Norme relative à la collecte de données sur la santé

1994 • 2019

Institut canadien d'information sur la santé

Canadian Institute for Health Information

Tous droits réservés.

Le contenu de cette publication peut être reproduit tel quel, en tout ou en partie et par quelque moyen que ce soit, uniquement à des fins non commerciales pourvu que l'Institut canadien d'information sur la santé soit clairement identifié comme le titulaire du droit d'auteur. Toute reproduction ou utilisation de cette publication et de son contenu à des fins commerciales requiert l'autorisation écrite préalable de l'Institut canadien d'information sur la santé. La reproduction ou l'utilisation de cette publication ou de son contenu qui sous-entend le consentement de l'Institut canadien d'information sur la santé, ou toute affiliation avec celui-ci, est interdite.

Pour obtenir une autorisation ou des renseignements, veuillez contacter l'ICIS :

Institut canadien d'information sur la santé
495, chemin Richmond, bureau 600
Ottawa (Ontario) K2A 4H6
Téléphone : 613-241-7860
Télécopieur : 613-241-8120
icis.ca
droitdauteur@icis.ca

© 2019 Institut canadien d'information sur la santé

Comment citer ce document :
Institut canadien d'information sur la santé. *Norme relative à la collecte de données sur la santé*. Ottawa, ON : ICIS; 2019.

This publication is also available in English under the title *Standard: Health Data Collection*.

Table des matières

Objectif 4
Portée 4
Définitions 4
Norme 5
Questions liées à la sécurité et participation des fournisseurs de données 5
Méthodes privilégiées pour la soumission des données 6
Conformité 8
Politiques, procédures et documents connexes 8
Pour en savoir plus 8

Objectif

La collecte de renseignements sur la santé par les fournisseurs de données fait partie intégrante du cycle de vie de l'information. Dans le processus de collecte de ces renseignements, l'Institut canadien d'information sur la santé (ICIS) doit préserver la confidentialité et l'intégrité des données au moment de leur transfert et de leur réception.

Portée

La norme dont il est ici question s'applique à la collecte par l'ICIS de données sur la santé. Pour les besoins de la présente, les données sur la santé comprennent les renseignements personnels sur la santé, les renseignements personnels des travailleurs de la santé et les données dépersonnalisées. La norme ne s'applique pas aux données agrégées — tel qu'elles sont définies dans les termes de la Politique de respect de la vie privée, 2010 ou de la Politique de respect de la vie privée des travailleurs de la santé, 2011 — ni aux renseignements diffusés publiquement que l'ICIS peut obtenir de sources externes.

Définitions

Remarque : Les définitions, sauf indication contraire, sont issues de la Politique de respect de la vie privée, 2010 et/ou de la Politique de respect de la vie privée des travailleurs de la santé, 2011 de l'ICIS.

Données agrégées : Données compilées à partir des enregistrements à un niveau d'agrégation qui garantit que l'identité des personnes ne pourra pas être établie selon des méthodes raisonnablement prévisibles. Les données agrégées dont la valeur des cellules est inférieure à 5 peuvent être considérées comme des données dépersonnalisées, des renseignements personnels sur la santé ou des renseignements personnels des travailleurs de la santé.

Renseignements confidentiels : Renseignements de nature très délicate qui doivent être protégés durant tout leur cycle de vie contre la perte ou le vol et contre l'accès, la communication, la copie, l'utilisation ou la modification non autorisés afin que leur confidentialité, leur intégrité et leur disponibilité soient assurées. Les renseignements confidentiels comprennent notamment les renseignements personnels sur la santé, les renseignements personnels des travailleurs de la santé et les données dépersonnalisées.

Données dépersonnalisées : Renseignements personnels sur la santé ou renseignements personnels des travailleurs de la santé qui ont été modifiés au moyen des processus de dépersonnalisation appropriés, de sorte que l'identité de la personne ne peut être déterminée selon une méthode raisonnablement prévisible.

Renseignements personnels des travailleurs de la santé : Renseignements au sujet d'un travailleur de la santé qui

- permettent d'identifier cette personne;
- peuvent être utilisés ou manipulés selon une méthode raisonnablement prévisible pour identifier cette personne; ou
- peuvent être associés, au moyen d'une méthode raisonnablement prévisible, à d'autres renseignements qui identifient cette personne.

Renseignements personnels sur la santé : Renseignements sur la santé qui identifient une personne ou qui permettraient d'identifier une personne selon une méthode raisonnablement prévisible, tel qu'ils sont définis dans la Politique de respect de la vie privée, 2010 de l'ICIS.

Membres du personnel : Toute personne qui travaille à l'ICIS, y compris les employés à temps plein ou à temps partiel, les personnes en détachement, les travailleurs temporaires, les étudiants et les employés contractuels, ainsi que les experts-conseils externes ou tout autre tiers fournisseur de services.

Norme

Questions liées à la sécurité et participation des fournisseurs de données

L'ICIS ne reçoit pas de renseignements personnels sur la santé en format papier. Les membres du personnel doivent encourager les fournisseurs de données à utiliser au moins une des méthodes de soumission indiquées dans la norme. Il est important, avant d'entreprendre la collecte de renseignements confidentiels auprès d'un fournisseur de données, d'informer ce fournisseur des méthodes de soumission privilégiées par l'ICIS.

Les membres du personnel doivent communiquer avec les responsables de la sécurité de l'information de l'ICIS (securite@icis.ca) avant d'accepter les données sur la santé d'un fournisseur de données au moyen de toute autre méthode.

