La protection des données est la protection des personnes

PROTECTION DES DONNÉES ET GUIDES DE CONFIDENTIALITÉ

MERCY CORPS

Le contenu ci-après est conçu pour aider le personnel de Mercy Corps à mieux comprendre et à mettre en œuvre des pratiques responsables en matière de données. Il rassemble plusieurs politiques et documents d'orientation existants de Mercy Corps, ainsi que des tutoriels simples et des liens vers d'autres ressources. Les informations peuvent être prises dans leur ensemble comme un guide complet, ou chaque section peut être utilisée comme un guide autonome sur un sujet particulier.

Bien que le guide soit principalement destiné au personnel de Mercy Corps et qu'il ait été conçu pour accompagner la trousse à outils sur les données responsables, nous le publions sous licence ouverte afin qu'il puisse bénéficier aux partenaires, aux organisations homologues et à d'autres personnes ayant besoin d'exemples de politiques, de modèles et d'instructions pour mettre en œuvre des pratiques de données responsables. Vous pouvez télécharger l'ensemble du contenu de notre guide via notre page Github à l'adresse suivante : https://github.com/mercycorps/DPP-guides.

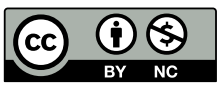
Table des matières

Citations et remerciements

Le contenu de ce guide fait partie des bonnes pratiques de gestion des données et du cycle de vie plus large des données, ou des activités globales de gestion des données individuelles dans le cadre d'un programme ou d'une intervention. Les ressources suivantes sont d'excellents points de départ pour une compréhension plus complète de la gestion responsable de vos données. Nous avons utilisé ou cité des parties de toutes ces ressources tout au long du guide et nous faisons référence aux chapitres ou sections spécifiques qui sont les plus pertinents pour un sujet particulier.

- La *trousse à outils sur la responsabilité des données* du Cash Learning Partnership est conçue spécifiquement pour les praticiens du secteur des transferts monétaires, mais elle constitue une référence en matière de conseils sur les données responsables. La trousse à outils est disponible en Anglais, Arabe, Français et Espagnol.
- La *trousse à outils de données pour le personnel de l'humanitaire* de l'Electronic Cash Transfer Learning Action Network's fournit une série de fiches-conseils sur les données permettant de comprendre les différents aspects des bonnes pratiques de gestion et de protection des données.
- Le Manuel sur la protection des données dans l'action humanitaire du *Comité international de la Croix-Rouge* est un guide détaillé sur presque tous les aspects des données humanitaires.
- Le Guide pratique sur la protection des données de la *Fédération internationale des sociétés de la Croix-Rouge et du Croissant-Rouge* est une excellente ressource d'exercices, de plans de session, de listes de contrôle et d'autres matériels pour vous aider à organiser des conversations et des activités avec votre équipe pour développer des activités de données responsables.
- Le Tutoriel en ligne du Humanitarian Data Centre pour la réalisation d'une évaluation des risques liés à la divulgation d'informations est une ressource très spécifique et technique, mais indispensable pour réduire véritablement le risque d'utilisation des données pour identifier des personnes.
- Le manuel du spécialiste en développement moderne *de The Engine Room* est un bon aperçu des données dans le contexte des activités de développement international.

License



Comprendre les données sensibles

Comprendre les différentes classifications des données peut être difficile, mais elles constituent une partie importante du travail avec les données humanitaires. Par exemple, quelle est la différence entre les données personnelles et les données sensibles ? Certains types de données peuvent nécessiter une attention particulière conformément aux lois régionales ou nationales ou aux politiques organisationnelles et peuvent présenter différents types de risques pour les participants au programme et les organisations. Les données sensibles sont une sous-catégorie de données personnelles et cette section fournit des conseils détaillés pour les traiter et les comprendre.

☆ Importance

La majorité des programmes et autres activités de Mercy Corps recueillent des informations personnelles sur les individus. Dans de nombreux cas, les programmes recueillent également des informations sur le profil culturel, l'orientation sexuelle, la santé, la biométrie et la génétique d'une personne. Ces types d'informations sont considérés comme des données sensibles et, si elles sont divulguées, consultées ou partagées de manière inappropriée, elles peuvent entraîner :

- des atteintes à une personne, telles que les sanctions, la discrimination et les menaces pour la sécurité,
- un impact négatif sur la capacité de Mercy Corps à mener ses activités et une diminution de la confiance ou de la perception du public.

Il est essentiel de prendre les mesures nécessaires pour protéger ces données.

Directive

Cette section contient deux documents :

- Le document « Utilisation de données sensibles » vous présente les données sensibles, les termes clés et les éléments à prendre en compte pour planifier leur collecte, leur stockage, leur analyse et leur partage.
  - Le personnel de Mercy Corps peut accéder au document dans la bibliothèque numérique interne de Mercy Corps.
  - Une version de l'orientation en PDF est disponible pour tous en anglais, arabe, espagnol, français et russe.
- Le « modèle d'évaluation des informations sensibles (SIA) » peut être utilisé avec une évaluation des incidences sur la vie privée pour documenter toutes les mesures de protection supplémentaires employées pour les données sensibles. Ce document présente également les différentes bases juridiques qui peuvent être utilisées pour justifier la collecte et l'utilisation de données sensibles.
  - Le personnel de Mercy Corps peut accéder au modèle SIA dans la bibliothèque numérique interne de Mercy Corps.
  - Tout le monde peut télécharger le modèle sous forme de **fichier Microsoft Word en** anglais, arabe, espagnol, français **et** russe.

Assistance supplémentaire

La planification de la collecte ou de l'utilisation de données sensibles doit faire partie d'une stratégie plus large pour le cycle de vie des données d'un programme ou d'une activité. Il existe plusieurs ressources qui peuvent vous aider.

- *Le Guide pratique sur la protection des données* de la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge (FICR) est une est une excellente ressource d'exercices, de plans de session, de listes de contrôle et d'autres documents pour vous aider à organiser des conversations et des activités avec votre équipe. Le Module 4 - Données responsable notamment est un bon point de départ.
- Le Manuel sur la protection des données dans l'action humanitaire du *Comité international de la Croix-Rouge* est un guide détaillé sur presque tous les aspects des données humanitaires. Le chapitre 3 traite spécifiquement de la base juridique du traitement des données à caractère personnel.
- La *trousse à outils sur la responsabilité des données* du Cash Learning Partnership est conçue spécifiquement pour les praticiens du secteur des transferts monétaires, mais elle constitue une référence en matière de conseils sur les données responsables. Plus précisément, *la fiche conseil #2, « Conception et planification »*, traite de la base légale pour les données sensibles. La trousse à outils est disponible en anglais, arabe, français et espagnol.

Évaluation des incidences sur la confidentialité (PIA)

Ce guide vous aidera à comprendre une évaluation des incidences sur la vie privée (PIA) et contient les directives et le modèle de PIA utilisés par Mercy Corps. Le modèle PIA contient une série de questions qui créent un cadre permettant d'identifier les risques potentiels pour la vie privée liés à la collecte et à la gestion des données qui font partie de la mise en œuvre d'un nouveau programme ou d'une nouvelle technologie. Une PIA est également importante lorsque le contexte d'un programme change de manière significative et que de nouveaux risques ou scénarios doivent être pris en compte.

Une PIA est nécessaire chaque fois qu'un nouveau programme, projet ou technologie implique la collecte ou l'utilisation de données personnelles ou sensibles.

☆ Importance

Une PIA vous permet d'analyser comment un projet particulier ou une nouvelle technologie affectera la vie privée des personnes concernées. Une EFVP permet également de documenter les stratégies d'atténuation qui protègent la vie privée des participants et renforcent la confiance du public dans notre travail. Une PIA permet d'identifier les problèmes potentiels dès le début, lorsque leur résolution sera plus simple, moins coûteuse et ne risquera pas de nuire aux participants ou au personnel du programme.

Principes

Les principes qui sous-tendent une PIA sont similaires à ceux de toute utilisation sécurisée des données personnelles. Vous trouverez ci-dessous quelques principes clés qui ont été adaptés du Cash Learning Partnership (CaLP) :

- identifier les risques pour la vie privée des personnes,
- identifier les obligations de conformité en matière de confidentialité et de protection des données pour votre organisation,
- faire preuve de responsabilité et de respect des politiques qui protègent les participants, les partenaires et le personnel du programme,
- s'assurer que l'organisation promeut le droit à la vie privée dans ses activités humanitaires et agit en tant que gestionnaire de données éthique.

Directive

Le personnel de Mercy Corps peut trouver le Guide de la PIA dans la bibliothèque numérique. Le document contient des réponses aux questions fréquemment posées concernant les PIA et des liens vers les archives internes de Mercy Corps des PIA complétées pour comparaison. Les directives de Mercy Corps en matière d'évaluation des incidences sur la vie privée sont disponibles pour tous en anglais, arabe, espagnol, français et russe.

N'oubliez pas que :

- Une PIA est un *processus* utilisé pour identifier et évaluer les risques pour la vie privée. Remplir un formulaire PIA n'est pas la fin du processus ! Réexaminez la PIA après le début de votre projet pour vous assurer qu'il n'y ait pas de nouveaux changements qui introduisent de nouveaux risques. Si c'est le cas, documentez les changements et les nouvelles stratégies d'atténuation nécessaires pour minimiser tout nouveau risque.

- La réalisation d'une PIA implique de travailler avec des personnes de Mercy Corps, et parfois avec des organisations partenaires et d'autres personnes, pour identifier et réduire les risques d'atteinte à la vie privée. Par exemple, si vous utilisez une nouvelle technologie, vous devrez peut-être chercher à savoir si l'entreprise avec laquelle vous travaillez dispose d'une politique de confidentialité et quelles garanties technologiques elle utilise pour assurer la protection des données. Vous devrez peut-être aussi vous renseigner sur les réglementations relatives à la protection de la vie privée en vigueur dans votre pays d'activité. Trois sites Web que vous pouvez utiliser pour surveiller les données et les lois sur la protection de la vie privée au niveau national sont les suivants :
  - les Lois sur la protection des données dans le monde ;
  - la Base de données de la Conférence des Nations unies sur le commerce et le développement sur la législation relative à la protection des données et de la vie privée dans le monde entier ; et
  - la Base de données One Trust Data Guidance des lois mondiales sur la protection de la vie privée.

- Il peut être utile de comparer les ÉFVP de programmes similaires. Vous pouvez effectuer cette recherche par vous-même ou demander de l'aide à l'équipe chargée de la protection des données et de la confidentialité.

Modèles

Le personnel de Mercy Corps peut trouver le formulaire long de la PIA dans la bibliothèque numérique. Le formulaire long est disponible pour tous en anglais, arabe, espagnol, français et russe.

Chaque formulaire long de la PIA comprend cinq cas d'utilisation, qui sont expliqués ci-dessous. En cliquant sur les liens ci-dessous, vous accéderez à un écran où vous pourrez télécharger les versions anglaises des différents cas d'utilisation au format **.odt** (compatible avec Microsoft Word et les applications open source comme OpenOffice et LibreOffice) en cliquant sur **Afficher brut** ou sur le bouton **Télécharger**.

- Une nouvelle Politique
- Un nouveau Processus ou procédure
- Un nouveau logiciel ou système technologique
  - Il s'agit principalement de la mise en œuvre de nouveaux systèmes mondiaux, nationaux ou spécifiques à une équipe.
  - Si vous sélectionnez ou utilisez un nouveau système dans le cadre d'un projet ou d'un programme plus vaste, utilisez plutôt l'option projet ou programme.

❱ Un nouveau prestataire ou partenaire

- Il s'agit principalement de valider les activités d'un fournisseur, d'un partenaire ou d'un tiers dans le cadre d'une activité unique ou ponctuelle.
- Si vous sélectionnez ou utilisez un nouveau fournisseur, partenaire ou tiers dans le cadre d'un projet ou d'un programme plus vaste, utilisez plutôt l'option projet ou programme.

