



Santé et Services sociaux Politique d'anonymisation

Énoncé de politique

Il est nécessaire d'adopter une approche cohérente à l'échelle du système de santé et des services sociaux concernant l'application des méthodes d'anonymisation, afin de respecter les exigences et de garantir la protection des renseignements personnels sur la santé.

Portée

La présente politique s'applique à tout le personnel du ministère de la Santé et des Services sociaux (le « Ministère ») et des administrations des services de santé et des services sociaux (les « administrations ») qui doivent anonymiser des renseignements.

Définitions

Les définitions suivantes s'appliquent à la présente politique :

« Administrations des services de santé et des services sociaux » s'entend de l'Administration des services de santé et des services sociaux des TNO et des conseils d'administration en vertu de la *Loi sur l'assurance-hospitalisation et l'administration des services de santé et des services sociaux*.

« Anonymisation » s'entend du processus consistant à manipuler des renseignements personnels sur la santé de manière à ce que la personne concernée ne puisse raisonnablement être identifiée.

« Désanonymisation » désigne le processus de manipulation de renseignements personnels sur la santé préalablement anonymisés, qui permet, de façon raisonnable, d'identifier la ou les personnes concernées.

« Gestionnaire de l'information » signifie une personne ou une organisation qui fournit un ou plusieurs des services suivants pour le Ministère et les ASSSS :

- a) Traitement, stockage, récupération ou destruction des renseignements personnels sur la santé.
- b) Transformation des renseignements personnels sur la santé, y compris la transformation des renseignements personnels sur la santé d'une personne pour créer ou pour produire des renseignements non personnellement identifiables.
- c) Services de gestion de l'information, de système d'information ou de technologie.

« Manipulation » désigne l'élagage, le codage ou la transformation par un autre moyen de renseignements personnels sur la santé.

« Membres du personnel » s'entend, pour l'application de la présente politique, de toute personne à l'emploi du Ministère ou des administrations, y compris les gestionnaires de l'information.

« Renseignements personnels sur la santé » s'entend des renseignements sous quelque forme que ce soit qui identifient une personne ou à l'égard desquels il est raisonnable de prévoir, dans les circonstances, qu'ils pourraient servir, seuls ou avec d'autres, à l'identifier :

- a) les renseignements concernant sa santé et les soins de santé qu'elle a déjà reçus;
- b) les renseignements concernant les services de santé qui lui sont fournis;
- c) les renseignements sur son admissibilité ou son inscription à un service de santé, ou à un produit ou à un avantage connexe;
- d) les renseignements sur le paiement relatif à un service de santé qui lui est fourni;
- e) les renseignements recueillis, même fortuitement, lorsqu'un service de santé lui est fourni, par exemple son nom et ses coordonnées;
- f) un numéro de santé personnel, un autre numéro identificateur, un symbole ou une autre caractéristique qui lui est propre concernant des services de santé ou des renseignements sur la santé;
- g) les renseignements prescrits concernant le fournisseur de services de santé qui lui fournit un service de santé;
- h) les renseignements sur tout don de parties de corps ou de substance corporelle qu'elle a fait;
- i) les renseignements considérés comme étant des renseignements personnels sur la santé dans le *Règlement sur les renseignements sur la santé*.

« Renseignements non identificatoires » s'entend de renseignements personnels sur la santé ne pouvant pas permettre de façon raisonnable d'identifier une personne ni d'arriver à une désanonymisation.

Dispositions

- 1) Le Ministère et les ASSSS doivent faire ce qui suit :
 - a) Prendre des précautions pour protéger les renseignements personnels sur la santé lorsqu'ils procèdent à une anonymisation.
 - b) Veiller à ce que les techniques d'anonymisation utilisées par des membres du personnel respectent les normes et les pratiques exemplaires définies dans les Lignes directrices pour l'anonymisation des renseignements personnels sur la santé (voir annexe 1), dans leur version la plus récente.
- 2) Les techniques d'anonymisation ne peuvent être utilisées que par des membres du personnel autorisés et désignés par le Ministère ou les administrations.
- 3) Le processus d'anonymisation des renseignements personnels sur la santé du Ministère (voir annexe 1) doit être suivi à la lettre.
- 4) Les membres du personnel autorisés doivent répondre aux questions suivantes pour choisir des techniques d'anonymisation adéquates :
 - a) Qui aura accès aux renseignements anonymisés?
 - b) À quelles fins consultera-t-on les renseignements anonymisés?
 - c) Quel est le risque de désanonymisation, notamment s'il existe d'autres renseignements pouvant concrétiser ce risque?

