MANITOBA OMBUDSMAN

RAPPORT D'ENQUÊTE EN VERTU DE LA LOI SUR LES RENSEIGNEMENTS MÉDICAUX PERSONNELS

Southern Health-Santé Sud

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

Dossier Nº MO-01541/2020-0251
Rapport public accompagné de recommandations

Date de publication :
Décembre 2024

Dispositions considérées :
LRMP – 5(1), 6(2), 13(1), 13(2), 16, 18(1), 18(2), 20(1), 20(2), 20(3), 57, 63(2)a), 63(2)b), 63(3)a)
Règlement sur les renseignements **médicaux personnels – 2, 3, 4(1), 4(4), 5, 6, 8(1), 8(2)**

SOMMAIRE

En mars 2020, l'office régional de la santé Southern Health-Santé Sud (l'ORS) a pris connaissance d'une atteinte à la vie privée, dans le cadre de laquelle un fonctionnaire chargé de la protection des renseignements médicaux personnels accédait sans autorisation à des renseignements médicaux personnels concernant une tierce personne. Le fonctionnaire chargé de la protection des renseignements médicaux personnels de l'ORS a signalé l'atteinte à notre bureau, et nous avons également reçu des plaintes de la part de deux personnes alléguant que leurs renseignements médicaux personnels avaient été consultés de manière inappropriée.

Notre bureau a mené une enquête sur les plaintes et a conclu que l'utilisation des renseignements médicaux personnels des plaignants n'était pas autorisée. Nous avons également examiné les politiques, les procédures et les autres renseignements fournis par l'ORS, et avons déterminé que ce dernier ne respectait pas les exigences et les normes de sécurité en matière de protection des renseignements médicaux personnels prévues par la Loi sur les renseignements médicaux personnels. Nous formulons donc des recommandations à l'intention de l'ORS afin de remédier aux problèmes relevés au cours de notre enquête.

TABLE DES MATIÈRES

INTRODUCTION

Le présent rapport porte sur une enquête menée en vertu de la *Loi sur les renseignements médicaux personnels* (LRMP) concernant l'accès non autorisé à des renseignements médicaux personnels de tierces personnes par un fonctionnaire chargé de la protection des renseignements médicaux personnels dans un établissement de soins de santé (l'établissement). L'établissement est exploité et doté en personnel par l'ORS. Notre bureau a déterminé que, puisque l'établissement ne constitue pas une entité distincte et que son personnel relève de l'ORS, c'est ce dernier qui est considéré comme le dépositaire en vertu de la LRMP.

Les renseignements médicaux personnels comptent parmi les renseignements les plus sensibles qu'on puisse détenir au sujet d'une personne. Le public doit pouvoir avoir confiance que les dépositaires n'en font pas un usage abusif ni ne mettent ces renseignements en danger.

Le manque de confiance en la protection de leurs renseignements médicaux personnels peut amener des personnes du public à refuser que les dépositaires les recueillent ou les utilisent. Cela peut aussi mener certaines personnes à retarder ou à annuler des rendez-vous médicaux, par crainte que leurs renseignements ne soient pas suffisamment protégés. Lorsque le public doute de la capacité du système de santé à assurer la confidentialité de ces renseignements, c'est la confiance envers l'ensemble du système de santé qui peut en être ébranlée.

Acronymes pertinents

- LRMP : Loi sur les renseignements médicaux personnels
- DEP : dossier électronique du patient

Parties concernées

- Office régional de la santé Southern Health-Santé Sud (l'ORS)
- Fonctionnaire chargé de la protection des renseignements médicaux personnels de l'office régional de la santé Southern Health-Santé Sud
- Établissement de soins de santé (l'établissement)
- Fonctionnaire chargé de la protection des renseignements médicaux personnels de l'établissement de soins de santé
- Personnes dont les renseignements médicaux personnels ont été consultés

CONTEXTE

Le 23 avril 2020, l'ORS a informé notre bureau qu'il y avait eu une atteinte à la vie privée d'une personne. Peu de temps après, nous avons reçu deux plaintes liées à cette situation. Trois personnes ont également porté plainte auprès de l'ORS concernant l'utilisation de leurs renseignements médicaux personnels. Ces plaintes ont été examinées par le fonctionnaire chargé de la protection des renseignements médicaux personnels de l'ORS.

Notre bureau a ouvert trois enquêtes : une enquête initiée par l'ombudsman[1] en vertu de la partie 4 de la LRMP, ainsi que deux enquêtes liées à des plaintes en vertu de la partie 5. Nous avons publié des rapports distincts pour chacune des deux plaintes, dans lesquels nous avons conclu à des atteintes à la vie privée concernant les renseignements médicaux personnels des deux personnes visées.

L'enquête initiée par l'ombudsman visait à examiner les circonstances entourant les atteintes à la vie privée, les mesures prises par l'ORS pour y remédier, ainsi que les actions entreprises pour réduire le risque que de telles atteintes se reproduisent. Plus précisément, nous avons voulu examiner les politiques, les procédures et les garanties mises en place par l'ORS. Le présent rapport concerne l'enquête initiée par l'ombudsman.

Enquêtes sur les atteintes à la vie privée menées par l'ORS

En réponse aux plaintes liées à la vie privée, le fonctionnaire chargé de la protection des renseignements médicaux de l'ORS a effectué une vérification des dossiers électroniques des personnes concernées. Ces vérifications ont confirmé que le fonctionnaire chargé de la protection des renseignements médicaux de l'établissement avait accédé aux renseignements médicaux personnels des personnes concernées. Le fonctionnaire chargé de la protection des renseignements médicaux de l'ORS a donc ouvert des enquêtes sur les atteintes à la vie privée liées à ces accès.

[1] Une enquête initiée par l'ombudsman est une enquête menée à la discrétion de l'ombudsman en vertu de l'alinéa 28a) de la LRMP. Ces enquêtes ne nécessitent pas le dépôt d'une plainte et visent à surveiller et à assurer le respect des exigences de la LRMP.

L'ORS a déterminé, dans le cas d'une des plaintes, que l'accès aux renseignements médicaux personnels de la personne concernée était autorisé, en raison du moment où l'accès a eu lieu et du type d'accès habituellement effectué par le fonctionnaire chargé de la protection des renseignements médicaux de l'établissement à cette période. Dans le cas d'une autre personne, le fonctionnaire de l'établissement a reconnu avoir consulté les renseignements médicaux personnels de façon inappropriée. À la lumière de cet aveu, l'ORS a conclu qu'il y avait eu atteinte à la vie privée.

Pour la dernière personne concernée, l'ORS n'a pas été en mesure de déterminer de façon concluante si l'accès était autorisé ou non. Il a finalement conclu que l'utilisation des renseignements médicaux personnels de cette personne était autorisée et qu'il n'y avait donc pas eu atteinte à la vie privée.

L'ORS a informé les personnes concernées de ses conclusions et de leur droit de porter plainte auprès de l'ombudsman.