❱ Un nouveau Projet ou programme

- Cela peut concerner n'importe quelle phase ou aspect d'un projet ou d'un programme.
- *Il s'agit de l'option PIA plus complète*, qui comprend des dispositions relatives à la sélection de nouveaux logiciels ou systèmes technologiques, et/ou d'un nouveau fournisseur ou partenaire.

Assistance supplémentaire

❱ La trousse de démarrage des données du Electronic Cash Transfer Learning Action Network fournit une fiche de conseils pour les PIA (**voir fiche de conseils n° 1**).

❱ Le bureau du commissaire à l'information du Royaume-Uni propose un code de pratique détaillé pour la réalisation d'évaluations d'impact sur la vie privée.

❱ Le Manuel sur la protection des données dans l'action humanitaire du *Comité international de la Croix-Rouge* est un guide détaillé sur presque tous les aspects des données humanitaires. Le chapitre 5 traite spécifiquement des évaluations d'impact sur la vie privée.

Meilleures pratiques en matière de partage de fichiers

Ce guide couvre les meilleures pratiques de partage de fichiers pour les membres de l'équipe de Mercy Corps qui utilisent les applications G Suite, en particulier Google My Drive. Pour simplifier ce guide, nous aborderons le partage d'un seul *fichier*, tel qu'une feuille de calcul. Cependant, les mêmes options sont disponibles lors du partage d'un *dossier My Drive*.

Note : Mercy Corps est en train de passer à Microsoft 365 pour le partage des fichiers. **Une fois que les meilleures pratiques pour cette plateforme auront été établies, un document ou une ressource similaire sera créé.**

☆ Importance

Il existe plusieurs raisons pour lesquelles il est préférable de partager un fichier en l'hébergeant dans Google Drive et en envoyant un lien plutôt qu'une pièce jointe dans un courriel.

- **Sécurité :** vous pouvez facilement modifier les personnes autorisées à accéder ou à modifier votre fichier. Vous pouvez également rendre le lien sensible au temps en n'autorisant l'accès au fichier que pendant une période donnée.
- **Contrôle de version :** lors du partage d'un fichier hébergé en ligne, de nombreuses personnes peuvent y accéder en même temps et toutes les modifications et commentaires resteront dans un seul fichier. L'envoi d'un fichier en pièce jointe donne souvent lieu à plusieurs versions du même document, avec des noms de fichiers, des modifications, des commentaires, etc. différents. Le propriétaire du document passera beaucoup de temps à essayer de compiler tout cela dans un seul fichier ! L'utilisation d'un lien garantit également que les destinataires ont toujours accès à la version la plus récente du document.
- **Taille des fichiers :** certains services informatiques imposent des restrictions sur la taille des pièces jointes autorisées. L'envoi d'un lien vous permet de partager des fichiers de toute taille.
- **Édition facile :** les fichiers partagés en tant que documents Google dans Drive, Microsoft Word dans OneDrive ou dans des formats similaires permettent au destinataire d'ouvrir et d'interagir avec le document à l'aide d'un navigateur web et il n'est pas nécessaire qu'il dispos de la version la plus récente d'un type de logiciel particulier.

Principes

Lorsque vous partagez des documents, vous devez tenir compte des points suivants :

- **réfléchissez bien à qui créera le fichier ou le dossier, qui le possédera/administrera et qui y aura accès. Si des contractants à court terme créent et administrent des fichiers, il y a un risque que les fichiers ou l'accès partent avec les contractants lors de leur départ !**
  - Ne donnez l'accès qu'à ceux qui ont besoin du fichier,

- Les contenus confidentiels, privés ou contenant des informations personnelles identifiables (PII) doivent toujours avoir un accès restreint. Si vous n'êtes pas en mesure de déterminer si ou comment le contenu doit être restreint, veuillez demander l'aide du service juridique ou de l'équipe chargée de la protection des données et de la confidentialité.

› Utilisez le niveau d'autorisation approprié.

- Prenons un exemple où une nouvelle charte de projet doit être créée. Le plus souvent, seule l'équipe responsable de la création de la charte doit avoir un accès complet. Lorsqu'il s'agit d'obtenir un retour d'information de la part d'autres personnes, accordez des autorisations supplémentaires qui permettent uniquement de visualiser ou de commenter.
- Soyez extrêmement prudent lorsque vous accordez des demandes d'accès à des membres de l'équipe qui pourraient accidentellement utiliser leurs comptes de messagerie personnels. Au lieu d'accorder l'accès à un compte e-mail personnel, accordez l'accès à leur compte Mercy Corps, et demandez au membre de l'équipe de se connecter avec ces informations d'identification.

› Les permissions changent au fil du temps.

- Si vous ne travaillez avec quelqu'un que pour une courte période ou avec des personnes extérieures à Mercy Corps, envisagez de donner des autorisations temporaires. Si vous oubliez de supprimer l'accès plus tard, une date d'expiration vous permettra de vous assurer que l'accès est suspendu au bon moment.
- Vérifiez périodiquement la liste des personnes ayant accès à vos fichiers, dossiers ou lecteurs partagés pour vous assurer que vous supprimez l'accès des membres de l'équipe qui ont changé de rôle ou qui ne font plus partie de Mercy Corps.

› Le contenu à risque nécessite des mesures supplémentaires.

- Les informations personnellement identifiables (PII), les informations démographiques identifiables (DII) ou d'autres types de données personnelles sont protégés par de multiples lois sur la protection des données. Avant de partager des données personnelles, vérifiez les exigences légales pour partager ces informations avec d'autres. Le partage inapproprié de données personnelles peut mettre en danger les participants au programme, les donateurs, les partenaires et les membres de l'équipe de Mercy Corps. Si vous avez des questions concernant les données personnelles ou les lois sur la protection des données, veuillez envoyer un courriel à l'équipe chargée de la protection des données et de la confidentialité à l'adresse dataprotection@mercycorps.org.
- Si les informations sont considérées comme confidentielles ou exclusives à des fins commerciales, ne les partagez qu'avec les parties requises et envisagez d'accorder un accès temporaire.
- Si la personne qui reçoit le fichier travaille dans un endroit non sécurisé, ou si le contenu comprend des données personnelles, envisagez de crypter le fichier ou de le protéger par un mot de passe. Voir les sections sur le cryptage et la dépersonnalisation pour des exemples de la manière de procéder.

› Ne déplacez jamais de fichiers sans l'autorisation du propriétaire.

- Déplacer des fichiers peut modifier l'identité de ceux qui y ont accès et rendre impossible la recherche du fichier par d'autres ! Vérifiez toujours avec le propriétaire du document avant de déplacer un fichier partagé vers un nouvel emplacement.

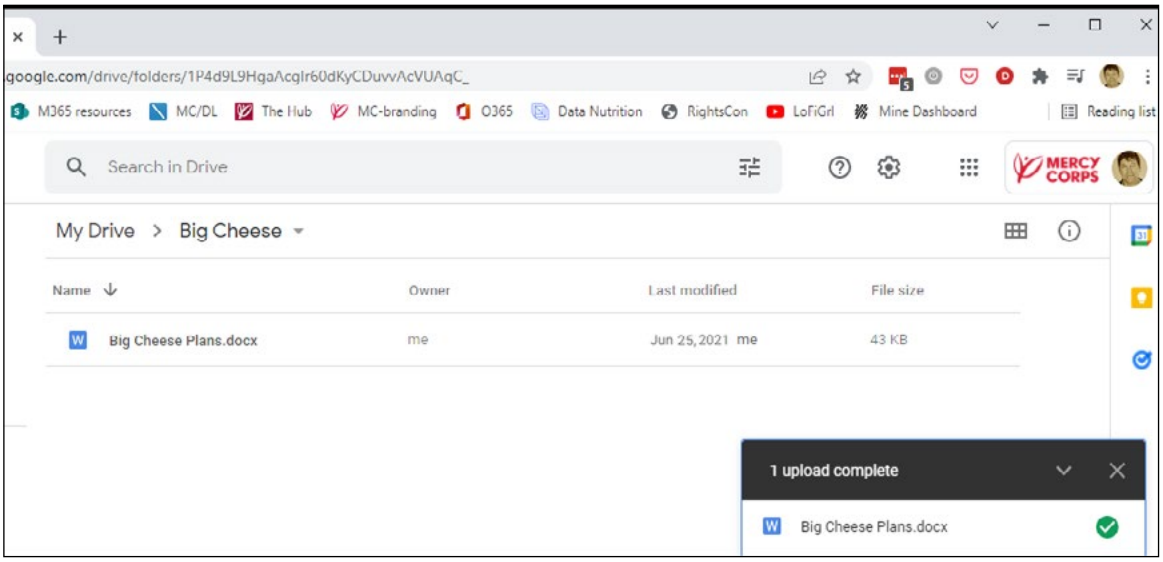
Partage de fichiers : GDrive

Voici un exemple de cas d'utilisation pour le partage d'un fichier en utilisant les meilleures pratiques de Google Drive. Imaginez que nous sommes en 2020 et que Mercy Corps travaille avec un consultant (PNW Rocks), afin de créer du matériel pour une nouvelle initiative majeure de Mercy Corps, dont le nom de code est Big Cheese. Le projet Big Cheese ne sera pas annoncé publiquement avant juillet 2021, il est donc important de limiter les personnes ayant accès au dossier. Pour commencer, nous voulons collaborer sur les prochaines étapes du projet dans un fichier appelé « Big Cheese Plans ».

Instructions

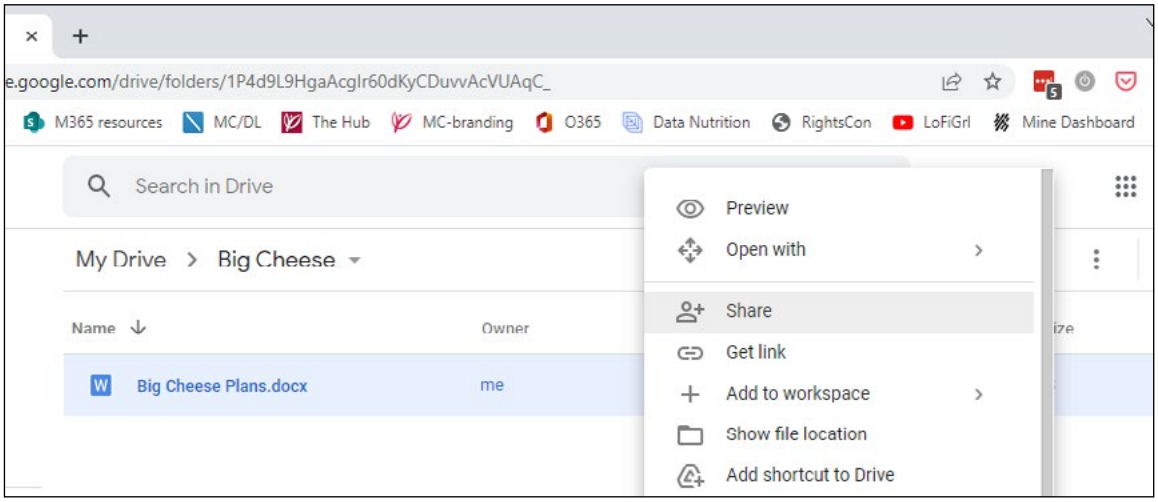
Étape 1 - Téléverser

Téléverser le fichier sur My Drive.



