

THE COLLEGE OF
FAMILY PHYSICIANS
OF CANADA



LE COLLÈGE DES
MÉDECINS DE FAMILLE
DU CANADA



Canada Health
Infoway Inforoute
Santé du Canada



CONSEIL PRATIQUE

Utilisation avancée et éclairée des DME

MODULE 5

Intendance des données

NOVEMBRE 2018

Les médecins ont l'obligation légale et éthique de conserver un ensemble de dossiers médicaux qui facilitent la prestation de soins médicaux et servent de registre légal. Ce dossier devrait inclure un plan de traitement, ainsi que la justification clinique et les renseignements pertinents. La plupart des médecins de famille canadiens respectent cette obligation en utilisant un dossier médical électronique (DME) dans leur pratique clinique. Chaque organisme de réglementation provincial/territorial établit des normes qui doivent être respectées en ce qui a trait aux obligations du médecin pour la gestion des données et des renseignements médicaux.

L'intendance des données comprend la responsabilité légale et éthique pour la collecte, l'utilisation, la divulgation, la gestion et la protection globales des données¹. **La propriété des données** est le droit d'un patient d'avoir accès à l'information qui se trouve dans son dossier médical et de la corriger. Ce droit est reconnu dans la législation provinciale et fédérale. L'Association canadienne de protection médicale (ACPM) est claire au sujet de ce concept, et remarque que :

« Bien que la propriété des dossiers de santé ou médicaux (en version papier ou électronique) revienne aux médecins, aux établissements ou aux cliniques qui les ont créés pour leurs patients, l'information qui s'y trouve demeure la propriété de ces patients, qui peuvent en régir l'accès². »

Les renseignements personnels sur la santé (RPS) sont les données que les médecins de famille ont l'obligation de protéger. Il s'agit des données démographiques, des antécédents médicaux, des résultats d'examen et d'analyses de laboratoire, des renseignements sur les assurances et d'autres données que les professionnels de la santé recueillent pour identifier un patient individuel et déterminer les soins appropriés.

TROIS DIMENSIONS DE L'INTENDANCE DES DONNÉES

L'intendance des données comporte trois dimensions essentielles : la sécurité, la protection des renseignements personnels et la confidentialité.

Protection des renseignements personnels : Le droit de contrôler l'accès à sa personne et à l'information sur soi-même. Le droit à la protection des renseignements personnels signifie que les personnes peuvent décider quels types de renseignements donner, quelle quantité, à qui les donner et à quelles fins.³

Sécurité : Les mécanismes par lesquels les politiques de confidentialité sont mises en œuvre dans les systèmes informatiques, y compris les dispositifs de contrôle d'accès, d'intégrité et de disponibilité⁴.

Confidentialité : L'assurance que l'information identifiable sur les personnes, dont la diffusion pourrait constituer une violation de la vie privée d'une personne, ne sera pas divulguée sans son consentement, sauf dans la mesure où ceci est permis par la loi⁴. La confidentialité a été une obligation de la profession médicale bien avant le serment d'Hippocrate :

« Quoique je voie ou entende dans la société pendant, ou même hors de l'exercice de ma profession, je tairai ce qui n'a jamais besoin d'être divulgué, regardant la discrétion comme un devoir en pareil cas. »

LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS LIÉES À L'INTENDANCE DES DONNÉES

Pour les pratiques médicales, la protection des renseignements personnels est régie par la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)*. Pour les institutions gouvernementales, la protection des renseignements personnels est régie par la *Loi sur la protection des renseignements personnels*. Pour une liste complète des lois sur la protection des renseignements personnels dans chaque province, voir le site Web du [Commissariat à la protection de la vie privée du Canada](#).

Le Code type sur la protection des renseignements personnels (CAN/CSA-Q830-96 (C2002)) de l'Association canadienne de normalisation (CSA) forme la base de la LPRPDE et de la majorité des lois provinciales adoptées depuis 1996 (voir l'Annexe 1).

Les médecins de famille peuvent respecter les normes en suivant les guides publiés par leurs ordres de médecins ou ordres professionnels provinciaux/territoriaux, comme la [section Privacy and Confidentiality](#) dans les divisions de la Colombie-Britannique du Family Practice Toolkit. Vous trouverez des guides et sites Web provinciaux/territoriaux, ainsi que quelques ressources générales, à l'Annexe 2.