L'ORS a également informé notre bureau de l'atteinte à la vie privée concernant les renseignements médicaux personnels d'une des personnes. Au moment où cette atteinte s'est produite, le signalement des atteintes à la vie privée à l'ombudsman était considéré comme une bonne pratique en vertu de la LRMP, mais n'était pas obligatoire[2].

Enquêtes de notre bureau sur les plaintes et poursuite

Nous avons terminé notre enquête sur les deux plaintes liées à l'accès aux renseignements médicaux personnels de certaines personnes en janvier 2021. Dans le cas d'une de ces personnes, l'ORS a déterminé qu'il y avait eu atteinte à la vie privée. Notre bureau est arrivé à la même conclusion et a déterminé que l'utilisation des renseignements médicaux personnels de cette personne n'était pas autorisée.

Comme mentionné plus haut, l'ORS n'a pas été en mesure de déterminer de façon concluante si l'accès était autorisé, et a conclu qu'il n'y avait pas eu atteinte à la vie privée. Cette conclusion reposait sur l'absence de preuve démontrant que l'utilisation des renseignements médicaux personnels de la personne concernée n'était pas

[2] En 2022, des modifications à la LRMP sont entrées en vigueur. Le paragraphe 19.0.1(2) exige désormais les dépositaires à informer les personnes concernées et à signaler toute atteinte à la vie privée à l'ombudsman lorsqu'il existe un risque réel de préjudice grave.

autorisée. Notre bureau est d'avis que les dépositaires doivent être en mesure de démontrer, à l'aide de preuves concrètes, que l'utilisation des renseignements médicaux personnels d'une personne est bel et bien autorisée.

En l'absence de telles preuves, l'utilisation doit être considérée comme non autorisée en vertu de la LRMP. Par conséquent, notre bureau a conclu que l'utilisation des renseignements médicaux personnels de cette personne n'était pas autorisée.

Poursuite

À la lumière des éléments recueillis au cours de notre enquête, le Service des poursuites du Manitoba a déterminé qu'il y avait suffisamment de preuves pour engager une poursuite liée à l'atteinte à la vie privée d'une personne concernant ses renseignements médicaux personnels.

Le 28 juin 2021, l'ombudsman a déposé trois accusations contre le fonctionnaire chargé de la protection des renseignements médicaux de l'établissement, en vertu des alinéas 63(2)a), 63(2)b) et 63(3)a) de la LRMP.

> ***Infraction par les employés, les dirigeants, les cadres ou les mandataires***
> ***63(2)*** *Malgré le paragraphe 61(2), commet une infraction l'employé, le dirigeant, le cadre ou le mandataire d'un dépositaire, d'un gestionnaire de l'information ou d'un organisme de recherche en matière de santé qui, sans l'autorisation de la personne ou de l'entité pour le compte de laquelle il travaille :*
>
> *a) communique volontairement des renseignements médicaux personnels dans des circonstances où cette personne ou cette entité ne serait pas autorisée à les communiquer sous le régime de la présente loi;*
>
> *b) utilise, consulte ou tente de consulter volontairement les renseignements médicaux personnels d'autrui.*

Infractions par les dépositaires et les gestionnaires de l'information

63(3) *Commet une infraction le dépositaire, le gestionnaire de l'information ou l'organisme de recherche en matière de santé qui :*

a) recueille, utilise, vend ou communique des renseignements médicaux personnels en contravention avec la présente loi;

Le 7 juillet 2022, le fonctionnaire chargé de la protection des renseignements médicaux de l'établissement a plaidé coupable à l'accusation d'utilisation non autorisée de renseignements médicaux personnels, en vertu de l'alinéa 63(2)b) de la LRMP, et a reçu une amende de 5 500,00 $.

Notre bureau ne publie pas de rapports d'enquête liés à une poursuite tant que celle-ci n'est pas terminée. Pendant cette période, l'enquête initiée par l'ombudsman a également été mise sur pause afin que tous les éléments liés à la poursuite puissent être menés à terme. Bien que les enquêtes et la publication des rapports aient été suspendues, notre bureau a assuré un suivi auprès des parties concernées pour les tenir informées de l'évolution de la poursuite.

Nous avons également demandé et reçu des mises à jour sur les mesures prises par l'ORS pour améliorer son programme de protection de la vie privée durant cette période. Le 10 novembre 2022, nous avons publié les rapports d'enquête finaux liés aux deux plaintes que nous avions reçues.

PARTIE 4 ENQUÊTE

Comme mentionné précédemment, notre bureau a également entrepris une enquête en vertu de la partie 4 de la LRMP afin d'évaluer la conformité de l'ORS à cette Loi. Ce type d'enquête vise à s'assurer que le dépositaire a pris les mesures appropriées pour traiter l'atteinte à la vie privée, et que ses politiques, procédures et pratiques permettent de réduire adéquatement le risque d'accès non autorisé futur aux renseignements médicaux personnels, tout en respectant les exigences de la LRMP.

Notre bureau a demandé des copies des politiques et procédures de l'ORS en matière d'atteintes à la vie privée, de vérifications, ainsi que toute autre politique liée à la LRMP. Nous avons également examiné les vérifications des activités des utilisateurs effectuées

par l'ORS concernant les accès du fonctionnaire de l'établissement aux renseignements médicaux personnels des personnes concernées.

Notre bureau considère cette atteinte à la vie privée comme étant grave, puisque la personne ayant accédé sans autorisation à des renseignements médicaux personnels occupait le poste de fonctionnaire chargé de la protection des renseignements médicaux personnels au sein de l'établissement. Cette personne agissait également à titre de gestionnaire de l'information, ce qui signifie qu'elle était responsable de veiller à l'exactitude des renseignements conservés dans les systèmes de gestion de l'information.

Le fonctionnaire chargé de la protection des renseignements médicaux de l'établissement avait accès aux renseignements conservés dans l'établissement ainsi qu'aux systèmes de l'ORS, y compris aux dossiers des patients ayant reçu des soins dans un établissement relevant de l'office. L'article 57 de la LRMP énonce les fonctions d'un tel fonctionnaire :

> ***Fonctionnaires chargés de la protection des renseignements médicaux personnels***
>
> ***57*** *Les établissement de soins de santé et les organismes de services de santé désignent un ou plusieurs de leurs employés à titre de fonctionnaires chargés de la protection des renseignements médicaux personnels. Il incombe à la ou aux personnes désignées :*
>
> *a) de s'occuper des demandes des particuliers qui désirent examiner et reproduire ou faire corriger des renseignements médicaux personnels sous le régime de la présente loi;*
>
> *b) de façon générale, de faciliter l'observation de la présente loi par le dépositaire.*

Faciliter la conformité d'un dépositaire à la Loi peut notamment consister à s'assurer que ses politiques et procédures respectent cette LRMP, à veiller à ce que les employés reçoivent une formation adéquate à ce sujet, à enquêter sur les plaintes liées à la vie privée, ainsi qu'à garantir que les renseignements médicaux personnels sous la garde et le contrôle du dépositaire sont protégés et utilisés de manière appropriée.

