



MANITOBA
OMBUDSMAN

Southern Health-
Santé Sud

Atteinte à la vie
privée : Utilisation,
divulgaration et
sécurité des
renseignements

Réponse aux
recommandations
formulées dans le
dossier n° MO-01541/
2020-0251

Date de publication :
Avril 2025

LOI SUR LES RENSEIGNEMENTS MÉDICAUX PERSONNELS

RÉPONSE AUX RECOMMANDATIONS DU RAPPORT D'ENQUÊTE



RÉPONSE AUX RECOMMANDATIONS

Le 31 décembre 2024, le bureau de l'ombudsman a publié un rapport contenant des recommandations à la suite d'une enquête sur l'utilisation non autorisée de renseignements médicaux personnels par un employé de l'office régional de la santé Southern Health-Santé Sud (l'ORS). Le bureau de l'ombudsman a formulé six recommandations qui stipule :

Recommandation 1 : Que l'ORS élabore une politique encadrant l'utilisation des vérifications et mette en place un programme de vérification visant à assurer le respect des exigences prévues à l'article 18 de la *Loi sur les renseignements médicaux personnels* et à l'article 4 du règlement. La politique et le programme de vérification doivent être conformes aux lignes directrices relatives à la vérification des documents concernant l'activité des utilisateurs.

Recommandation 2 : Que l'ORS revoie sa politique sur la confidentialité des renseignements médicaux personnels et offre une formation supplémentaire à ses employés concernant cette politique et les exigences liées aux conflits d'intérêts.

Recommandation 3 : Que l'ORS établisse un processus officiel et élabore des lignes directrices pour déterminer à quel moment le dépositaire ou ses employés devraient évaluer les risques accrus pour la vie privée dans le cadre d'enquêtes en milieu de travail ou d'autres situations susceptibles d'entraîner une atteinte à la vie privée. Ces lignes directrices devraient traiter des éléments suivants :

- A. les facteurs de risque potentiels, comme le niveau d'accès aux renseignements médicaux personnels et aux systèmes d'information, le rôle de l'employé au sein du dépositaire, la nature de la plainte formulée, ainsi que tout autre facteur pouvant accroître le risque d'atteinte à la vie privée, notamment le motif de l'accès;
- B. les mesures à prendre pour atténuer ces risques, comme effectuer des vérifications des documents concernant l'activité des utilisateurs ou modifier les droits d'accès de l'employé aux systèmes d'information;
- C. la pertinence de consulter la personne responsable de la protection de la vie privée, ainsi que la nature des renseignements à lui transmettre.

Recommandation 4 : Que l'ORS précise dans ses politiques, ses procédures et ses formations que, lorsqu'il est impossible pour le dépositaire de déterminer si un accès était autorisé, il ne doit pas présumer par défaut que cet accès l'était. Dans de tels cas, le dépositaire doit :

- A. revoir ses processus afin de cerner toute lacune dans sa capacité à déterminer si un accès est autorisé;
- B. déterminer les garanties ou les processus qui permettraient de combler ces lacunes, et les mettre en place dès que possible.

Recommandation 5 : Que l'ORS élabore des lignes directrices à l'intention des employés concernant les démarches à suivre s'ils n'ont pas accès à l'information ou aux systèmes dont ils ont besoin pour accomplir leurs tâches. Ces lignes directrices doivent inclure un processus pour :

- A. mettre à jour ou demander la mise à jour des droits d'accès d'un utilisateur,
- B. demander l'accès à de l'information dans des situations d'urgence où il n'est pas possible de prendre le temps de réviser et d'attribuer de nouveaux droits d'accès,
- C. consigner les accès effectués en situation d'urgence par une personne qui ne détient pas les droits d'accès requis,
- D. vérifier les accès d'urgence de ce type afin de s'assurer que les renseignements médicaux personnels ne sont consultés de cette manière que lorsqu'il est réellement nécessaire de le faire.

Recommandation 6 : Que l'ORS s'assure que la formation offerte à ses employés comporte des renseignements adéquats sur ses systèmes électroniques d'information sur la santé.