CONSIDÉRATIONS PRATIQUES POUR LES MÉDECINS DE FAMILLE

Dans la pratique médicale, les dossiers médicaux sont souvent maintenus par le fournisseur de service d'application qui héberge le DME du médecin. Le médecin signe une entente de partage de données⁵ avec le fournisseur de DME qui décrit quelles données seront partagées et de quelles façons, et limite habituellement la responsabilité du fournisseur en cas de violation de la vie privée (« clauses de dégage ment de responsabilités »).

Les médecins signent aussi des accords de gestion des données en tant que tierces parties pour les sources de données provinciales/territoriales et régionales (p. ex., services Web des pharmacies à l'échelle provinciale, portails de DSE en milieu hospitalier, des registres d'imagerie diagnostique basés sur le DSE comme des systèmes d'archivage d'image et de communication). Pour déterminer qui a eu accès aux données et à quel moment, de tels systèmes nécessitent une piste de vérification propre à l'utilisateur et une responsabilité de vérification. Chaque utilisateur, y compris les médecins de famille, a habituellement un identifiant d'ouverture de session qui lui est propre et signe une entente de sécurité.

De plus en plus, des questions sont soulevées entourant le type d'utilisation légitime de ces données sur la santé. Les médecins de famille n'ont pas besoin d'obtenir le consentement explicite pour partager les RPS avec des agents dans le cercle de soins des patients — par exemple, les consultants ou d'autres médecins spécialistes, le personnel et les ordres provinciaux — tant que ces échanges ont lieu dans le cadre de soins aux patients ou d'activités commerciales nécessaires (comme la facturation).

L'utilisation de RPS comprend l'échange de données rendues anonymes avec des groupes de médecins ou des agences gouvernementales pour des fins d'amélioration de la qualité ou de la santé des patients. Cependant, la controverse survient lorsque les parties utilisent les RPS ou les données rendues anonymes pour des fins de marketing ou pour créer un profil des prestataires de soins ou des patients individuels.

Enfin, les médecins de famille font souvent face à des frais imposés par les fournisseurs de DME pour l'accès à certains aspects de leurs données de façon significative, comme les données agrégées sur des populations de patients, ou les analyses intelligentes des données.

La [position du CMFC](#) à cet égard précise que les données sur les patients devraient être disponibles sans restriction pour favoriser l'amélioration de la qualité et les mesures de santé publique sans frais additionnels, et que les fournisseurs de DME devraient exposer une interface d'application qui permet aux médecins d'utiliser ou de transférer des données pour ces fins à peu de frais ou gratuitement.

Cette position correspond et appuie les piliers clés du [Centre de médecine de famille \(CMF\)](#), étant donné que ceux-ci sont liés à la mesure et à l'amélioration continue de la qualité; c'est-à-dire, exploiter les DME afin d'améliorer les soins aux patients. En tant que lieu de prestation de soins de confiance, le CMF devrait promouvoir l'assurance que les RPS confiés par les patients à la pratique sont strictement protégés, et utilisés aux fins prévues.





Annexe 1

RÈGLES POUR L'INTENDANCE DES DONNÉES: LES DIX PRINCIPES POUR LA PROTECTION LÉGALE DES RENSEIGNEMENTS PERSONNELS

1. **Responsabilité:** Une organisation est responsable des renseignements personnels dont elle a la gestion. Elle doit nommer une personne qui devra s'assurer de sa conformité à ces principes relatifs à l'équité.
2. **Détermination des fins de la collecte des renseignements:** Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci.
3. **Consentement:** Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.
4. **Limitation de la collecte:** L'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.
5. **Limitation de l'utilisation, de la communication et de la conservation:** À moins que la personne concernée n'y consente ou que la loi ne l'exige, les renseignements personnels ne doivent être utilisés ou communiqués qu'aux fins auxquelles ils ont été recueillis. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour répondre à ces fins.
6. **Exactitude:** Les renseignements personnels doivent être aussi exacts, complets et à jour que possible afin de satisfaire aux fins auxquelles ils sont destinés.
7. **Mesures de sécurité:** Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.
8. **Transparence:** Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles au public.
9. **Accès aux renseignements personnels:** Une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées.
10. **Possibilité de porter plainte à l'égard du non-respect des principes:** Toute personne doit être en mesure de se plaindre du non-respect des principes ci-dessus en communiquant avec la ou les personnes responsables de les faire respecter au sein de l'organisation concernée.