Lorsqu'une personne chargée de veiller à la bonne utilisation des renseignements médicaux personnels en fait plutôt un usage inapproprié, cela porte gravement atteinte à la relation de confiance non seulement pour la personne dont la vie privée a été compromise, mais aussi pour l'ensemble de la communauté. Des atteintes de ce genre influencent la perception qu'ont les membres de la communauté quant à la protection de leurs renseignements médicaux personnels et peuvent affecter leur relation avec le système de santé.

Au cours de cette enquête, notre bureau a relevé plusieurs préoccupations concernant la façon dont l'ORS a traité l'atteinte à la vie privée, ainsi que les mesures en place pour éviter qu'une situation semblable ne se reproduise.

Nous présentons et analysons ci-dessous chacun des enjeux soulevés.

1. Documentation des activités liées aux vérifications

La réalisation régulière de vérifications des accès aux renseignements médicaux personnels favorise la transparence et la reddition de comptes quant à leur utilisation, ce qui renforce la confiance du public envers la capacité du système de santé à gérer ces renseignements de façon responsable et à protéger la vie privée.

Exigences législatives

Le *Règlement sur les renseignements médicaux personnels* (le règlement) établit les exigences que doivent respecter les dépositaires pour assurer la sécurité des renseignements médicaux personnels et pour vérifier l'efficacité de leurs garanties. Le règlement exige également que les dépositaires disposent de politiques et de procédures écrites en matière de sécurité, et qu'ils effectuent des vérifications des documents concernant l'activité des utilisateurs.

> ***Directives écrites***
> ***2*** *Le dépositaire établit des directives écrites qu'il observe et qui contiennent :*
>
> *a) des dispositions pour la sécurité des renseignements médicaux personnels au cours de leur collecte, de leur utilisation, de leur communication, de leur stockage et de leur destruction, notamment des mesures :*

(i) garantissant la sécurité des renseignements si un document les contenant est retiré d'un lieu désigné d'accès réservé,

(ii) garantissant la sécurité des renseignements sous forme électronique si le matériel informatique ou les supports électroniques amovibles servant à leur consignation sont utilisés à une autre fin ou qu'il en soit disposé;

b) des dispositions prévoyant la consignation des atteintes à la sécurité des renseignements;

c) des mesures correctrices visant à remédier aux atteintes à la sécurité des renseignements.

Protection supplémentaire des systèmes d'information électronique en matière de santé

4(1) *Conformément aux directives du ministre, le dépositaire établit et conserve ou fait établir et conserver un document concernant l'activité des utilisateurs pour tout système d'information électronique qu'il utilise afin de maintenir des renseignements médicaux personnels.*

4(4) *Conformément aux directives du ministre, le dépositaire examine les documents concernant l'activité des utilisateurs afin de déceler les atteintes à la sécurité.*

Vérification

8(1) *Le dépositaire vérifie les mesures de protection qu'il a prises au moins une fois tous les deux ans.*

8(2) *Le dépositaire corrige dès que possible les carences que la vérification lui permet, le cas échéant, de déceler dans les mesures de protection qu'il a prises.*

La LRMP oblige également les dépositaires à veiller à ce que les renseignements médicaux personnels qu'ils utilisent ou communiquent soient exacts, à jour, complets et non trompeurs :

Obligation quant à l'exactitude des renseignements

16 *Avant d'utiliser ou de communiquer des renseignements médicaux personnels, le dépositaire prend toutes les dispositions possibles pour faire en sorte que les renseignements soient exacts, à jour, complets et non trompeurs.*

La LRMP exige que les dépositaires mettent en place des garanties pour protéger les renseignements médicaux qu'ils recueillent. Une partie de cette responsabilité consiste à s'assurer que seules les personnes ayant le droit d'accéder aux renseignements médicaux personnels le font. Ces exigences sont présentées ci-dessous.

Obligation d'établir des garanties

18(1) *En conformité avec les exigences réglementaires, le dépositaire protège les renseignements médicaux personnels en établissant des garanties administratives, techniques et physiques satisfaisantes afin que soient assurées la confidentialité, la sécurité, l'exactitude et l'intégrité des renseignements.*

Garanties particulières

18(2) *Sans préjudice du paragraphe (1), le dépositaire :*

a) met en œuvre des dispositifs qui limitent le nombre de personnes qui peuvent utiliser les renseignements médicaux personnels qu'il maintient à celles qu'il autorise explicitement à cette fin;

b) met en œuvre des dispositifs visant à garantir que les renseignements médicaux personnels qu'il maintient ne puissent être utilisés que si :

(i) la personne qui cherche à les utiliser est bien l'une des personnes qu'il a autorisées à cette fin,

(ii) l'utilisation projetée est effectivement autorisée sous le régime de la présente loi;

c) met en œuvre des mesures visant à empêcher l'interception de renseignements médicaux personnels par des personnes non autorisées,

s'il utilise des moyens électroniques pour demander la communication de tels renseignements ou pour répondre à des demandes de communication;

d) veille à ce que les demandes de communication de renseignements médicaux personnels auxquelles il répond contiennent suffisamment de détails pour identifier uniquement le particulier que les renseignements concernent.

L'objectif de ces dispositions de la LRMP et du règlement est de faire en sorte que les renseignements médicaux personnels ne soient consultés que par une personne autorisée et uniquement dans un but autorisé, et que ces renseignements soient exacts et à jour. Les vérifications liées à la protection de la vie privée dans les systèmes électroniques aident les dépositaires à savoir quand, comment et par qui les renseignements médicaux personnels sont utilisés.

Le fait de consigner ces vérifications permet aux dépositaires de cerner les habitudes normales d'accès et de détecter les tendances révélatrices d'un accès potentiellement inapproprié. Cette consignation permet aussi de documenter les motifs pour lesquels les renseignements médicaux personnels ont été consultés durant la vérification. Les vérifications axées sur l'assurance de la qualité aident les dépositaires à garantir que les renseignements sont exacts et à jour.

Le ministre de la Santé a établi une série de lignes directrices en lien avec les document concernant l'activité des utilisateurs, lesquelles comprennent des directives sur la réalisation de vérifications liées à la protection de la vie privée dans les systèmes contenant des renseignements médicaux personnels, comme l'exige le paragraphe 4(4) du règlement.

Les lignes directrices exigent que les dépositaires mettent en place un processus encadrant la réalisation des vérifications liées à la protection de la vie privée. Elles exigent également que les dépositaires mettent en place un processus de surveillance des personnes responsables des vérifications. Ce dernier vise à s'assurer que les accès effectués par les employés chargés de surveiller les systèmes et les actions des autres employés font eux aussi l'objet d'un examen, afin de confirmer qu'ils utilisent les renseignements médicaux personnels de façon appropriée.

