

- ✓ elles sont rendues publiques ?
- ✓ elles sont partagées avec des parties prenantes spécifiques ?
- ✓ des parties prenantes spécifiques y accèdent, même sans autorisation² ?

Prenez en considération les risques par rapport à l'utilisation de ces ensembles de données particuliers.

² Nous devons partir du principe qu'il est toujours possible qu'un accès non autorisé à de telles données se produise, comme cela a été le cas pour de nombreuses organisations humanitaires. Dans certains cas, il peut s'agir d'un piratage non autorisé du système informatique, dans d'autres cas, d'une personne à un point de contrôle qui peut passer par les questionnaires papier des enquêteurs ou vérifier les téléphones / tablettes. En outre, la plupart des fuites de données se produisent en raison d'une erreur humaine, parce que quelqu'un envoie la mauvaise pièce jointe, indique les mauvaises adresses électroniques dans son courriel, perd un questionnaire rempli sur le chemin du bureau ou ne conserve pas ses informations sous clé.

- ✓ Quelle peut être la gravité des conséquences sur les communautés et les individus que nous servons, si ces données deviennent connues de ces parties prenantes spécifiques ?
- ✓ Quelle est la probabilité que ces parties prenantes spécifiques aient accès à ces données ?
- ✓ Quelles mesures pouvons-nous raisonnablement mettre en place pour minimiser ce risque ?
- ✓ Quelle est la probabilité que ces parties prenantes spécifiques aient accès à ces données, même après la mise en œuvre de telles mesures ?

NE PAS collecter ces données si l'utilisation prévue ne justifie pas le risque probable

Comment rendre le partage plus sûr ?

Si l'utilisation prévue justifie le risque, partagez en toute sécurité

- Recenser et mettre en œuvre des mesures de protection pour ces ensembles de données aux étapes de la collecte, du stockage et du partage (à la fois pour les données et documents numériques et papier), y compris en trouvant des formulations alternatives pour les questions, en utilisant des indicateurs de remplacement, en protégeant l'accès aux fichiers numériques, en mettant en sécurité sous clé les fichiers papier, en détruisant les fichiers inutiles et en regroupant les ensembles de données à un niveau d'administration supérieur.
- Signer des accords de partage de données³ avec les partenaires spécifiques qui utiliseront les données aux fins prévues. Les accords de partage de données comprennent des procédures opérationnelles standard détaillant comment le partage, le stockage et la destruction des données auront lieu en toute sécurité.
- N'oubliez pas que les erreurs humaines sont toujours la première cause de partages de données fortuits :
 - réfléchissez bien à qui est le destinataire de votre courriel, qui fait partie de votre liste de diffusion (les connaissez-vous tous ? Font-ils partie des organisations avec lesquelles vous devriez partager ? Ont-ils quitté le pays et travaillent-ils désormais ailleurs ?). Avant de partager les données avec ces personnes, assurez-vous qu'elles ont besoin de recevoir les données et qu'elles savent comment les gérer en toute sécurité.
 - Examinez attentivement **tous les ensembles de données du tableau avant de les télécharger sur le Web ou de les partager**. Tous ces ensembles de données sont-ils sûrs et nécessaires dans la sphère publique ou pour le destinataire ? Y a-t-il un ensemble de données dont vous aviez convenu qu'il ne devait ni être rendu public, ni envoyé au destinataire figurant dans votre tableau ? Vérifiez tout particulièrement le champ « Commentaires » et les champs « Protection ». Existe-t-il des informations susceptibles de mettre en danger les enquêteurs, les personnes interrogées, la communauté ou même l'organisation ?

³ Pour les modèles, voir : <https://dtm.iom.int/dtm-partners-toolkit/dtm-data-sharing-forms>

L'analyse des données peut-elle nuire ?

- Lors de la conception de vos outils de collecte de données, tenez compte de la formulation des questions qui se traduiront par des **ensembles de données qui, par le passé, ont été mal compris, mal interprétés et même mal utilisés à dessein contre les communautés et les individus que nous servons**. Par exemple, accordez une attention particulière à l'obtention de données sur les motifs réels des déplacements / mouvements de population. Ces informations auront des conséquences sur leur statut et une formulation incorrecte peut exclure des communautés entières de leurs droits à une protection juridique.
- Prenez en considération les conséquences sur l'accès de la population à ses droits légaux également **lorsque vous concevez l'exercice et les questions spécifiques**, ainsi que lorsque **vous présentez des données sur les catégories de population**. Par exemple, le fait de fournir des chiffres séparés sur les personnes qui sont rentrées volontairement et les personnes qui ont été forcées de rentrer peut augmenter l'impact des partenaires de Protection. La distinction entre les personnes de retour de l'étranger et les personnes de retour d'un déplacement interne aidera à comprendre les raisons et les besoins potentiels des rapatriés. La distinction entre les personnes déplacées à l'intérieur de leur pays, les personnes fuyant la persécution ou la violence généralisée, les personnes se déplaçant pour des raisons économiques, les personnes fuyant la pauvreté facilitera l'accès à la protection juridique et humanitaire et une meilleure compréhension des besoins et des ressources de la population.

Demandez à vos collègues et partenaires de la Protection de vous aider à trouver la formulation la plus appropriée des questions et des choix de réponse ainsi que les catégories de population les plus précises pour

Promouvoir une utilisation sûre des données DTM

Outils disponibles

- Un cadre pour le partage de données dans la pratique : <http://pim.guide/essential/a-framework-for-data-sharing-in-practice/>
- Directives de partage de données : <https://dtm.iom.int/dtm-partners-toolkit/data-sharing-guidelines>
- Formulaires d'accès aux données : <https://dtm.iom.int/dtm-partners-toolkit/dtm-data-sharing-forms>