Méthodes privilégiées pour la soumission des données

L'ICIS a privilégié 3 méthodes de soumission des données sur la santé par les fournisseurs de données; les voici en ordre de préférence :

Applications Web ou application serveur à serveur de l'ICIS

Les méthodes de soumission électronique approuvées par l'ICIS sont à privilégier et demeurent les plus sécuritaires d'entre toutes. Les applications utilisées permettent la transmission de données conformément aux normes de l'industrie au moyen de sessions chiffrées sécuritaires.

Dans la mesure du possible, les fournisseurs de données doivent utiliser les méthodes de soumission électronique de l'ICIS pour soumettre des données sur la santé. Pour déterminer si une méthode de soumission électronique existante convient à votre demande, communiquez avec le service Soutien et engagement des clients à ccs_data_trans@icis.ca. S'il est impossible d'utiliser une méthode de soumission électronique, les responsables du service détermineront avec l'équipe de la sécurité de l'information la méthode de soumission de données la plus sécuritaire.

Messagerie

Les renseignements confidentiels soumis en format électronique doivent être chiffrés et protégés par mot de passe au moyen d'une méthode approuvée. Pour en savoir plus sur les méthodes approuvées, écrivez à securite@icis.ca. Si la soumission comprend une disposition de l'abrégé ou un dictionnaire de données, le fournisseur de données devra envoyer ces documents à l'ICIS soit avec les fichiers chiffrés, soit dans un envoi distinct (p. ex. par courriel). Les mots de passe doivent être communiqués par un autre moyen (p. ex. par téléphone).

Pour soumettre des renseignements confidentiels par service de messagerie, le fournisseur de données doit utiliser un double emballage (2 enveloppes ou tout autre double emballage similaire) comme suit :

Enveloppe interne :

- Adresse du destinataire : celle de l'ICIS
- Adresse de l'expéditeur : celle du fournisseur de données
- Étiquette d'expédition (texte suggéré) : « Renseignements confidentiels. À ouvrir seulement par le destinataire. »

Enveloppe externe :

- Adresse du destinataire : celle de l'ICIS
- Adresse de l'expéditeur : celle du fournisseur de données

Le fournisseur de données qui soumet des données chiffrées en format électronique par service de messagerie doit joindre aux données une lettre de présentation indiquant que le contenu est chiffré et protégé par mot de passe et comportant les coordonnées, dont le nom et le numéro de téléphone, de toute personne que pourra contacter le destinataire pour confirmer la réception des documents ou obtenir les mots de passe nécessaires. Mention suggérée : « Fichiers chiffrés et protégés par mot de passe. Dès réception, communiquez avec <nom du fournisseur> au <numéro de téléphone du fournisseur> pour connaître le mot de passe requis. »

Tout service de messagerie utilisé pour soumettre des renseignements sur la santé doit être doté d'un service électronique de suivi et de confirmation de la réception.

Courriel

L'ICIS accepte les données soumises par courriel si aucune autre méthode n'est disponible. Les renseignements confidentiels en format électronique, avant d'être envoyés, doivent être chiffrés et protégés par mot de passe au moyen d'une méthode approuvée. Pour en savoir plus sur les méthodes approuvées, écrivez à securite@icis.ca.

Si la soumission comprend une disposition de l'abrégé ou un dictionnaire de données, le fournisseur de données devra envoyer ces documents à l'ICIS soit avec les fichiers chiffrés, soit dans un envoi distinct (p. ex. courriel). Les mots de passe doivent être communiqués par un autre moyen (p. ex. téléphone). Le fournisseur doit inclure les renseignements suivants dans le courriel accompagnant les données :

- Attestation que les fichiers sont chiffrés et protégés par mot de passe.
- Directives à suivre dès réception, y compris le nom et le numéro de téléphone de la personne à contacter pour obtenir les mots de passe requis. Mention suggérée : « Communiquez avec <nom du fournisseur> au <numéro de téléphone du fournisseur> pour connaître le mot de passe requis. »
- Directives si le courriel parvient au mauvais destinataire. Mention suggérée : « IMPORTANT : Ce courriel peut contenir des renseignements confidentiels. S'il ne vous est pas destiné, veuillez le supprimer. Merci de votre collaboration. »

Conformité

Le *Code de conduite de l'ICIS* (en anglais seulement) définit les comportements éthiques et professionnels au chapitre des relations, des renseignements, y compris des renseignements personnels sur la santé, et du milieu de travail. Les employés sont tenus de se conformer au code ainsi qu'aux politiques, procédures et protocoles de l'ICIS. La conformité au programme de respect de la vie privée et de sécurité de l'ICIS fait l'objet d'un contrôle, et les cas de non-conformité sont traités conformément au *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information* de l'ICIS. Les contraventions au code — y compris les contraventions aux politiques, aux procédures et aux protocoles de respect de la vie privée et de sécurité — sont référées aux Ressources humaines, au besoin, et peuvent entraîner des mesures disciplinaires allant jusqu'au congédiement.

Politiques, procédures et documents connexes

Politique de respect de la vie privée, 2010

Politique de respect de la vie privée des travailleurs de la santé, 2011

Pour en savoir plus

Pour en savoir plus, écrivez à securite@icis.ca.

aide@icis.ca

ICIS Ottawa
495, chemin Richmond
Bureau 600
Ottawa (Ont.)
K2A 4H6
613-241-7860

ICIS Toronto
4110, rue Yonge
Bureau 300
Toronto (Ont.)
M2P 2B7
416-481-2002

ICIS Victoria
880, rue Douglas
Bureau 600
Victoria (C.-B.)
V8W 2B7
250-220-4100

ICIS Montréal
1010, rue Sherbrooke Ouest
Bureau 602
Montréal (Qc)
H3A 2R7
514-842-2226

icis.ca

21166-1119