La version anglaise figure aussi dans: **CAN/CSA-Q830-96 (R2002) Model Code for the Protection of Personal Information**. © 1996 Canadian Standards Association. Reproduit avec permission.

Source: Principes relatifs à l'équité dans le traitement de l'information de la LPRPDE. Commissariat à la protection de la vie privée du Canada. Dans: www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/p_principe



Annexe 2

RESSOURCES PROVINCIALES ET TERRITORIALES — NORMES POUR L'INTENDANCE DES DONNÉES

Alberta

Collège des médecins et chirurgiens de l'Alberta

- [Standard of Practice – Patient Record Content](#)
- [Data Stewardship Principles Information Sharing Agreements](#)
- [Data Stewardship: Secondary Use of Health Information](#)
- [EMR Security Checklist](#)

Association médicale de l'Alberta

- [Guidelines for Data Sharing in Primary Care](#)
- [What you need to know about privacy agreements](#)

Colombie-Britannique

Collège des médecins et chirurgiens de la Colombie-Britannique

- [Practice Standard – Medical Records](#)

Doctors of BC

- [Physician Office IT Security Guide 2015](#)
- [Doctors of BC, College of Physicians and Surgeons BC, Office of the Information and Privacy Commissioner for BC. *BC Physician Privacy Toolkit: A guide for physicians in private practice, 3rd edition*. Vancouver, BC: authors; 2017.](#)

Manitoba

Gouvernement du Manitoba (conformément aux obligations à l'égard de la vie privée de la *Loi sur les renseignements médicaux personnels*)

- [Privacy Toolkit for Health Professionals](#)

Programme cybersanté du Manitoba

- [Confidentialité et sécurité](#)

Nouveau-Brunswick

Bureau du commissaire à l'intégrité du Nouveau-Brunswick

- [Loi sur l'accès et la protection en matière de renseignements personnels sur la santé](#)

Service Nouveau-Brunswick

- [Confidentialité et sécurité](#)

Terre-Neuve et Labrador

Collège des médecins et chirurgiens de Terre-Neuve et Labrador

- [Personal Health Information Act](#)

Health and Community Services

- [The Personal Health Information Act](#) (voir Resources for Custodians)

Territoires du Nord-Ouest

Bureau de l'accès à l'information et de la vie privée des Territoires du Nord-Ouest

- [Legislation](#) (Health Information Act, Access to Information and Protection of Privacy Act, etc.)

Nouvelle-Écosse

- [Personal Health Information Act](#)

Collège des médecins et chirurgiens de la Nouvelle-Écosse

- [Professional Standard Regarding Medical Records](#)
- [Privacy Policy](#)

Doctors Nova Scotia

- [EMRs and privacy](#)

Nunavut

Office of the Information and Privacy Commissioner of Nunavut

- [Legislation](#) (including Consolidation Of Access to Information and Protection of Privacy Act)
- [Access and Privacy Resources](#)

Ontario

Collège des médecins et chirurgiens de l'Ontario

- [Policy: Medical Records](#)
- [Policy: Confidentiality of Personal Health Information](#)
- [Privacy Code](#)

Île-du-Prince-Édouard

Collège des médecins et chirurgiens de l'Île-du-Prince-Édouard

- [Policy: The Application of the Principles of Privacy](#)
- [Policy: Retention, Access and Transfer of Medical Records](#)

Québec

Collège des médecins du Québec

- [Collège des médecins du Québec. La rédaction et la tenue des dossiers par le médecin en milieu](#)

extrahospitalier. Montréal, QC : auteur ; 2013

- Règlements sur les dossiers, les lieux d'exercice et la cessation d'exercice d'un médecin

Commission d'accès à l'information du Québec

Loi sur la protection de la vie privée liée aux dossiers sur la santé

- *Loi sur les services de santé et les services sociaux*
- *Lois sur l'assurance maladie*
- *Loi sur la Régie de l'assurance maladie du Québec*