Sources

Loi sur l'accès à l'information et la protection de la vie privée

Loi sur les renseignements sur la santé

Directive ministérielle 2016-02 : Normes, politiques et procédures sur la confidentialité

<signature d'origine par>

Sous-ministre

3 mai 2017

Date

Lignes directrices pour l'anonymisation des renseignements personnels sur la santé

En tant que membres du personnel du système de santé et des services sociaux, nous sommes tenus de protéger les renseignements personnels des usagers lorsque nous utilisons des données sur la santé, et plus précisément lorsque nous appliquons des techniques d'anonymisation.

Le Ministère a élaboré ces lignes directrices¹ afin d'aider le personnel du Ministère et des ASSSS à :

- utiliser les techniques adéquates d'anonymisation;
- évaluer les risques de désanonymisation.

Définitions

« Anonymisation » s'entend du processus consistant à modifier les renseignements personnels sur la santé afin qu'on ne puisse, de façon raisonnable, deviner l'identité de la personne concernée, transformant ainsi ces renseignements en renseignements sur la santé anonymisés, dont l'utilisation (seule ou avec d'autres variables) ne peut mener à une désanonymisation.

« Désanonymisation » s'entend du processus consistant à modifier les renseignements personnels sur la santé préalablement anonymisés afin qu'on puisse retrouver, de façon raisonnable, l'identité d'une ou de plusieurs personnes.

« Données agrégées » s'entend des données recueillies dans des dossiers pour obtenir une moyenne ou un classement par catégories et présentées sous forme de totaux de manière à ne comporter aucune variable permettant d'identifier directement une personne.

« Données tirées d'un dossier » s'entend des données portant sur un individu.

Utilisation des techniques d'anonymisation

Avant d'utiliser une technique d'anonymisation, prenez en compte les principes d'anonymisation suivants :

- Les divulgations ne doivent comporter qu'un minimum de données.
- Diverses techniques d'anonymisation peuvent être appliquées (voir le tableau intitulé Techniques d'anonymisation recommandées).
- Aucune technique ne peut prendre en compte à elle seule les différentes exigences d'anonymisation des renseignements personnels sur la santé.

¹ Ces lignes directrices ont été élaborées, avec les autorisations requises, à partir des directives sur la dépersonnalisation des renseignements personnels produites pour le Commissariat à la protection de la vie privée du Canada (avril 2007), des outils pour l'anonymisation des renseignements personnels sur la santé créés pour le Groupe pancanadien sur la protection des renseignements personnels sur la santé (septembre 2009), et des *Lignes directrices sur les pratiques exemplaires pour la gestion de la divulgation de renseignements de santé anonymisés* produites pour l'Institut canadien d'information sur la santé (octobre 2010).

- Chaque projet ou dossier d'anonymisation nécessite de suivre un processus unique comportant ses propres types et combinaisons de techniques.
- Il faut savoir utiliser les outils d'anonymisation et comprendre les exigences réglementaires liées à l'anonymisation.

Pour choisir une technique d'anonymisation adéquate :

- Relire la demande d'anonymisation et déterminer quel type de données peut être divulgué (données tirées d'un dossier ou données agrégées). Il est plus facile de désanonymiser les données tirées d'un dossier que celles qui sont agrégées.
- Déterminer quelle est ou quelles sont les techniques les plus appropriées. On utilise plus souvent les techniques de réduction des données que les techniques de modification des données. Ces dernières sont plus radicales et peuvent compromettre grandement l'informativité des données.
- Commencer par utiliser la technique de réduction des détails avant de passer à la technique de suppression. Ces méthodes sont :
 - les plus utilisées dans le milieu;
 - les moins coûteuses à appliquer;
 - les plus faciles à comprendre;
 - celles qui permettent d'évaluer le plus facilement le risque de désanonymisation.
- Pour la technique de pseudonymisation, voir à ce que les pseudonymes générés soient rattachés à un ensemble de données bien défini. Cela protège le contrôle des données et la possibilité future de les relier, si besoin est.

Évaluation du risque de désanonymisation

L'évaluation des risques a pour but de déterminer le degré d'anonymisation à appliquer afin d'amener le risque de désanonymisation à un niveau acceptable. (Voir le tableau des dépendances.)