Les lignes directrices présentent également plusieurs types de vérifications liées à la protection de la vie privée qui devraient être effectuées. Les vérifications aléatoires sont réalisées à des intervalles déterminés au hasard par le dépositaire. Elles peuvent être mises en place pour repérer certaines situations particulières, par exemple lorsqu'un employé consulte les renseignements médicaux personnels d'une personne portant le même nom de famille que lui ou d'une personne ayant récemment fait les manchettes. Il existe aussi des vérifications ciblées, qui sont menées lorsque le dépositaire relève un enjeu précis devant faire l'objet d'une enquête, par exemple à la suite d'une plainte pour utilisation non autorisée.

La LRMP, le règlement et les lignes directrices exigent tous que les dépositaires s'assurent que les systèmes contenant des renseignements médicaux personnels font l'objet de vérifications, et qu'un processus clair encadre la manière dont ces vérifications sont effectuées.

Tout processus de vérification mis en place par un dépositaire doit inclure des exigences précisant comment les utilisateurs sont sélectionnés aux fins de vérification, à quelle fréquence les vérifications sont effectuées, quels types d'accès sont examinés, quelles mesures sont prises en cas d'accès suspect, de quelle manière la vérification est consignée, ainsi que les résultats de la vérification.

Renseignements sur les vérifications fournis par l'ORS

L'ORS a indiqué que des vérifications liées à la protection de la vie privée sont effectuées soit par l'office lui-même, soit à l'échelle de l'établissement – dans ce cas-ci, par l'établissement. Divers types de vérifications peuvent nécessiter l'examen des renseignements médicaux personnels de patients dans les systèmes électroniques. Certaines de ces vérifications (tel que l'exige la LRMP) peuvent être effectuées de façon aléatoire ou en réponse à une plainte. D'autres vérifications sont effectuées à des fins d'assurance de la qualité, par exemple pour concilier les données statistiques de fin de mois ou pour s'assurer que l'information figurant dans les dossiers des patients, comme l'adresse d'un médecin, est exacte.

Le fonctionnaire chargé de la protection des renseignements médicaux de l'ORS a indiqué que les vérifications liées à l'assurance de la qualité ont généralement lieu à un moment précis de l'année. Ainsi, si des dossiers de patients sont consultés durant ces périodes, on suppose que ces accès sont liés à cet exercice. Dans le cadre de ces

vérifications, les dossiers peuvent être sélectionnés au hasard ou, si certains renseignements doivent être mis à jour, des dossiers précis sont alors examinés.

Notre bureau a demandé à l'ORS comment les dossiers sont sélectionnés aux fins de vérifications liées à la protection de la vie privée. L'office a indiqué que plusieurs systèmes électroniques d'information sur la santé sont utilisés dans le réseau, et que chacun de ces systèmes dispose de ses propres méthodes pour effectuer ce type de vérification.

Les principaux systèmes utilisés par l'ORS sont DossiÉ, le dossier électronique du patient (DEP) et le dossier médical électronique (DME). Soins communs, qui agit à la fois comme dépositaire des renseignements médicaux personnels contenus dans DossiÉ et comme gestionnaire de l'information (fournisseur de solutions informatiques) pour le système DEP, effectue des vérifications centrées sur les utilisateurs de ces systèmes tous les un à deux ans. Soins communs effectue également des vérifications de « même nom »[3] sur ces systèmes à des intervalles aléatoires.

Le DME est géré par l'ORS. Deux autres systèmes peuvent également être consultés par les employés de l'office : Le système de gestion de l'information sur la santé publique et Procura. Comme pour DossiÉ et le DEP, l'ORS ne lance pas lui-même les vérifications pour ces systèmes, mais participe aux activités de vérification menées par Soins communs.

Notre bureau a demandé des copies de toute politique de l'ORS liée aux vérifications. L'ORS a fourni une politique liée aux vérifications, qui exige qu'une vérification des garanties soit effectuée tous les deux ans. Même s'il n'existe aucune politique imposant d'autres types de vérifications, le fonctionnaire chargé de la protection des renseignements médicaux de l'ORS a commencé à effectuer des vérifications de même nom dans le système DME en 2022.

Le fonctionnaire chargé de la protection des renseignements médicaux de l'ORS a indiqué qu'il demanderait à Soins communs | Santé numérique un rapport sur l'activité

[3] Une vérification de « même nom » désigne le processus qui consiste à repérer, dans une base de données, les personnes portant le même nom. L'un des objectifs principaux de ce type de vérification est de veiller à ce que chaque personne soit correctement associée à ses propres données et à son historique d'accès, même si d'autres personnes portent le même nom.

des utilisateurs dans les systèmes DossiÉ et DEP, lorsqu'il s'agit d'une personne d'intérêt (par exemple, une personne ayant fait les manchettes) ou lorsqu'on soupçonne qu'un employé a pu accéder à des renseignements ou poser des gestes pouvant contrevenir aux dispositions de la LRMP. L'ORS peut également demander une vérification de l'activité des utilisateurs dans les autres systèmes, au besoin.

Le fonctionnaire chargé de la protection des renseignements médicaux de l'ORS tient à jour un tableau de toutes les vérifications liées à la protection de la vie privée dont il est informé. Il consigne également tous les incidents, réels ou soupçonnés, ainsi que les plaintes concernant des atteintes potentielles à la vie privée. Chaque entrée du registre contient un lien vers un dossier.

Le tableau permet de suivre trois types de vérifications : les vérifications de même nom, les vérifications spéciales (celles demandées lorsqu'il y a une préoccupation particulière concernant l'accès d'un employé) et les vérifications aléatoires des documents concernant l'activité des utilisateurs. Cependant, le tableau n'inclut pas les vérifications effectuées à d'autres fins, comme l'assurance de la qualité ni celles réalisées dans d'autres systèmes.

Analyse

Lorsque l'ORS a enquêté sur les atteintes à la vie privée concernant les renseignements médicaux personnels des personnes concernées, il a déterminé que les renseignements d'une de ces personnes avaient probablement été consultés dans le cadre d'une vérification de l'activité des utilisateurs effectuée par le fonctionnaire chargé de la protection des renseignements médicaux de l'établissement, et qu'un tel accès à des fins de vérification était autorisé. L'ORS n'a toutefois pas été en mesure de déterminer si l'accès aux renseignements médicaux personnels d'une autre personne faisait lui aussi partie d'une vérification.

Les politiques et procédures de l'ORS ne précisent pas les modalités du processus de vérification liées à la protection de la vie privée, comme l'exigent les lignes directrices établies par le règlement. Elles ne contiennent pas non plus d'exigence quant à la conservation des documents concernant ces vérifications.

Tenir un registre des vérifications de l'activité des utilisateurs aide les dépositaires à démontrer qu'ils respectent les exigences prévues par la LRMP, le règlement et les lignes

directrices. Même si la LRMP n'oblige pas les dépositaires à tenir un registre des vérifications effectuées à des fins d'assurance de la qualité, le fait d'en tenir un permettrait tout de même de démontrer que les renseignements médicaux personnels ont été consultés dans ce contexte. Cela aiderait ainsi le dépositaire à vérifier et à démontrer à la fois l'identité de la personne ayant accédé aux renseignements, ainsi que le motif et l'autorisation de cet accès, comme l'exige l'alinéa 18(2)b) de la LRMP.