Saskatchewan

Association médicale de la Saskatchewan

- Saskatchewan EMR program – Privacy and Security
- EMR Privacy Resources

Office of the Saskatchewan Information and Privacy Commissioner

- The Health Information Protection Act

Yukon

Commissaire à l'information et à la protection de la vie privée du Yukon

- *Loi sur la protection et la gestion des renseignements médicaux*
- Resources for Custodians

Yukon Medical Council

- Standards of Practice – Administration of Practice: [Records Management](#)

RESSOURCES : GÉNÉRAL

Arricale C, Barthold M, Brady JW, Eilenfield V, Gensinger RA, Houston SM, et al. *CPHIMS Review Guide, Third Edition: Preparing for Success in Healthcare Information and Management Systems*. Chicago, IL: Healthcare Information and Management Systems Society; 2013.

British Columbia Divisions of Family Practice. Practice Toolkit: Chapter 4. Privacy and Confidentiality website. www.divisionsbc.ca/provincial/ptprivacyconfident. Date de consultation : Le 25 juin 2018.

Collège des médecins de famille du Canada. Énoncé de position : Accès aux données du dossier médical électronique pour l'amélioration de la qualité et la recherche. Dans : http://www.cfpc.ca/uploadedFiles/Health_Policy/CFPC_Policy_Papers_and_Endorsements/CFPC_Policy_Papers/CFPC-Position-Statement-Supporting-access-data-electronic-medical-records-FR.pdf. Date de consultation : Le 25 juin 2018.

Site Web de la législation (Justice) du gouvernement du Canada. Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). laws-lois.justice.gc.ca/fra/lois/P-8.6/index.html. Date de consultation : Le 25 juin 2018.

Site Web de la législation (Justice) du gouvernement du Canada. Loi sur la protection des renseignements personnels. laws-lois.justice.gc.ca/fra/lois/P-21. Date de consultation : Le 25 juin 2018.

Commissariat à la protection de la vie privée du Canada. Lois et organismes de surveillance provinciaux et territoriaux en matière de protection de la vie privée. priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/lois-et-organismes-de-surveillance-provinciaux-et-territoriaux-en-matiere-de-protection-de-la-vie-privee/. Date de consultation : Le 25 juin 2018.

Site Web du Centre de médecine de famille. patientsmedicalhome.ca/fr. Date de consultation : Le 25 juin 2018.

Prater VS. Confidentiality, privacy and security of health information: Balancing interests. Dans : healthinformatics.uic.edu/resources/articles/confidentiality-privacy-and-security-of-health-information-balancing-interests. Date de consultation : Le 25 juin 2018.

Conseil canadien des normes. Model Code for the Protection of Personal Information (CAN/CSA-Q830-96 (R2002)). www.scc.ca/en/standardsdb/standards/6176. Date de consultation : Le 25 juin 2018.



Références

1. Certified Professional in Healthcare Information and Management Systems-Canada (CPHIMS-CA). *CPHIMS-CA Canadian Health Informatics Review and Reference Guide*. Toronto, ON: CPHIMS-CA; 2013. Available from: digitalhealthcanada.com/product/2013-cphims-ca-canadian-health-informatics-review-reference-guide. Date de consultation : Le 19 juin 2018.
2. Association canadienne de protection médicale. Le saviez-vous? Les patients peuvent restreindre l'accès à leurs renseignements de santé. Ottawa, ON: ACPM; 2017. Dans : www.cmpa-acpm.ca/fr/advice-publications/browse-articles/2017/did-you-know-patients-can-restrict-access-to-their-health-information. Date de consultation : Le 19 juin 2018.
3. Cavoukian A. *Privacy by Design: From Rhetoric to Reality*. Toronto, ON: Commissaire à l'information et à la protection de la vie privée de l'Ontario; 2012.
4. O'Carroll P, Yasnoff W, Ward M, Ripp L, Martin E, eds. *Public Health Informatics and Information Systems*. New York, NY: Springer Science & Business Media; 2006.
5. Association médicale canadienne. *Accords d'échange de données : Principes pour les dossiers médicaux électroniques/dossiers de santé électroniques*. Ottawa, ON: Association médicale canadienne; 2009. Dans : policybase.cma.ca/dbtw-wpd/Policypdf/PD09-01F.pdf. Date de consultation : Le 21 juin 2018.