L'évaluation des risques de désanonymisation doit comporter les éléments suivants :

- Cartographie des risques de désanonymisation afin d'utiliser des techniques d'anonymisation adéquates. Veuillez consulter les *Best Practice Guidelines for Managing the Disclosure of the De-Identified Health Information* (document de l'ICIS) et les *Directives sur la dépersonnalisation des renseignements personnels sur la santé pour l'ensemble du Canada*, au besoin.
- Évaluer les intentions et le degré de désanonymisation des données possible, penser aux mesures d'atténuation, évaluer la probabilité d'une tentative de désanonymisation, déterminer le degré d'anonymisation nécessaire.
- Envisager de fixer des lignes directrices souples pour les degrés de risque de désanonymisation acceptables, qui tiennent compte de différents scénarios de risques de désanonymisation.

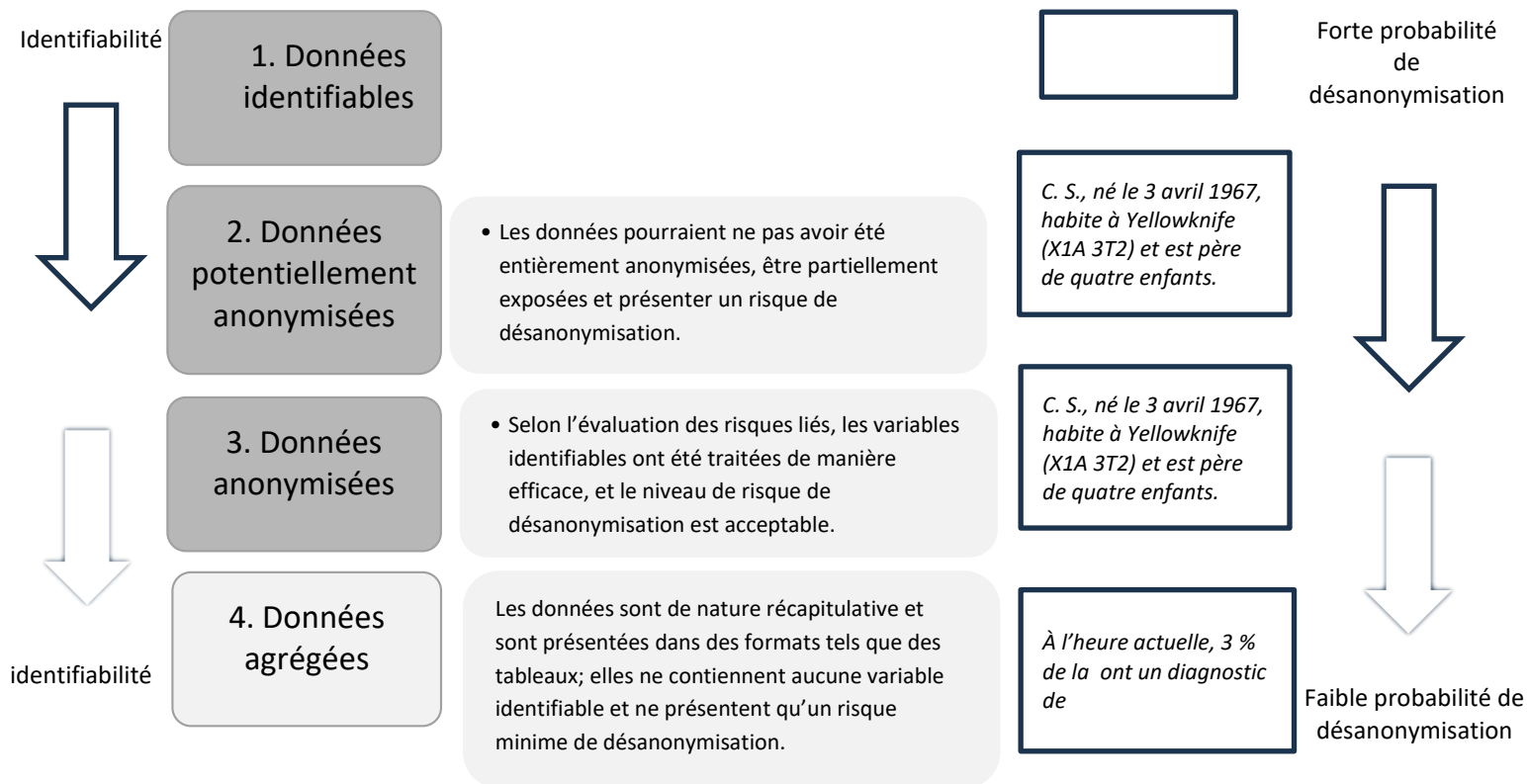
Le risque de désanonymisation peut évoluer en fonction des progrès technologiques et de l'augmentation de la quantité de renseignements accessibles. Il est judicieux de réévaluer régulièrement ce risque, notamment en vérifiant les points suivants :