Étape 2 - Partager

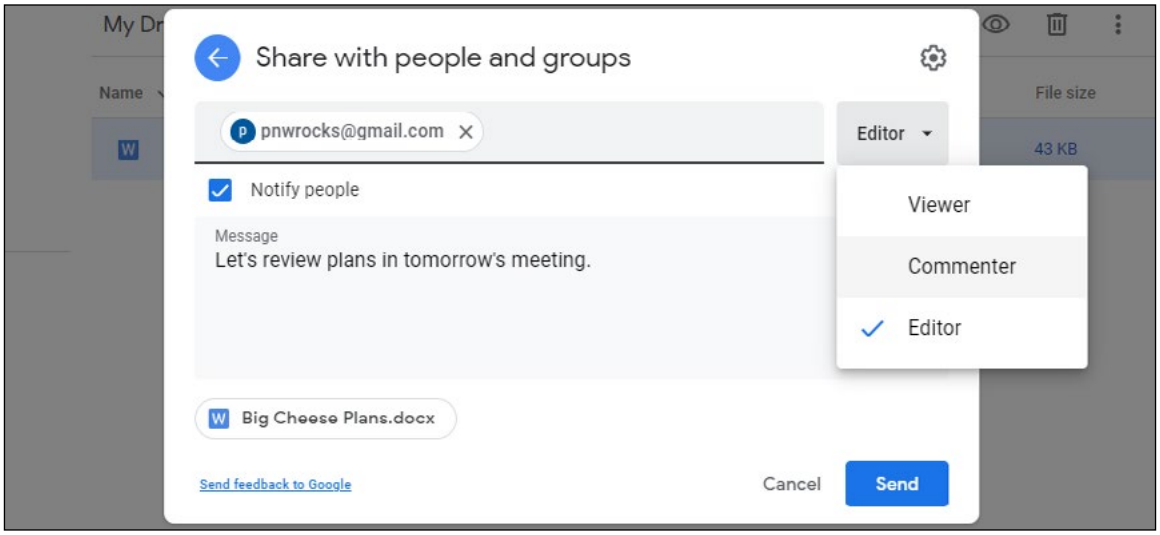
Pour partager le fichier, cliquez avec le bouton droit de la souris sur le fichier, puis cliquez sur **Partager**.



- Ne donnez l'accès qu'à ceux qui ont besoin du fichier. Lorsque vous partagez un fichier dans Mon lecteur, le paramètre par défaut est **Restreint** (aux personnes ou aux groupes), ce qui est la meilleure pratique. Les contenus confidentiels, privés ou contenant des informations personnelles identifiables (PII) devraient toujours avoir un accès restreint.
- L'option **Toute personne ayant le lien** ne doit être utilisée que pour les fichiers qui ne contiennent aucune information confidentielle et qui sont ouverts au public. Si le paramètre **Toute personne ayant un lien** est utilisé sur un fichier contenant des données confidentielles privées, personnelles ou financières, il pourrait facilement et accidentellement être partagé et faire courir un risque juridique immédiat à Mercy Corps et faciliter l'utilisation des informations à des fins criminelles par de mauvais acteurs.

Étape 3 - Sélectionner le niveau d'accès

Saisissez l'adresse électronique de la personne avec laquelle vous souhaitez partager, puis choisissez le niveau d'accès. Par défaut, Google propose un accès **Éditeur**, qui ne convient qu'aux membres de l'équipe qui ont besoin d'un accès complet au document. Lorsque vous sollicitez le retour d'information des parties prenantes, choisissez **Visionneur** ou **Commentateur**. La meilleure pratique consiste à informer la personne concernée et à ajouter un message expliquant pourquoi vous avez partagé le fichier. Pour notifier, laissez la case **Notifier les personnes** cochée. Lorsque vous avez terminé les modifications, cliquez sur **Envoyer**.

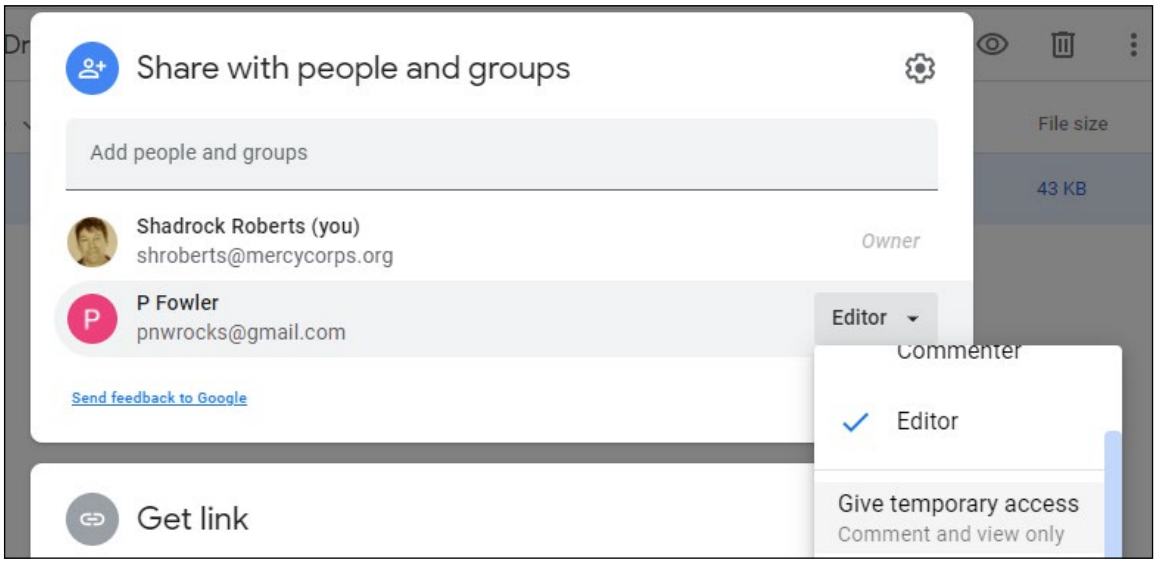


Une autre option consiste à envoyer un courriel distinct contenant un lien vers le fichier. Pour notifier séparément par e-mail, décochez la case **Notifier les personnes**. Après avoir cliqué sur **Terminé**, faites un clic droit sur le fichier et choisissez **Obtenir le lien**. Dans la nouvelle fenêtre contextuelle, cliquez sur le bouton **Copier le lien**, puis collez-le dans votre courriel.

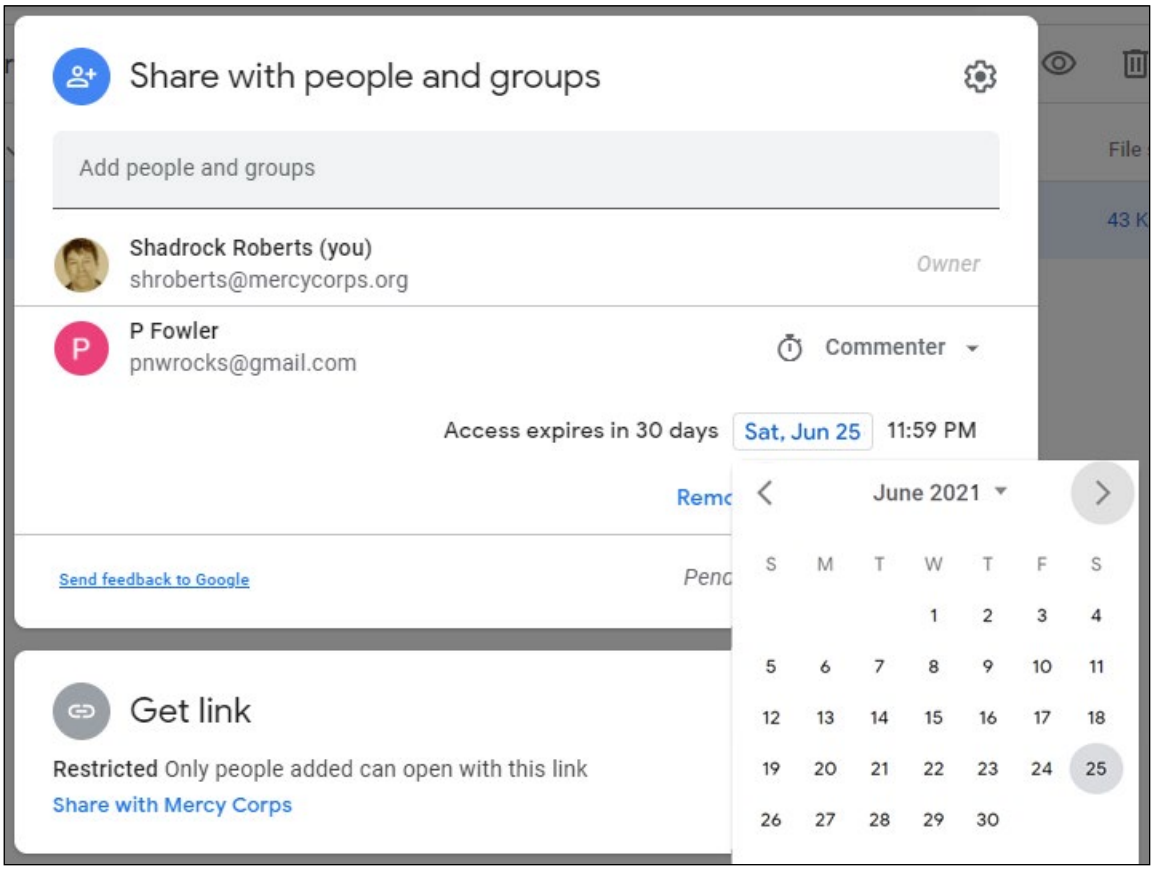
- Pour en savoir plus sur les niveaux d'accès, visitez Partager et collaborer dans My Drive.
- Si vous limitez un fichier et qu'une personne ayant un accès partage le lien avec une autre personne, cette dernière n'aura pas automatiquement accès à ce contenu dans Google Drive. Au lieu de cela, ils verront une page web avec la possibilité de demander un accès. La demande d'accès sera adressée au propriétaire du dossier. Les demandes d'accès doivent être examinées, et les personnes, qui reçoivent les demandes d'accès, ne doivent pas simplement accorder l'autorisation à toutes les demandes, sans examiner les notes et considérations ci-dessus.

Étape 4 - Accès temporaire

Une fois l'autorisation accordée, la période de partage peut être raccourcie. Pour limiter l'accès, cliquez à nouveau sur le fichier avec le bouton droit de la souris, puis cliquez sur **Partager**. Trouvez l'adresse électronique que vous venez de partager et faites un clic droit sur le niveau d'accès. Vous verrez apparaître de nouvelles options ; sélectionnez **Donner un accès temporaire**.



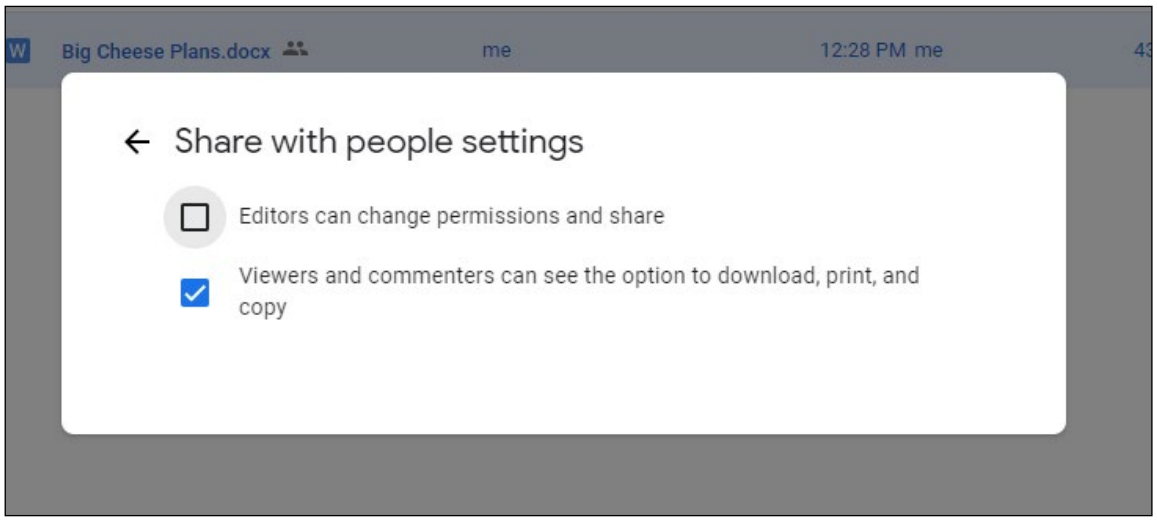
Un calendrier s'affiche. Naviguez jusqu'au mois où l'accès doit expirer, et cliquez sur la date correspondante.