L'alinéa 2(b) du règlement exige que les dépositaires adoptent des politiques et des procédures prévoyant la consignation des atteintes à la sécurité. Tenir un registre des atteintes soupçonnées permet aux dépositaires de répondre à cette exigence et de se conformer aux obligations prévues par la LRMP, notamment en ce qui concerne l'évaluation des risques associés à une atteinte à la vie privée, l'avis aux personnes concernées et le signalement des atteintes à notre bureau lorsqu'elles présentent un risque réel de préjudice grave pour la personne[4].

Le processus informel utilisé par le fonctionnaire chargé de la protection des renseignements médicaux de l'ORS pour faire le suivi des vérifications liées à la protection de la vie privée reçues de Soins communs | Santé numérique constitue un bon point de départ. Toutefois, en l'absence d'une politique ou d'une procédure écrite exigeant que ces vérifications soient consignées, bon nombre d'entre elles ne l'étaient pas au moment des atteintes. Les vérifications liées à l'assurance de la qualité, qui représentent une part importante de l'ensemble des vérifications effectuées par le dépositaire, ne font quant à elles l'objet d'aucun suivi.

L'absence de suivi et de documentation des vérifications liées à l'assurance de la qualité fait en sorte que, même si l'on croyait que les accès aux renseignements médicaux personnels des personnes concernées étaient liés à une vérification de ce type, aucune preuve directe ne permettait de confirmer que l'utilisation de leurs renseignements était bel et bien autorisée. L'ORS a conclu que les accès étaient autorisés en se fondant sur la période de l'année où ils ont eu lieu et sur l'absence de preuves indiquant qu'ils ne l'étaient pas.

[4] Comme mentionné plus haut, l'obligation d'aviser les personnes concernées et de signaler les atteintes à notre bureau a été ajoutée à la LRMP après le début de cette enquête, mais elle est maintenant en vigueur.

Cela n'est pas suffisant au regard des exigences de la LRMP. Certaines dispositions de la LRMP et du règlement exigent que les dépositaires adoptent des politiques et des procédures en matière de sécurité de l'information, et il leur incombe de s'assurer que les renseignements médicaux personnels ne sont utilisés que lorsqu'un tel usage est autorisé. Lorsqu'un dépositaire est incapable de déterminer si l'utilisation était autorisée, il ne doit pas présumer par défaut que l'accès ou l'utilisation l'était.

Ce genre de situation devrait inciter l'ORS à revoir ses politiques, ses procédures et ses formations, afin d'en corriger les lacunes et d'apporter les ajustements nécessaires, en particulier ceux qui lui permettraient de mieux établir, à l'avenir, si un accès était bel et bien autorisé.

Les citoyens ont le droit de savoir quand et comment leurs renseignements médicaux personnels sont utilisés, et les dépositaires doivent tout mettre en œuvre pour s'assurer de pouvoir fournir cette information aux personnes qui ont des questions ou des préoccupations concernant l'accès à leurs renseignements.

L'absence d'exigence visant à consigner ou à documenter les vérifications, ou tout autre accès à des renseignements médicaux personnels, dans les cas où il existe peu ou pas d'éléments permettant de justifier l'accès (contrairement aux notes médicales ou aux relevés de facturation, qui, eux, contiennent des éléments permettant de comprendre le contexte) empêche l'ORS de déterminer de façon satisfaisante si un accès était autorisé. Cela peut mener à une situation où, comme dans le présent cas, une personne perd confiance en la capacité de l'ORS de protéger sa vie privée et la sécurité de ses renseignements médicaux personnels.

Notre bureau conclut que l'ORS n'a pas pleinement respecté les exigences de la LRMP, du règlement et des lignes directrices, puisqu'il ne disposait ni d'une politique, ni d'un processus encadrant la réalisation des vérifications, ni d'un mécanisme pour documenter celles qu'il avait effectuées.

2. Non-respect de la politique de l'ORS en matière de confidentialité des renseignements médicaux personnels

Le fonctionnaire chargé de la protection des renseignements médicaux de l'établissement a accédé aux renseignements médicaux personnels d'une personne alors qu'il y avait un risque potentiel de conflit d'intérêts. L'ORS a jugé que cet accès était autorisé, car il avait eu lieu à une période où des vérifications sont généralement effectuées, et d'autres accès réalisés par ce fonctionnaire correspondaient au même type de vérifications. La capacité d'un organisme à reconnaître un conflit d'intérêts potentiel et à y réagir de manière appropriée a une incidence directe sur le niveau de confiance que les citoyens accordent à cet organisme.

C'est un aspect d'une importance cruciale pour les organismes de santé qui traitent des renseignements médicaux personnels. Plus l'information est sensible, plus les répercussions potentielles d'un conflit d'intérêts peuvent être importantes pour la personne concernée. Or, les renseignements médicaux personnels comptent parmi les plus sensibles qui soient.

Exigences législatives

La LRMP exige que les dépositaires mettent en place des mécanismes de contrôle précisant qui peut accéder aux renseignements médicaux personnels qu'ils détiennent :

> ***Garanties particulières***
> ***18(2)*** *Sans préjudice du paragraphe (1), le dépositaire :*
>
> *a) met en œuvre des dispositifs qui limitent le nombre de personnes qui peuvent utiliser les renseignements médicaux personnels qu'il maintient à celles qu'il autorise explicitement à cette fin;*
>
> *b) met en œuvre des dispositifs visant à garantir que les renseignements médicaux personnels qu'il maintient ne puissent être utilisés que si :*
>
> *(i) la personne qui cherche à les utiliser est bien l'une des personnes qu'il a autorisées à cette fin,*

(ii) l'utilisation projetée est effectivement autorisée sous le régime de la présente loi;

La LRMP exige également que les dépositaires limitent l'utilisation des renseignements médicaux personnels par leurs employés à la quantité minimale nécessaire pour atteindre un objectif autorisé par la LRMP :

> **Limite visant les employés du dépositaire**
> **20(3)** *Le dépositaire limite l'utilisation des renseignements médicaux personnels qu'il maintient à ceux de ses employés et mandataires qui doivent les connaître pour réaliser la fin à laquelle les renseignements ont été recueillis ou reçus ou une des fins qu'autorise l'article 21.*

Le règlement exige qu'un dépositaire détermine quels renseignements médicaux personnels chaque employé est autorisé à consulter :

> **Accès autorisé**
> **5** *Le dépositaire détermine les renseignements médicaux personnels auxquels chacun de ses employés et mandataires a accès.*

Les lignes directrices exigent aussi que les dépositaires disposent de politiques et de procédures qui garantissent le respect des exigences prévues par la LRMP.