L'ombudsman a demandé à l'ORS de fournir, au plus tard le 14 février 2025, une réponse écrite indiquant s'il acceptait ou non les recommandations. Le 10 février 2025, l'ORS a informé notre bureau qu'il acceptait entièrement les recommandations 1, 2, 3, 4 et 6. Il a aussi indiqué accepter la recommandation 5, mais avec certaines modifications, comme suit :

Nous reconnaissons l'importance de cette recommandation et, bien que nous soyons d'accord avec le principe qui la sous-tend, nous souhaitons proposer une approche modifiée.

- A. Comme le mentionne le rapport d'enquête, l'office de la santé a collaboré avec d'autres autorités sanitaires de la province afin de créer des rôles de sécurité standardisés à attribuer au personnel des services de soutien. Ces rôles de sécurité seront établis en fonction des autorisations requises selon les fonctions occupées (p. ex., adjoints comptables, préposés à l'inscription, commis aux dossiers médicaux, etc.). Un travail similaire est en cours pour définir des rôles de sécurité standard pour les cliniciens, les infirmières et infirmiers, ainsi que les professionnels de la santé paramédicaux.

Les processus et les formulaires permettant de mettre à jour les droits d'accès des utilisateurs sont disponibles ici. Il incombe aux gestionnaires d'activer, de mettre à jour ou de désactiver les profils d'utilisateur. Santé numérique fournit aux gestionnaires des rapports de gestion des sites, qui présentent les utilisateurs actifs et inactifs à des fins de révision.

À la lumière de l'enquête, nous reconnaissons la nécessité d'offrir davantage d'encadrement et de formation au personnel concernant l'activation, la mise à jour et la désactivation des profils d'utilisateur.

Nous acceptons pleinement cette recommandation.

- B. Fournir des lignes directrices ou un processus permettant au personnel sans privilèges d'accès de demander, en situation d'urgence, l'accès à de l'information en leur nom pourrait être interprété comme une permission et va à l'encontre de la politique actuelle, qui interdit strictement d'accéder à de l'information au nom d'un autre membre du personnel.

Étant donné la récente standardisation des rôles de sécurité et les travaux en cours, il ne devrait y avoir aucune situation où un membre du personnel demande l'accès à de l'information à laquelle il n'est pas autorisé à accéder. Nous ne croyons donc pas que cette recommandation soit pertinente.

- C. Bien que les demandes d'accès non autorisé ne devraient pas se produire, il peut arriver qu'un utilisateur disposant des autorisations appropriées soit bel et bien autorisé à consulter un dossier, mais que les preuves permettant de le confirmer soient difficiles à vérifier en raison du délai entre l'accès et la vérification.

Les systèmes électroniques de santé ne permettent pas tous d'ajouter des notes complémentaires, ce qui signifie que les justifications d'accès devront être consignées en dehors du dossier de santé.

Nous ne sommes pas en faveur d'exiger que le personnel consigne les raisons de chaque accès, car cela pourrait entraîner des goulots d'étranglement, accroître les risques d'atteinte à la vie privée et mener à un blocage opérationnel lié à la protection des renseignements personnels. Nous privilégierons plutôt la sensibilisation du personnel à l'importance de fournir des preuves à l'appui. Si des notes complémentaires ne peuvent pas être ajoutées au dossier de santé, le personnel sera invité à informer son gestionnaire de tout enjeu potentiel lié à un accès, afin que ce dernier puisse conserver de façon sécuritaire les détails pertinents aux fins de vérification et déterminer si une formation supplémentaire est nécessaire.

Nous acceptons donc cette recommandation, avec la modification indiquée.

D. Nous acceptons cette recommandation en tenant compte de la modification décrite au point C.

CONCLUSION

L'ombudsman a examiné les modifications proposées par l'ORS et a déterminé que la recommandation modifiée répondait de façon adéquate aux préoccupations sur lesquelles elle était fondée.

L'ombudsman a demandé à l'ORS de fournir un plan de mise en œuvre des recommandations dans un délai de 60 jours suivant leur acceptation. Notre bureau a reçu le plan de mise en œuvre et assurera le suivi de son application.

Avril 2025
Ombudsman du Manitoba

Offert en d'autres formats sur demande.

OMBUDSMAN DU MANITOBA
5, rue Donald, bureau 300, Winnipeg (Manitoba) R3L 2T4
204-982-9130 | 1-800-665-0531 | ombudsman@ombudsman.mb.ca
www.ombudsman.mb.ca