Le calendrier disparaît et la date affichée change. Une fois que vous pouvez voir que l'accès expirera à la bonne date. Cliquez sur **Enregistrer**.

Étape 5 - Options supplémentaires

Si vous craignez que d'autres personnes ne prennent des mesures inappropriées avec le contenu, des options supplémentaires sont disponibles dans l'écran des paramètres. Les paramètres des fichiers sont accessibles à partir de l'icône d'engrenage en haut à droite de la fenêtre de partage. Cliquez sur l'engrenage et vous verrez des options permettant de restreindre le partage ultérieur, ou de désactiver l'option de téléchargement, d'impression ou de copie. Pour toute fonction que vous souhaitez désactiver, il suffit de décocher la case. Le fichier sera rapidement mis à jour, enregistrant le nouveau paramètre.



- Pour en savoir plus, visitez Restreindre les options de partage sur Drive.

Considérations supplémentaires

- Ne placez pas de fichiers confidentiels dans des dossiers qui sont largement partagés. Les autorisations des dossiers partagés se répercutent sur chaque fichier et sous-dossier, de sorte que votre fichier confidentiel peut être consulté par toute personne disposant d'une autorisation pour le dossier parent ! Déplacez plutôt votre fichier confidentiel vers un nouvel emplacement, en dehors de la structure du dossier partagé.
- Une fois qu'un fichier a été partagé, vous pouvez avoir la possibilité d'en **faire une copie** et/ou de le **déplacer** vers un autre emplacement. Ne déplacez jamais de fichiers sans l'autorisation du propriétaire !
- Si vous avez besoin de voir le fichier dans votre My Drive ou dans un emplacement secondaire, la meilleure pratique est d'utiliser l'option Ajouter un raccourci à Drive .
- Si une copie de fichier est effectuée, ou si le fichier est déplacé, sachez qu'il ne disposera pas des mêmes autorisations que le fichier d'origine, à moins que vous ne définissiez explicitement ces autorisations.

Ce guide ne couvre pas le partage de fichiers dans les lecteurs partagés de Google, ni les plateformes externes de partage de fichiers. Pour en savoir plus sur celles-ci, visitez les pages Meilleures pratiques pour les lecteurs partagés ou gestion des lecteurs partagés de Google. Chacune de ces pages est disponible en plusieurs langues : faites défiler la page jusqu'en bas pour sélectionner votre langue.

La meilleure façon de contrôler l'accès aux fichiers à l'aide de Drive est de créer un groupe Google et d'attribuer des autorisations aux membres du groupe. Les groupes Google ne servent pas uniquement à envoyer des courriels ; les groupes sont des outils puissants et pratiques pour gérer les autorisations de dossiers et de fichiers. En savoir plus sur les groupes Google.

Si votre projet nécessite l'utilisation d'applications en dehors de G Suite, encouragez votre équipe à télécharger Google Drive for desktop. Ce programme vous permet de visualiser tous les documents de My Drive ou des lecteurs partagés comme s'ils étaient sur votre ordinateur portable, même hors ligne, et sans avoir à télécharger l'élément ou à le convertir dans un format Google.

Assistance supplémentaire

La manière dont vous partagerez les données et les personnes avec qui vous le ferez doivent faire partie d'une stratégie plus large pour le cycle de vie des données d'un programme ou d'une activité. Il existe plusieurs ressources qui peuvent vous aider.

- *Le Guide pratique sur la protection des données* de la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge (FICR) est une est une excellente ressource d'exercices, de plans de session, de listes de contrôle et d'autres documents pour vous aider à organiser des conversations et des activités avec votre équipe. Le Module 7 - Partage des données notamment est un bon point de départ.
- Le Manuel sur la protection des données dans l'action humanitaire du *Comité international de la Croix-Rouge* est un guide détaillé sur presque tous les aspects des données humanitaires. Le chapitre 2 traite spécifiquement du partage des données.
- La trousse à outils sur la responsabilité des données du Cash Learning Partnership est conçue spécifiquement pour les praticiens du secteur des transferts monétaires, mais elle constitue une référence en matière de conseils sur les données responsables. Consultez plus précisément la Fiche conseil #6, « Partage des données » La trousse à outils est disponible en anglais, arabe, français et espagnol.

Désidentification des données

Ce guide fournit un exemple de suppression d'informations personnelles identifiables (PII) d'un ensemble de données. Il existe plusieurs façons de « désidentifier » les données, c'est-à-dire les activités ou les méthodes de traitement visant à empêcher la révélation de l'identité d'une personne concernée. Deux types courants de désidentification sont l'« anonymisation » et la « pseudonymisation ».

L'**anonymisation** est le processus par lequel les données personnelles sont rendues anonymes de sorte qu'un individu (ou « personne concernée ») n'est plus identifiable : il s'agit d'une modification permanente des données. Les méthodes courantes consistent à supprimer les informations d'identification personnelle ou à brouiller les valeurs de certains ensembles d'IPI.

> Exemple : imaginez qu'une organisation dispose de données d'enquête contenant des champs pour le nom, le numéro d'identification national, le nom du village, l'affiliation ethnique, l'âge, le niveau d'éducation et les indicateurs de santé. Dans ce cas, la suppression du nom et du numéro d'identification national serait la première étape pour rendre les données anonymes, car ces « attributs directs » sont des données personnelles qui identifient directement une personne. Les « attributs indirects » que sont le nom du village, l'appartenance ethnique, l'âge, le niveau d'éducation et les indicateurs de santé seraient conservés.

Toutefois, même si certains attributs semblent « anonymes », ils peuvent ne pas l'être Si l'enquête a été collectée dans un très petit village où seuls deux résidents s'identifient comme une affiliation ethnique particulière, et qu'ils sont tous d'âges différents, alors l'utilisation de ces deux attributs indirects pourrait permettre d'identifier ces individus ! Le processus par lequel tous les attributs sont examinés pour réduire le risque de réidentification d'une personne concernée est appelé contrôle statistique de la divulgation. La première étape de ce processus est l'évaluation du risque de divulgation et le Humanitarian Data Centre dispose d'un tutoriel en ligne pour réaliser une évaluation du risque de divulgation.

La **pseudonymisation**, quant à elle, décrit le traitement des données personnelles de telle sorte que celles-ci ne puissent plus être attribuées à une personne concernée spécifique sans l'utilisation d'informations supplémentaires, telles qu'un code clé.

> Exemple : imaginez qu'une enquête contienne votre nom, votre adresse électronique, votre âge, votre nationalité et votre lieu de travail. La pseudonymisation prend les données qui vous identifient spécifiquement (votre nom, votre adresse électronique, votre âge) et les rend inaccessibles et distinctes des données non identifiantes, comme votre nationalité. Les données pseudonymes peuvent être reconstituées à un moment donné afin que toutes les informations puissent être reliées à une source ou à une personne spécifique. C'est pourquoi la pseudonymisation exige que les informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles visant à garantir que les données personnelles ne sont pas attribuées à la personne concernée.

Faut-il choisir l'anonymisation ou la pseudonymisation ?

L'anonymisation sera généralement plus sûre et réduira le risque d'exposer les informations personnelles identifiables (PII). Cependant, cela peut parfois rendre les données trop générales, ce qui peut ne pas les rendre utiles pour des programmes tels que l'aide sous forme de bons en espèces. Dans le cas des programmes de santé qui impliquent des vaccinations ou d'autres traitements, il peut être important de contacter les personnes pour un suivi du traitement. Dans ces deux cas, la pseudonymisation serait le meilleur choix, car il est toujours possible de reconstituer les données pour identifier un individu en cas de besoin.

Il n'existe pas de réponse unique et correcte quant au choix d'une méthode plutôt qu'une autre et il est important de comprendre pourquoi les données ont été collectées, les risques potentiels associés à la détention de ces données et les besoins du programme, avant de choisir la manière de dépersonnaliser vos données.

Il est également important de comprendre que les techniques utilisées pour rendre les données anonymes et pour les pirater deviennent de plus en plus sophistiquées et que même les données dépersonnalisées ne sont pas toujours sûres à cent pour cent. En cas de doute, contactez votre équipe chargée des données ou de l'informatique pour obtenir de l'aide.

☆ Importance

Les récentes violations de données au Comité international de la Croix-Rouge, les piratages de courriels s à l'Agence américaine pour le développement international et le partage inapproprié de données par l'ONU. Haut-Commissariat aux Réfugiés montrent tous plusieurs façons dont les données humanitaires sont en danger. Les données issues d'enquêtes auprès des ménages, d'évaluations des besoins et d'autres formes de micro données constituent un volume de données de plus en plus important dans le secteur humanitaire. Ces types de données sont essentiels pour déterminer les besoins et les perspectives des participants aux programmes et des communautés dans lesquelles nous travaillons, mais ces données présentent également des risques. Il est essentiel de comprendre comment évaluer et gérer la sensibilité de ces données pour garantir qu'elles sont utilisées de manière sûre, éthique et efficace dans différents contextes d'intervention.

Les avantages de l'utilisation de données anonymes par rapport aux données personnelles sont notamment les suivants :

- la protection contre la divulgation inappropriée de données à caractère personnel,
- moins de restrictions légales s'appliquent aux données anonymes et
- permettant aux organisations de créer des données ouvertes ou accessibles au public tout en se conformant à leurs obligations en matière de protection des données.

Principes

La dépersonnalisation des données fait partie du traitement des données, et le traitement des données personnelles entrepris par les organisations humanitaires doit respecter les principes suivants.

- **L'équité et la licéité du traitement :** les méthodes doivent être conformes à la législation ou aux politiques régionales, nationales ou locales qui peuvent limiter les données pouvant être dépersonnalisées et l'utilisation de certaines technologies. Tout traitement de données à caractère personnel doit être transparent pour les personnes concernées.

- **Limitation de la finalité :** les organisations humanitaires doivent déterminer et énoncer les finalités spécifiques pour lesquelles les données sont traitées. Ces objectifs doivent être explicites et légitimes.
- **Proportionnalité :** s'assurer que chaque activité particulière liée au traitement des données personnelles est appropriée à l'objectif déclaré. Par exemple : la collecte de données se limite-t-elle au minimum requis ? Des mesures techniques et organisationnelles appropriées sont-elles en place pour réduire les risques liés au traitement des données ?
- **Changements technologiques :** les nouveaux ensembles de données et les nouveaux outils pour les analyser changent et progressent rapidement, tout comme les moyens par lesquels les données sont piratées ou volées. Il est important de comprendre les risques nouveaux et émergents pour vos données et de continuer à adapter vos méthodes et pratiques en conséquence.

Pseudonymisation

Voici un exemple d'une façon de dépersonnaliser des données dans une feuille de calcul. Il existe de nombreuses façons de procéder à la dépersonnalisation. Cet exemple utilise un "code clé" pour supprimer les informations personnelles identifiables contenues dans les identifiants directs et les conserver dans un fichier séparé. Les informations personnellement identifiables (IPI) sont des informations qui peuvent être utilisées pour identifier un individu. Les exemples courants sont le nom, l'adresse, le numéro de téléphone, la date de naissance et le numéro de sécurité sociale ou d'identification nationale.