Exigences des politiques de l'ORS

Le dépositaire a fourni une copie de sa politique sur la confidentialité des renseignements médicaux personnels, laquelle prévoit notamment ce qui suit :

- **Le personnel n'est pas autorisé à accéder à des renseignements confidentiels les concernant eux-mêmes, leur famille, leurs amis ou leurs collègues** *sans suivre les procédures d'accès à l'information établies dans la politique de Southern Health-Santé Sud.*

- **Le personnel qui***, dans l'exercice de ses fonctions,* **doit accéder à des renseignements confidentiels** *concernant* **un membre de sa famille, un ami ou un collègue doit :**

- **consulter son gestionnaire** *pour déterminer s'il est possible de confier la tâche à un autre membre du personnel;*

- **lorsque cela est requis et possible, obtenir le consentement verbal** *de la personne concernée avant de s'acquitter de ses tâches.*

C'est nous qui soulignons.

Analyse

Notre bureau n'a trouvé aucune preuve directe indiquant que l'accès aux renseignements médicaux personnels de la personne concernée faisait partie d'une vérification. Rien n'indique non plus que le fonctionnaire chargé de la protection des renseignements médicaux de l'établissement ait consulté son gestionnaire avant d'accéder aux renseignements, comme l'exige pourtant la politique.

L'ORS n'a pas non plus fourni d'information indiquant si le fonctionnaire chargé de la protection des renseignements médicaux de l'établissement avait discuté de la situation avec son gestionnaire (c'est-à-dire le fonctionnaire de l'office régional ou le directeur général), ou s'il avait obtenu le consentement de la personne concernée avant d'accéder à ses renseignements médicaux personnels. L'enquête menée par l'ORS ne précise pas non plus si les exigences de cette politique ont été prises en compte dans le cadre de sa décision.

La politique est claire : elle exige qu'un employé consulte son gestionnaire et obtienne le consentement de la personne concernée, lorsque cela est requis et possible, avant d'accéder aux renseignements médicaux personnels d'un membre de sa famille, d'un ami ou d'un collègue.

Les employés ne sont généralement pas autorisés à accéder aux renseignements médicaux personnels de leur famille, de leurs amis ou de leurs collègues en raison du risque de conflit d'intérêts, réel ou perçu. Consulter un gestionnaire et obtenir le consentement de la personne concernée sont des moyens de répondre aux préoccupations qu'un conflit d'intérêts perçu peut soulever.

En vertu de la LRMP, le droit d'un employé d'accéder à des renseignements médicaux personnels découle des responsabilités et fonctions que le dépositaire lui a attribuées.

Les dépositaires peuvent également restreindre davantage l'accès de chaque employé à ces renseignements au moyen de garanties techniques, administratives et physiques.

La LRMP et le règlement exigent que les dépositaires limitent l'accès de leurs employés aux seuls renseignements médicaux personnels nécessaires à l'exercice de leurs fonctions. Ces limites peuvent notamment prendre la forme de restrictions d'accès à certains types de renseignements ou à certains systèmes, réservés à des rôles ou à des personnes précises. Il s'agit alors d'une garantie technique. D'autres limites peuvent être établies par voie de politique (garantie administrative), comme l'interdiction d'accéder aux renseignements médicaux personnels de personnes connues de l'employé.

L'ORS limite l'accès de ses employés aux renseignements médicaux personnels lorsque ces renseignements concernent l'employé lui-même, un membre de sa famille, un ami ou un collègue, à moins que certaines étapes précises ne soient respectées. Tout accès effectué sans avoir suivi les étapes requises n'est pas autorisé par le dépositaire – et tout accès non autorisé par le dépositaire ne l'est pas non plus en vertu de la LRMP.

Si le fonctionnaire chargé de la protection des renseignements médicaux de l'établissement effectuait une vérification autorisée au moment d'accéder aux renseignements médicaux personnels de la personne concernée, il aurait dû consulter son gestionnaire ou obtenir le consentement de la personne, comme il se doit. Conformément à la politique de l'ORS, le fait de ne pas avoir suivi l'une ou l'autre de ces étapes signifie que cet accès n'était pas autorisé.

Comme rien n'indique que l'une ou l'autre de ces étapes a été suivie par le fonctionnaire chargé de la protection des renseignements médicaux de l'établissement, l'accès aux renseignements médicaux personnels de la personne concernée n'était pas autorisé. Notre bureau conclut donc qu'il y a eu atteinte à la vie privée.

Notre bureau conclut également que l'ORS n'a pas respecté sa propre politique en matière d'utilisation des renseignements médicaux personnels. Il s'agit, en fin de compte, d'un manquement aux exigences prévues par la LRMP et le règlement, qui obligent les dépositaires à veiller à ce que ces renseignements ne soient utilisés que de façon autorisée, et uniquement par les personnes qui ont besoin de les connaître.

3. Manque de communication entre les différents rôles et secteurs au sein de l'ORS

Dans le cas d'une des personnes concernées, l'ORS était au courant de tensions dans la relation entre cette personne et le fonctionnaire chargé de la protection des renseignements médicaux de l'établissement, ainsi que de la plainte déposée par cette personne. Idéalement, une plainte visant un employé dont le rôle (à la fois comme fonctionnaire responsable de la protection des renseignements médicaux et comme gestionnaire de l'information) lui donne un accès accru à ces renseignements aurait dû amener l'office à soulever des préoccupations quant à la protection de la vie privée.

Toutefois, dans ce cas, le risque potentiel pour la vie privée n'a pas été relevé, et le fonctionnaire chargé de la protection des renseignements médicaux de l'ORS n'a pas été informé de la plainte. L'absence de reconnaissance du risque a entraîné un manque de communication entre les différentes fonctions au sein de l'office. Par conséquent, le fonctionnaire chargé de la protection des renseignements médicaux de l'ORS n'a pas été en mesure d'évaluer adéquatement la légitimité de l'accès du fonctionnaire de l'établissement aux renseignements médicaux personnels des personnes concernées ni les motivations possibles derrière cet accès, dans le cadre de son enquête.

Exigences législatives

La LRMP exige que les dépositaires protègent les renseignements médicaux personnels en mettant en place des garanties administratives, techniques et physiques :

> ***Obligation d'établir des garanties***
>
> ***18(1)*** *En conformité avec les exigences réglementaires, le dépositaire protège les renseignements médicaux personnels en établissant des garanties administratives, techniques et physiques satisfaisantes afin que soient assurées la confidentialité, la sécurité, l'exactitude et l'intégrité des renseignements.*

Ces garanties comprennent notamment le fait de s'assurer que tous les employés du dépositaire reçoivent une formation adéquate pour savoir à quels renseignements ils peuvent accéder, dans quelles circonstances, et comment reconnaître un accès non autorisé ou un risque potentiel d'atteinte à la sécurité des renseignements.