- Déterminer s'il est nécessaire d'anonymiser davantage.

- Déterminer si la divulgation de renseignements anonymisés pourrait contribuer à désanonymiser les éléments d'information déjà accessibles.
- Évaluer les caractéristiques des rapports analytiques dans les systèmes électroniques lorsqu'on interroge un système électronique.

Tableau des dépendances

Identifiabilité et probabilité de désanonymisation en fonction du type de données



Techniques d'anonymisation recommandées

Technique d'anonymisation		Application		
		Géographique	Numérique	Alphanumérique
Réduction des données	Réduction des détails Réduire les détails en arrondissant les données ou en les regroupant en plus grandes catégories.	Limiter le code postal aux trois premiers caractères (région de tri d'acheminement).	Arrondir la date de naissance à l'année. Donner des dates par rapport à une date repère.	
	Suppression Implique l'élimination ou la rétention de dossiers de données.	En règle générale, il faut supprimer les codes géographiques lorsqu'ils contiennent six observations ou moins.	En règle générale, il faut supprimer les nombres lorsqu'ils contiennent six observations ou moins.	En règle générale, il faut supprimer les variables alphanumériques lorsqu'elles contiennent six observations ou moins.
	Échantillonnage Implique l'utilisation d'un échantillon aléatoire de dossiers d'une base de données.	Par exemple, la base de données comporte trop de dossiers pour l'analyse. Si l'analyse porte sur un échantillon aléatoire ou sur le cinquième des dossiers d'une base de données et qu'une technique supplémentaire a été appliquée (p. ex. réduction des détails). L'échantillonnage est souvent combiné à d'autres techniques afin de limiter les risques de désanonymisation.		
Modification des données	Ajout aléatoire de « bruit » aux données On ajoute du « bruit » en modifiant de façon aléatoire les valeurs des données afin de dissimuler des renseignements.	Modifier aléatoirement les codes postaux à un degré prédéterminé et acceptable (p. ex. les deux premiers ou derniers caractères).	Modifier aléatoirement la date de naissance à un degré prédéterminé acceptable (p. ex. décalage de six mois).	Modifier aléatoirement le nom à un degré acceptable prédéterminé (p. ex. le prénom ou le nom de famille).
	Permutation de données Implique l'identification des dossiers de deux personnes partageant des caractéristiques similaires avant de procéder à une permutation des données.	Des renseignements personnels sur la santé anonymisés sont créés à partir des dossiers qui ne sont pas les originaux, mais l'analyse produit les mêmes résultats que si on avait utilisé les renseignements originaux.		
	Substitution Permet de ne plus faire d'association entre un individu et des données identificatoires en remplaçant les données originales par des valeurs aléatoires ou échangées.	Si le code postal est modifié, il faut alors vérifier que l'indicatif régional du numéro de téléphone y correspond bien.	Si le numéro de la carte de santé est modifié, il faut alors vérifier que le nouveau numéro puisse être validé par la somme de contrôle.	Choisir de nouveaux noms dans une proportion raisonnable par rapport à leur usage dans la population générale. Si le nom de famille est modifié, le nouveau doit comporter le même nombre de caractères et avoir la même origine ethnique que l'original.
	Pseudonymisation Permet de ne plus faire d'association entre un individu et des données identificatoires en remplaçant les données par un ou plusieurs pseudonymes (ou noms de codes)	Peut être utilisée pour la plupart des données géographiques.	Peut être utilisée pour la plupart des données numériques. La date de naissance (ou le nom) peut être remplacée par un pseudonyme unique. Les pseudonymes doivent être générés de façon indépendante.	Peut être utilisée pour la plupart des données alphanumériques. Pour faciliter les liens entre les bases de données, le pseudonyme généré pour une personne donnée doit toujours être le même.