Instructions

Vous pouvez suivre ces instructions de pseudonymisation pour parcourir un exemple de base de pseudonymisation d'un ensemble de données. L'exercice utilise un ensemble de données type qui se trouve dans le dossier de données du guide en ligne.

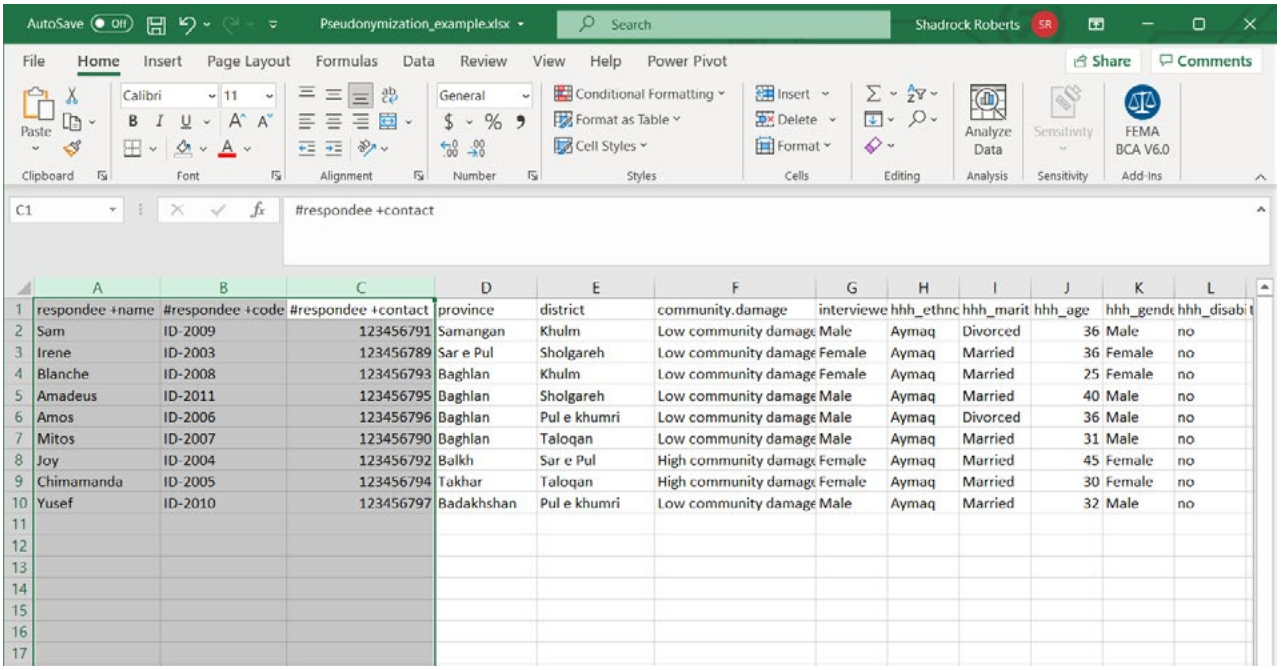
Une fois que vous avez pseudonymisé les données de l'échantillon, vous pouvez continuer avec le tutoriel pour effectuer une évaluation du risque de divulgation.

Étape 1 - Identifier les informations personnelles identifiables (PII)

Commencez par identifier les informations personnelles identifiables (PII) dans les données. Idéalement, vous disposerez de métadonnées - données ou document définissant vos données - pour vous aider à comprendre quels champs contiennent des informations personnelles identifiables (PII). Dans les données de l'échantillon, il y a trois colonnes qui contiennent des informations personnelles identifiables (PII) potentielles :

- **#respondee +name** semble contenir un nom.
- **#respondee +code** contient probablement un numéro d'identification quelconque.
- **#respondee +contact** contient éventuellement un numéro de téléphone mobile

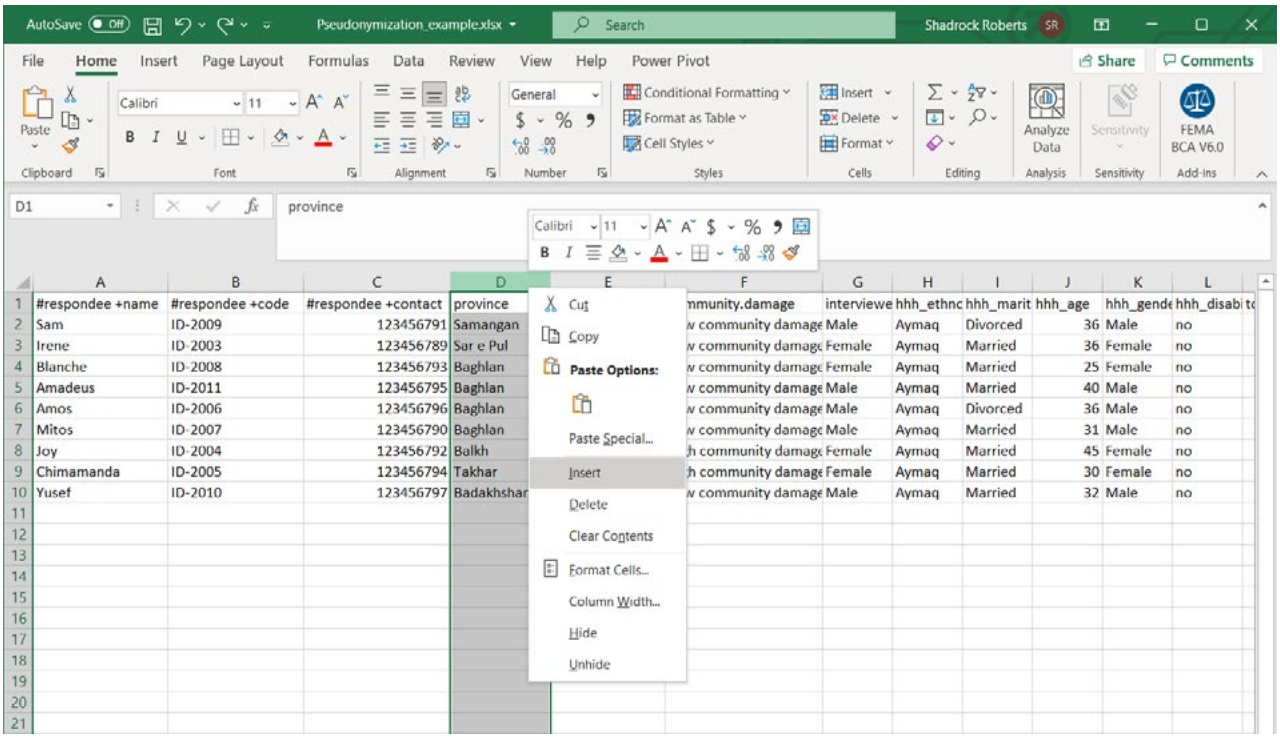
Chacun de ces identificateurs directs utilise le Humanitarian Exchange Language for tagging data.



	A	B	C	D	E	F	G	H	I	J	K	L
1	respondee +name	#respondee +code	#respondee +contact	province	district	community.damage	interviewe	hhh_ethnc	hhh_marit	hhh_age	hhh_gende	hhh_disabi
2	Sam	ID-2009	123456791	Samangan	Khulm	Low community damage	Male	Aymaq	Divorced	36	Male	no
3	Irene	ID-2003	123456789	Sar e Pul	Sholgareh	Low community damage	Female	Aymaq	Married	36	Female	no
4	Blanche	ID-2008	123456793	Baghlan	Khulm	Low community damage	Female	Aymaq	Married	25	Female	no
5	Amadeus	ID-2011	123456795	Baghlan	Sholgareh	Low community damage	Male	Aymaq	Married	40	Male	no
6	Amos	ID-2006	123456796	Baghlan	Pul e khumri	Low community damage	Male	Aymaq	Divorced	36	Male	no
7	Mitos	ID-2007	123456790	Baghlan	Taloqan	Low community damage	Male	Aymaq	Married	31	Male	no
8	Joy	ID-2004	123456792	Balkh	Sar e Pul	High community damag	Female	Aymaq	Married	45	Female	no
9	Chimamanda	ID-2005	123456794	Takhar	Taloqan	High community damag	Female	Aymaq	Married	30	Female	no
10	Yusef	ID-2010	123456797	Badakhshan	Pul e khumri	Low community damage	Male	Aymaq	Married	32	Male	no

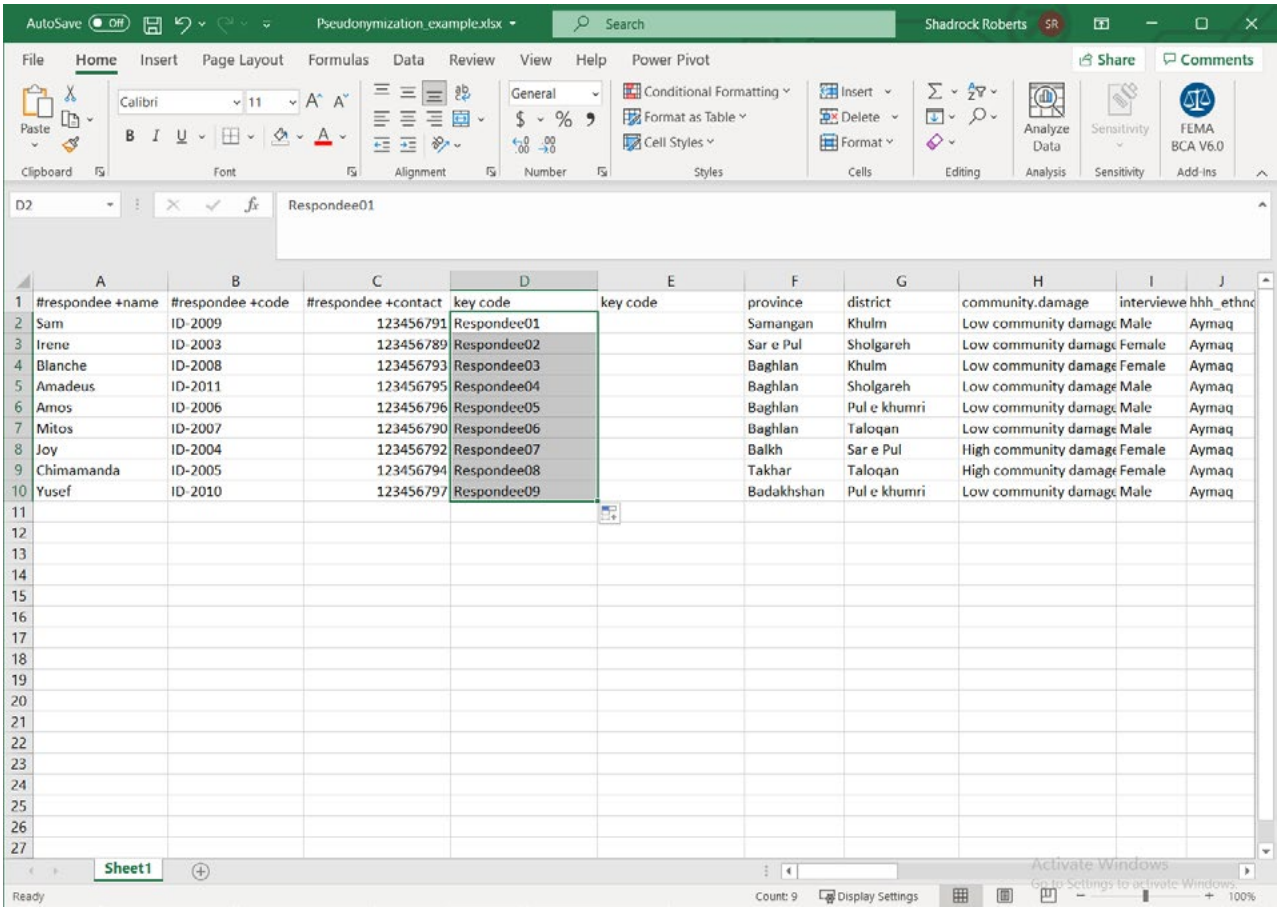
Étape 2 - Créer de nouvelles colonnes pour le code clé

Nous utiliserons un code clé, une valeur que nous générons, pour extraire les informations personnelles identifiables (PII). Puisque les identifiants directs sont tous regroupés, nous allons créer deux nouvelles colonnes entre les colonnes C, **#respondee +contact** et la colonne D **province**. Dans Excel, nous faisons cela en mettant en surbrillance une colonne à droite de l'endroit où nous voulons insérer de nouvelles colonnes, en faisant un clic droit sur la colonne et en sélectionnant **Insérer**. Répétez ce processus pour créer une autre colonne vide.