Le règlement exige que les dépositaires offrent une formation à leurs employés :

Orientation et formation des employés

6 *Le dépositaire donne des sessions d'orientation et une formation continue à ses employés et à ses mandataires au sujet des directives que vise l'article 2.*

Exigences des politiques de l'ORS

La politique de l'ORS sur la déclaration et l'enquête en cas d'atteinte à la vie privée ou de plainte prévoit les exigences suivantes :

> *Les ressources appropriées, notamment les ressources humaines, le spécialiste de la protection de la vie privée et de l'accès à l'information, ou encore les services de qualité, sécurité des patients et accréditation, doivent être consultées avant de rencontrer un membre du personnel lorsqu'une mesure éducative ou corrective pourrait être nécessaire.*
>
> *Si l'on détermine qu'une atteinte à la vie privée a eu lieu, le gestionnaire doit consulter les Ressources humaines ainsi que le spécialiste de la protection de la vie privée et de l'accès à l'information afin de déterminer le niveau approprié de formation ou des mesures correctives à appliquer.*

La politique sur la confidentialité des renseignements médicaux personnels exige que tous les employés de l'ORS protègent les renseignements confidentiels, y compris les renseignements médicaux personnels. Cette politique comprend notamment les exigences suivantes :

- *Le personnel est tenu de protéger les renseignements confidentiels, comme indiqué ci-dessous, et comprend que cette obligation demeure même après la fin de son emploi, de son contrat, de son lien d'association ou de sa nomination au sein de Southern Health-Santé Sud.*
- *Tous les employés et toutes les personnes associées au dépositaire sont responsables de la protection de tous les renseignements médicaux personnels, y compris les renseignements démographiques (qu'ils soient oraux ou consignés sous quelque forme que ce soit) obtenus, traités, entendus, appris ou consultés dans le cadre de leur travail ou de leur lien avec le dépositaire.*

- *Le personnel a la responsabilité légale, professionnelle et éthique de protéger tous les renseignements confidentiels, qu'ils soient oraux ou consignés sous quelque forme que ce soit, obtenus, traités, entendus, appris ou consultés dans le cadre de son travail ou de son lien avec Southern Health-Santé Sud.*

Analyse

La LRMP exige que tous les employés d'un dépositaire soient au courant des exigences qu'elle prévoit. Pour que son application soit réellement efficace, les employés doivent comprendre dans quelles circonstances ils sont autorisés à accéder à des renseignements médicaux personnels, et dans quelles circonstances ils ne le sont pas. Ils doivent aussi être en mesure de reconnaître les risques potentiels pour la vie privée qui peuvent découler de leurs fonctions, y compris lorsqu'ils supervisent le travail d'autres personnes.

La politique de l'ORS exige que les différents secteurs de programme soient informés des enquêtes et des résultats liés aux atteintes à la vie privée, et qu'ils y participent. Toutefois, cette communication devrait aller dans les deux sens : les secteurs de programme devraient également être tenus d'aviser le fonctionnaire chargé de la protection des renseignements médicaux dès qu'un risque pour la vie privée est identifié ou survient.

Dans cette situation, une plainte précise visait un employé ayant accès à une quantité importante de renseignements personnels. Compte tenu du poste occupé par cet employé et de la nature de la plainte, le personnel de l'ORS aurait dû reconnaître les risques potentiels pour la vie privée et consulter le fonctionnaire chargé de la protection des renseignements médicaux de l'office.

Si le fonctionnaire chargé de la protection des renseignements médicaux de l'ORS avait été informé de la plainte, cela aurait pu modifier l'issue de l'enquête de l'office sur l'accès aux renseignements médicaux personnels des personnes concernées, et inciter l'organisation à mettre en place des mesures pour prévenir tout accès futur à ces renseignements par le fonctionnaire de l'établissement.

Notre bureau conclut que l'ORS n'a pas respecté la LRMP ni son règlement en ne reconnaissant pas le risque potentiel pour la sécurité des renseignements médicaux

personnels, et en ne fournissant pas à ses employés une formation suffisante leur permettant d'identifier ce type de risque

4. Traitement des plaintes liées aux atteintes à la vie privée par l'ORS

La LRMP interdit aux dépositaires et à leurs employés d'utiliser ou de communiquer des renseignements médicaux personnels, sauf dans les cas prévus, et exige qu'ils se limitent à la quantité minimale nécessaire pour atteindre l'objectif.

L'article 18 de la LRMP oblige les dépositaires à mettre en place des garanties pour protéger les renseignements médicaux personnels, tandis que l'article 20 stipule que le dépositaire « ne peut utiliser ou communiquer des renseignements médicaux personnels que dans la mesure prévue ».

L'emploi du terme « ne peut... que » dans la LRMP traduit une interdiction claire, qui établit une obligation stricte à laquelle les dépositaires doivent se conformer. La LRMP n'impose aucune exigence de ce type aux particuliers.

Faire reposer sur la personne concernée le fardeau de prouver qu'un renseignement médical personnel a été utilisé sans autorisation peut également nuire à la confiance qu'elle accorde au dépositaire, ainsi qu'au système de santé dans son ensemble et à sa capacité de protéger ses renseignements.

Les dépositaires ont la responsabilité de s'assurer que les renseignements médicaux personnels sont utilisés conformément à la LRMP, et c'est à eux que revient le fardeau de démontrer que l'utilisation était autorisée. Ce fardeau ne devrait pas incomber à la personne dont les droits ont potentiellement été atteints.

Exigences législatives

Obligation d'établir des garanties

18(1) *En conformité avec les exigences réglementaires, le dépositaire protège les renseignements médicaux personnels en établissant des garanties administratives, techniques et physiques satisfaisantes afin que soient assurées la confidentialité, la sécurité, l'exactitude et l'intégrité des renseignements.*

Obligations générales des dépositaires

20(1) *Le dépositaire ne peut utiliser ou communiquer des renseignements médicaux personnels que dans la mesure prévue dans la présente section.*

Nombre de renseignements

20(2) *L'utilisation ou la communication par un dépositaire de renseignements médicaux personnels se limite au nombre minimal de renseignements nécessaires à la réalisation de la fin à laquelle ils sont destinés.*

Limite visant les employés du dépositaire

20(3) *Le dépositaire limite l'utilisation des renseignements médicaux personnels qu'il maintient à ceux de ses employés et mandataires qui doivent les connaître pour réaliser la fin à laquelle les renseignements ont été recueillis ou reçus ou une des fins qu'autorise l'article 21.*

Renseignements fournis par l'ORS

L'ORS a indiqué avoir enquêté sur les atteintes présumées à la vie privée liées aux renseignements médicaux personnels des personnes concernées. Dans le cas d'une de ces personnes, l'office n'a trouvé aucun élément indiquant que les accès étaient non autorisés. Il a conclu que l'accès aux renseignements médicaux personnels de cette personne avait eu lieu à une période de l'année où une vérification liée à l'assurance de la qualité est habituellement effectuée, et que les renseignements d'autres personnes avaient également été consultés.