Étape 3 - Créer le code clé

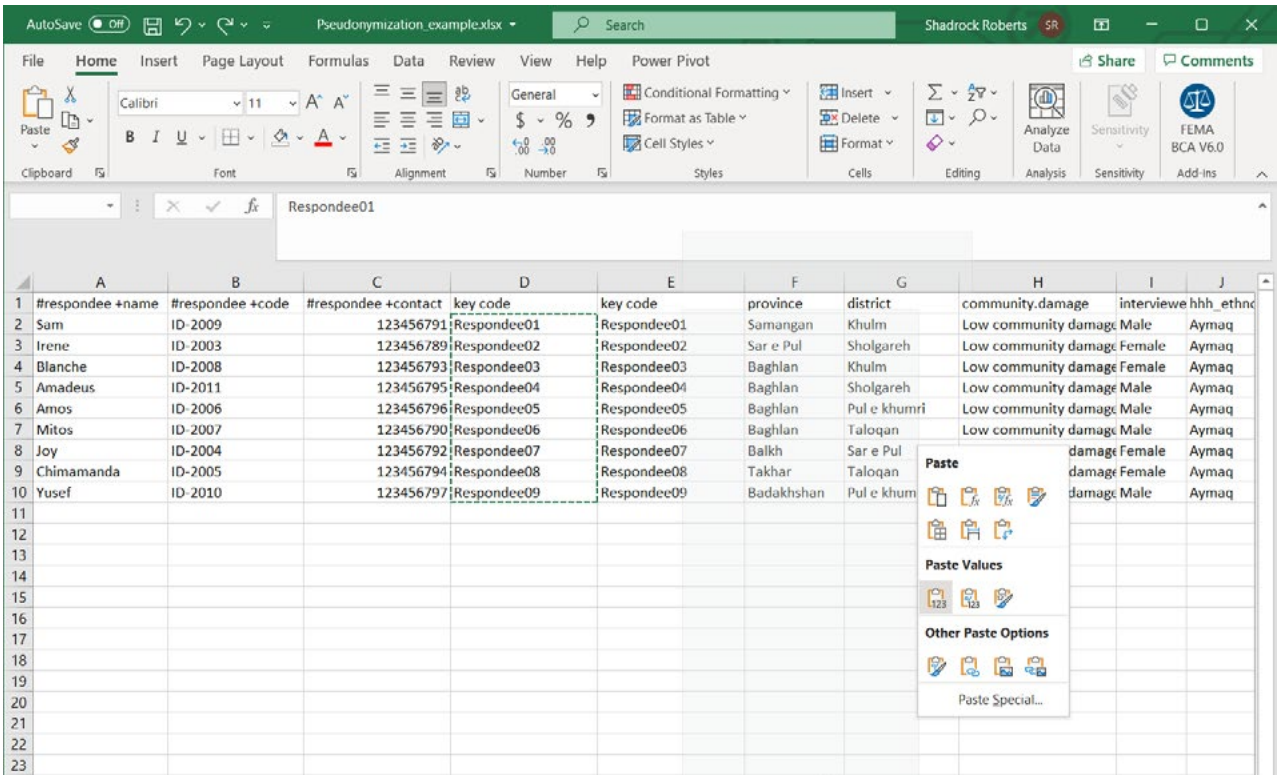
Commencez par nommer vos nouvelles colonnes. Nous utiliserons un « code clé » dans chacune d'elles : chaque colonne contiendra les mêmes valeurs. Ce serait le bon moment pour mettre à jour les métadonnées de cet ensemble de données afin d'expliquer la signification du **code clé** ! Ensuite, nous allons utiliser la fonction de remplissage automatique d'Excel pour créer un code simple. Tapez **Respondee01** dans la première cellule. Ensuite, mettez cette cellule en surbrillance, cliquez sur la poignée de déplacement dans le coin inférieur droit de la cellule et faites-la glisser jusqu'à la fin de l'ensemble de données. Le numéro final de chaque enregistrement sera automatiquement complété, de sorte que chaque personne interrogée aura désormais un nouveau code.



	A	B	C	D	E	F	G	H	I	J
1	#respondee +name	#respondee +code	#respondee +contact	key code	key code	province	district	community.damage	interviewe	hhh_ethnc
2	Sam	ID-2009	123456791	Respondee01		Samangan	Khulm	Low community damage	Male	Aymaq
3	Irene	ID-2003	123456789	Respondee02		Sar e Pul	Sholgareh	Low community damage	Female	Aymaq
4	Blanche	ID-2008	123456793	Respondee03		Baghlan	Khulm	Low community damage	Female	Aymaq
5	Amadeus	ID-2011	123456795	Respondee04		Baghlan	Sholgareh	Low community damage	Male	Aymaq
6	Amos	ID-2006	123456796	Respondee05		Baghlan	Pul e khumri	Low community damage	Male	Aymaq
7	Mitos	ID-2007	123456790	Respondee06		Baghlan	Taloqan	Low community damage	Male	Aymaq
8	Joy	ID-2004	123456792	Respondee07		Balkh	Sar e Pul	High community damage	Female	Aymaq
9	Chimamanda	ID-2005	123456794	Respondee08		Takhar	Taloqan	High community damage	Female	Aymaq
10	Yusef	ID-2010	123456797	Respondee09		Badakhshan	Pul e khumri	Low community damage	Male	Aymaq

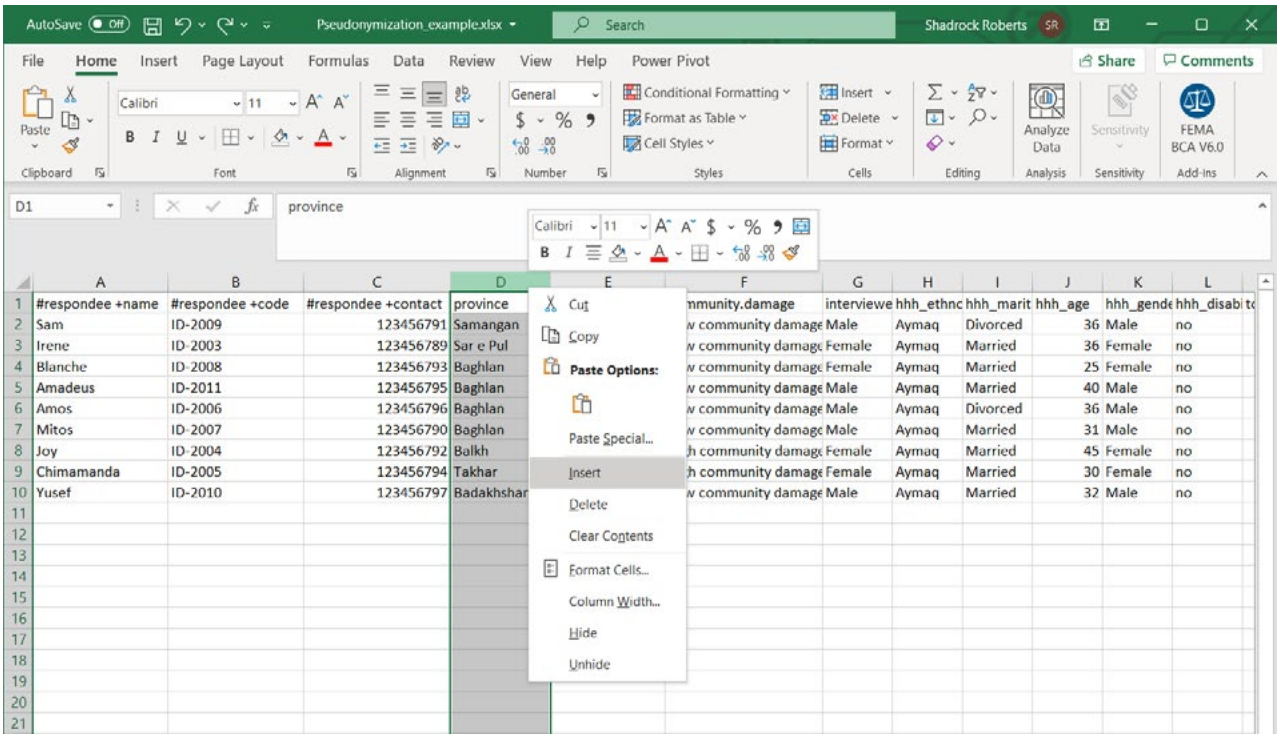
Étape 4 - Dupliquer le code clé et supprimer les formules

Nous allons maintenant copier le code clé et le coller dans la colonne adjacente. Pour ce faire, vous pouvez utiliser des commandes clavier de base telles que ctrl + C ou mettre en surbrillance les cellules que vous souhaitez copier, faire un clic droit dessus et sélectionner Copier. Dans la colonne adjacente, mettez en surbrillance les cellules dans lesquelles vous souhaitez coller le nouveau code clé, faites un clic droit et choisissez Coller. J'ai choisi de ne coller spécifiquement que les valeurs. Si vous avez utilisé une formule pour créer un nouveau code, il sera important de ne conserver *que les valeurs* pour les utiliser comme code clé !

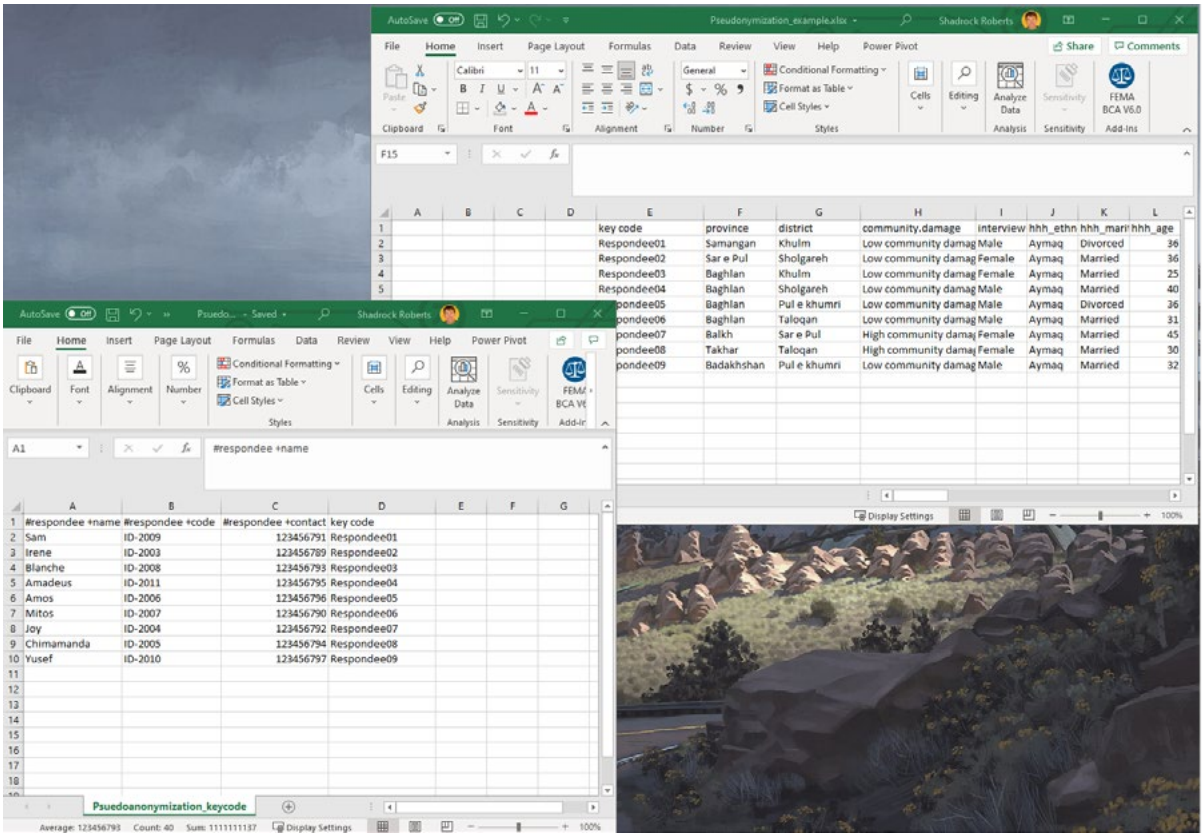


Étape 5 - Séparer les identifiants directs et indirects

Mettez en évidence les colonnes qui contiennent les identificateurs directs avec les informations personnelles identifiables (PII) ainsi qu'une des colonnes de code clé. Dans cet exemple, nous mettons en surbrillance les colonnes A-D. Cliquez dessus avec le bouton droit de la souris et sélectionnez **Couper**.



Ensuite, ouvrez une nouvelle feuille de calcul et collez ces valeurs en utilisant le raccourci clavier **ctrl + V**, ou une autre méthode. Enregistrez la nouvelle feuille de calcul. Vous avez maintenant deux feuilles de calcul : l'une d'elles contient les identifiants indirects tandis que la nouvelle feuille contient les identifiants directs avec les informations personnelles identifiables (PII). Les deux ensembles de données contiennent un code clé pour chaque enregistrement des données afin que toutes les données puissent être recombinées si nécessaire.



Next Steps

Les deux dossiers contiennent un code clé qui permettra de les reconstituer. Une façon d'y parvenir dans Excel est d'utiliser la fonction VLOOKUP pour remplir automatiquement les cellules en fonction de la valeur d'autres cellules. Dans ce cas, vous pouvez remplir les cellules vides du fichier d'origine avec les informations personnelles identifiables (PII) manquantes en vous basant sur la valeur du **code clé**.

Comme le nouveau fichier contient les identifiants directs contenant les informations personnelles identifiables (PII), il doit être stocké de manière sécurisée. Un excellent moyen d'y parvenir est de crypter le fichier et d'utiliser le stockage en nuage pour limiter les personnes ayant accès au fichier (**voir les guides des meilleures pratiques en matière de cryptage et de partage de fichiers**).

N'oubliez pas : si la feuille de calcul originale a été dépersonnalisée en supprimant les identifiants directs qui contiennent des informations personnelles identifiables (PII) évidentes, les autres identifiants indirects peuvent être combinés avec d'autres données ou analysés de manière à permettre l'identification d'une personne.

Pour cette raison, les deux fichiers doivent toujours être stockés de manière sécurisée. Si vous souhaitiez partager plus largement le fichier original, sans DPI, il serait essentiel de procéder à une évaluation du risque de divulgation afin de garantir le risque minimum que les données puissent être réidentifiées. Le Humanitarian Data Centre dispose d'un tutoriel en ligne permettant de réaliser une évaluation du risque de divulgation à l'aide d'un du logiciel statistique à code source ouvert « R ». De plus, la page web Poverty Action Lab's De-identification for data publication fournit une excellente discussion sur la dé-identification des données et inclut un exemple de code pour le logiciel statistique Sata. Pour le personnel de Mercy Corps, l'ébauche de directive de T4D est disponible en interne et fournit des formules Excel supplémentaires.

Enfin, toutes ces mesures contribuent à atténuer le risque d'exposition des DPI. Elles doivent donc être mentionnées dans l'évaluation des incidences sur la vie privée (**voir le guide de l'évaluation des incidences sur la vie privée**) afin que les autres comprennent comment ces données sont protégées.

Assistance supplémentaire

La désidentifcation des données fait partie des bonnes pratiques de gestion des données et du cycle de vie des données au sens large, c'est-à-dire l'ensemble des activités de collecte de données individuelles dans le cadre d'un programme ou d'une intervention. Les ressources suivantes sont d'excellents points de départ pour une compréhension plus complète de la gestion responsable de vos données.

- La trousse à outils sur la responsabilité des données du Cash Learning Partnership est conçue spécifiquement pour les praticiens du secteur des transferts monétaires, mais elle constitue une référence en matière de conseils sur les données responsables. La trousse à outils est disponible en anglais, arabe, Français et espagnol.
- La *trousse à outils de données pour le personnel de l'humanitaire de l'Electronic Cash Transfer Learning Action Network's* fournit une série de fiches-conseils sur les données permettant de comprendre les différents aspects des bonnes pratiques de gestion et de protection des données.
- Le Manuel sur la protection des données dans l'action humanitaire du *Comité international de la Croix-Rouge* est un guide détaillé sur presque tous les aspects des données humanitaires. Le chapitre 2 traite spécifiquement de la désidentification des données.
- Le manuel *du spécialiste en développement moderne de The Engine Room* est un bon aperçu des données dans le contexte des activités de développement international. La section sur le *partage des données* traite spécifiquement de la désidentification.

Cryptage d'un fichier

Cette section aborde un exemple de base de cryptage d'un fichier à l'aide d'une fonction Microsoft disponible sur les ordinateurs de Mercy Corps. Il existe une série de facteurs à prendre en compte lors du cryptage d'un fichier, mais nous nous concentrons ici sur l'utilisation d'un mot de passe et le cryptage d'un seul fichier. Voir les liens ci-dessous pour des ressources qui explorent le cryptage de manière plus approfondie. Pour ce guide, il est toutefois utile de comprendre la différence subtile entre « protection par mot de passe » et « cryptage ».

Considérez la protection par mot de passe comme une boîte munie d'un verrou. Lorsque vous « protégez » votre document par un mot de passe, vous le placez dans une boîte électronique que vous verrouillez à l'aide d'un mot de passe : seules les personnes disposant du mot de passe peuvent ouvrir la boîte. Cependant, si le mot de passe que vous choisissez n'est pas très fort, ou s'il est partagé avec la mauvaise personne, quelqu'un peut facilement entrer dans la boîte et voir votre document ! En revanche, le cryptage utilise des algorithmes complexes pour coder des informations, ce qui nécessite de disposer d'une clé pour décrypter ces informations. Imaginez que vous prenez votre document et le passez dans un destructeur de papier qui attribue une clé spéciale pour reconstituer le document.

Lorsque vous combinez protection par mot de passe et cryptage, vous doublez effectivement votre protection. Si quelqu'un réussit à forcer le mot de passe du boîtier électronique, il ne pourra voir que les morceaux de papier déchiqueté sans avoir également la clé appropriée. Tous les ordinateurs portables de Mercy Corps sont cryptés à l'aide de Microsoft BitLocker. Cela permet d'éviter que le disque dur d'un ordinateur portable Mercy Corps soit retiré et accessible sur un autre ordinateur.

☆ Importance

Le cryptage est essentiel car il permet de garantir la confidentialité et la sécurité des informations. Sans cryptage, les données peuvent être interceptées et lues par toute personne qui y a accès. Lorsque vous envisagez de crypter ou non des données, posez-vous la question suivante : « Quel est le risque pour les participants aux programmes de Mercy Corps, son personnel et ses partenaires si ces données étaient perdues ou volées ? » Une bonne règle de base est de chiffrer tout ce qui contient des informations personnelles identifiables ou sensibles.

Principes

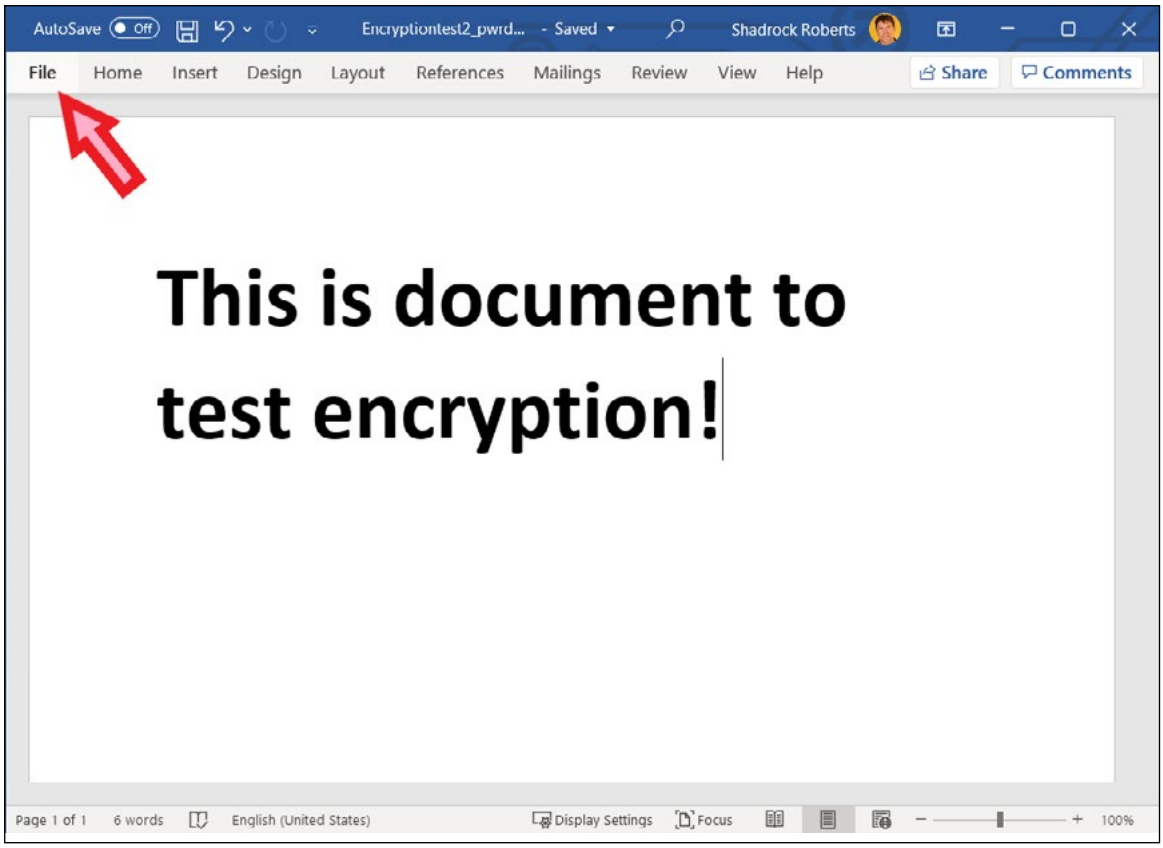
- Utilisez les systèmes approuvés de Mercy Corps pour le transfert et le stockage de données cryptées (par exemple, Microsoft SharePoint ou Google Drive). En cas de doute, demandez conseil à votre équipe informatique locale.
- Cryptez les données sensibles à tous les stades de leur collecte, utilisation, transmission et stockage.
- Utilisez des mots de passe forts et ne réutilisez pas les mots de passe. Les listes de mots de passe circulent en ligne et permettent à une personne possédant l'un de vos mots de passe d'accéder plus facilement à plusieurs de vos comptes ou fichiers ! Vous pouvez utiliser un gestionnaire de mots de passe, tel que

Lastpass. Cependant, les gestionnaires de mots de passe peuvent être vulnérables aux cyberattaques par de fausses applications. Il est donc essentiel que les gestionnaires de mots de passe soient utilisés dans le cadre d'une approche plus large de la sécurisation des données.

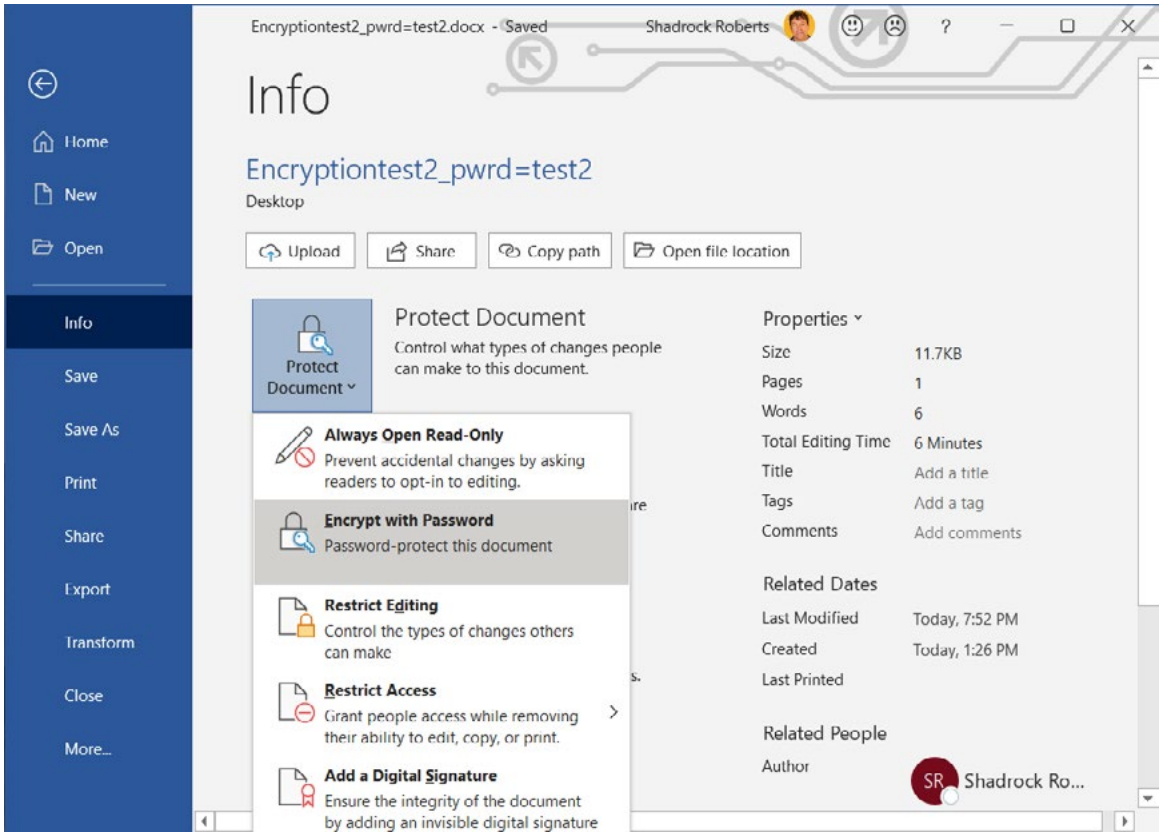
- Dans un environnement d'équipe, le cryptage est aussi bon que le maillon le plus faible. Si une seule personne n'utilise pas le cryptage, les données de votre programme sont en danger. Il est extrêmement important de communiquer ce point à votre équipe : le cryptage n'est pas seulement une question de technologie, mais aussi de changement de comportement.
- Comprenez les lois qui régissent le cryptage dans votre pays. Les lois locales d'un certain nombre de pays (comme le Soudan, le Yémen et le Pakistan) imposent des limites aux logiciels de cryptage. En cas de doute, demandez conseil à votre équipe informatique locale : en général, elle travaillera avec vous pour s'assurer que le disque dur de vos ordinateurs soit correctement crypté à l'aide d'Intune.

Instructions

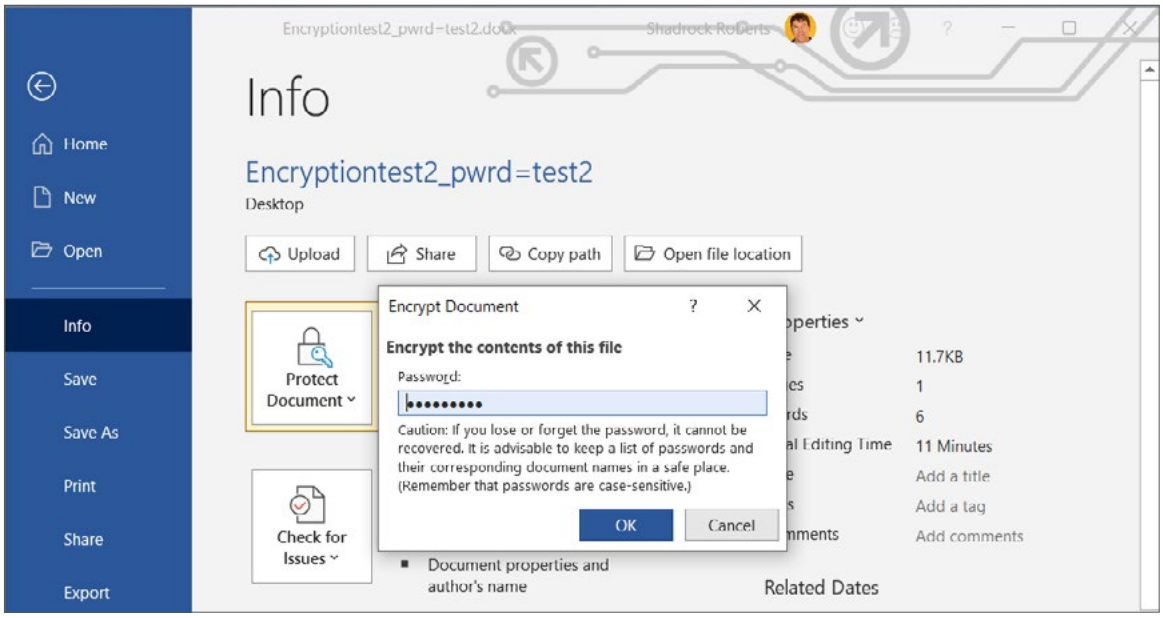
1 Ouvrez le fichier Word, Excel ou PowerPoint que vous souhaitez crypter et sélectionnez le menu **Fichier**.



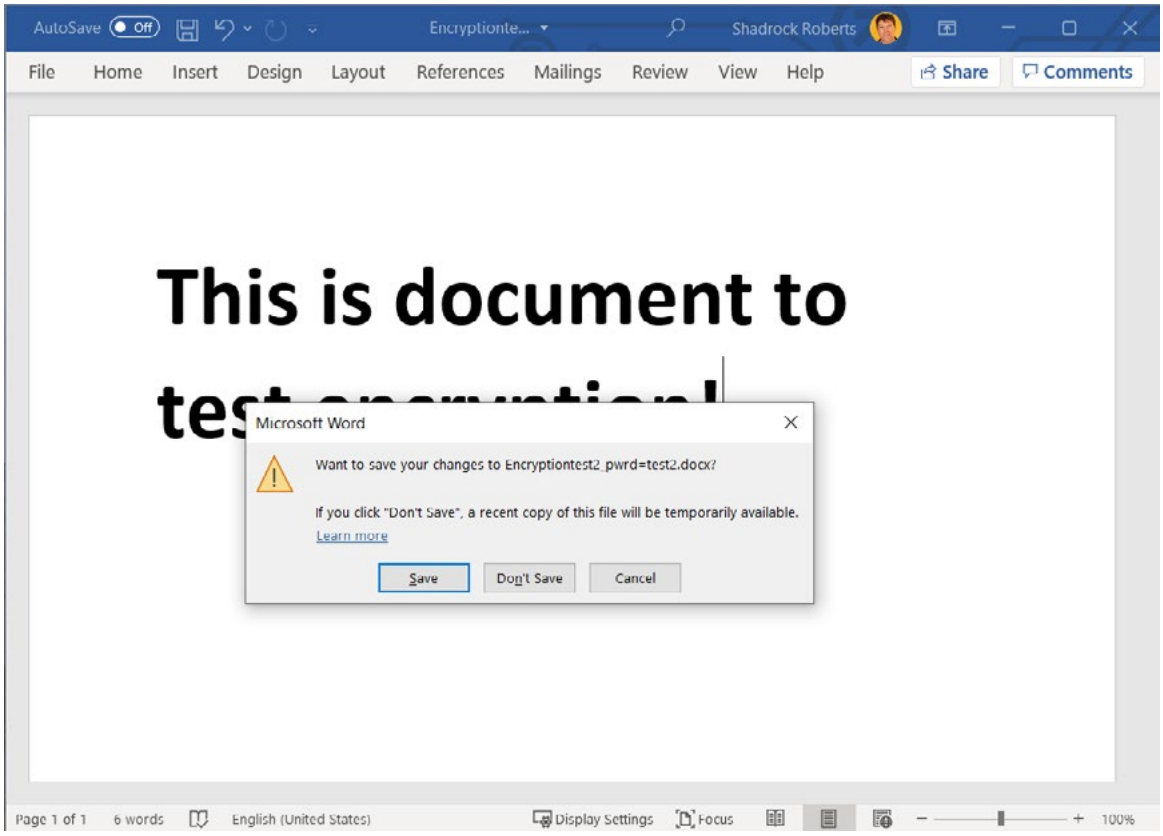
2 Naviguez jusqu'à **Info** > **Protéger le document** > **Crypter avec un mot de passe**.



3 Tapez un mot de passe, cliquez sur **OK** puis tapez-le à nouveau pour le confirmer.



4 Ouvrez le fichier pour vous assurer que le mot de passe prenne effet.



Vous pouvez maintenant partager le fichier et le mot de passe avec les personnes qui ont besoin d'y accéder. La meilleure pratique consiste à placer le fichier sur un service en nuage approuvé par Mercy Corps, tel que G Suite ou SharePoint. N'oubliez pas d'envoyer le lien du fichier et celui du mot de passe séparément. Par exemple, vous pouvez partager le fichier à l'aide de Google Drive (**voir la section Partage de fichiers**) et générer un avis indiquant que le fichier a été partagé via Google, puis communiquer le mot de passe par courrier électronique à un collègue.

Assistance supplémentaire

- La trousse de démarrage des données du Electronic Cash Transfer Learning Action Network fournit une fiche de conseils pour le cryptage (voir fiche de conseils n° 5).
- L'Electronic Frontier Foundation fournit un aperçu plus détaillé des différentes formes de cryptage.
- Le Manuel du spécialiste en développement moderne de The Engine Room comprend une section sur la gestion des données qui fournit des réflexions supplémentaires de haut niveau sur le cryptage.

CONTACT

HEATHER LOVE
Directrice, Protection des données mondiales et confidentialité | IT
hlove@mercycorps.org

SHADROCK ROBERTS
Spécialiste de la protection des données | IT
shroberts@mercycorps.org

À propos de Mercy Corps

Mercy Corps est une organisation mondiale de premier plan animée par la conviction qu'un monde meilleur est possible. Nous nous associons dans plus de 40 pays du monde pour mettre en œuvre des solutions audacieuses, en aidant les gens à triompher de l'adversité lors de catastrophes et de situations difficiles, et à bâtir des communautés plus fortes de l'intérieur. Maintenant et pour l'avenir.

MERCY CORPS

Siège mondial
45 SW Ankeny Street
Portland, Oregon 97204
888.842.0842
mercycorps.org

Siège européen
96/3 Commercial Quay
Édimbourg,
EH6 6LX Écosse, RU
+44.131.662.5160
mercycorps.org.uk