L'ORS n'a trouvé aucun élément permettant de confirmer ou d'infirmer l'autorisation de l'accès dans le cas de la deuxième personne. L'accès aux renseignements médicaux personnels de cette personne ne s'est pas produit à une période particulière de l'année, n'a pas coïncidé avec l'accès aux renseignements d'autres personnes, et rien n'indiquait qu'une vérification aléatoire était en cours.

L'ORS a conclu que l'accès aux renseignements médicaux personnels des deux personnes concernées était autorisé. Il a précisé que cette décision reposait sur l'idée que, en l'absence de preuve directe d'un accès non autorisé ou d'un comportement fautif (comme un aveu du fonctionnaire de l'établissement), l'accès devait être considéré comme autorisé.

Analyse

Lorsqu'aucune information n'est disponible quant au motif de l'accès, les dépositaires ne doivent pas présumer par défaut que l'accès ou l'utilisation était autorisé. Le paragraphe 20(1) de la LRMP stipule qu'un dépositaire « *ne peut utiliser ou communiquer des renseignements médicaux personnels que dans la mesure prévue* », et les articles 21 à 24 énumèrent précisément les situations dans lesquelles un dépositaire est autorisé à utiliser (art. 21) ou à communiquer (art. 22, 23 et 24) de tels renseignements. Toute utilisation ou divulgation qui ne figure pas dans ces articles n'est pas autorisée en vertu de la LRMP.

Il revient aux dépositaires de démontrer que leur accès à des renseignements médicaux personnels est autorisé en vertu de la LRMP. Or, lorsque le fonctionnaire chargé de la protection des renseignements médicaux de l'ORS a examiné les plaintes liées aux atteintes à la vie privée, le fardeau de la preuve a été placé sur les personnes concernées. Autrement dit, on a présumé que l'accès était autorisé, à moins que ces personnes ne soient en mesure de démontrer le contraire.

Notre bureau a expliqué à l'ORS que cette façon de déterminer si un accès était autorisé en vertu de la LRMP n'était pas appropriée. Le fonctionnaire chargé de la protection des renseignements médicaux de l'office a indiqué avoir compris et s'est engagé à modifier sa façon de traiter les atteintes à la vie privée à l'avenir.

Notre bureau a conclu que l'utilisation des renseignements médicaux personnels d'une des personnes concernées n'était pas autorisée, car le fonctionnaire de l'établissement n'a pas respecté les exigences de la politique de l'ORS applicables dans le cadre d'un accès réellement justifié par des raisons professionnelles.

Le fonctionnaire de l'établissement n'a pas obtenu le consentement de la personne avant d'utiliser ses renseignements, et rien n'indique qu'il ait rencontré son gestionnaire pour discuter du conflit d'intérêts potentiel, comme l'exige pourtant la politique de l'office.

Il n'existe par ailleurs aucune preuve directe indiquant que l'accès avait été effectué à des fins autorisées. Le seul élément laissant croire qu'il aurait pu s'inscrire dans le cadre d'une vérification est le moment de l'année où il a eu lieu, ainsi que l'accès aux renseignements médicaux personnels d'autres personnes pendant la même période.

Notre bureau a conclu que l'accès aux renseignements médicaux personnels de l'autre personne concernée n'était pas autorisé, puisqu'aucun élément ne permettait de déterminer la raison de cet accès. Aucun indice contextuel ne laissait non plus croire qu'il aurait pu s'inscrire dans le cadre d'une vérification ou d'un autre motif légitime.

La LRMP exige que les dépositaires veillent à ce que leurs employés n'accèdent aux renseignements médicaux personnels que lorsqu'ils ont un motif autorisé. Cela signifie qu'un dépositaire doit connaître la raison pour laquelle un employé accède à ces renseignements. Il revient au dépositaire de s'assurer que l'accès ou l'utilisation par ses employés est autorisé et que seule la quantité minimale d'information nécessaire à cette fin est consultée ou utilisée.

Lorsqu'il est impossible de déterminer si un accès était autorisé, le dépositaire devrait revoir ses politiques, ses directives, l'attribution des droits d'accès des utilisateurs, la formation offerte ainsi que tout autre élément pertinent. L'objectif est de s'assurer que les employés comprennent clairement ce qui constitue un accès autorisé dans le cadre de leurs fonctions, et d'identifier les ajustements nécessaires pour faciliter l'identification des accès autorisés à l'avenir.

La LRMP exige également que les dépositaires mettent en place des garanties administratives raisonnables, ce qui comprend notamment l'enquête sur les atteintes à la vie privée et l'identification adéquate des risques en matière de confidentialité. Lorsqu'un dépositaire transfère le fardeau de la preuve à la personne plaignante dans le cadre d'une enquête sur une atteinte à la vie privée, il devient incapable de repérer les risques potentiels pour la confidentialité engendrés par les gestes de ses employés ou par ses propres politiques et procédures.

Notre bureau conclut que l'ORS n'a pas respecté l'obligation qui lui incombe en vertu de l'article 20, en tirant des conclusions qui ne respectent pas les exigences de la LRMP et en plaçant sur les plaignants le fardeau de prouver qu'il y avait eu atteinte à la vie privée. Par conséquent, l'office a commis une erreur en concluant que l'utilisation des renseignements médicaux personnels des personnes concernées était autorisée.

Notre bureau conclut également que l'ORS n'a pas mené une enquête suffisante sur les plaintes liées aux atteintes à la vie privée et n'a donc pas été en mesure d'identifier les lacunes dans son processus ni les garanties administratives supplémentaires à mettre en place, comme l'exige l'article 18 de la LRMP.

5. Absence de documentation sur l'utilisation des renseignements médicaux personnels

La LRMP exige que les dépositaires limitent la collecte, l'utilisation et la divulgation des renseignements médicaux personnels à la quantité minimale nécessaire pour atteindre un objectif autorisé, et il leur incombe de veiller au respect de cette exigence. Les personnes concernées ont le droit d'accéder à leurs propres renseignements médicaux personnels. Cela inclut le droit de savoir qui y a accédé et dans quel but.

Le droit d'accès n'a de véritable portée que s'il est exercé sans délai, de façon transparente, exacte et complète. Si un dépositaire est incapable d'expliquer à une personne qui a accédé à ses renseignements médicaux personnels ou pour quel motif, il ne respecte pas les exigences prévues par la LRMP.

Un dépositaire ne peut s'acquitter de ses responsabilités en matière de sécurité des renseignements médicaux personnels, de limitation de leur collecte, de leur utilisation et de leur divulgation, ni offrir un accès pertinent à l'information aux personnes concernées, s'il ne consigne pas qui a accédé aux renseignements, à quel moment, à quelles données, pour quel motif et de quelle manière. La façon de démontrer qu'un accès est autorisé peut varier selon le rôle de l'employé, mais une forme de documentation doit toujours être en place.

Comme nous l'avons mentionné tout au long du présent rapport, lorsqu'un dépositaire ne respecte pas les exigences de la LRMP, n'offre pas un accès pertinent aux renseignements médicaux personnels et ne protège pas les droits des personnes en matière de vie privée, cela mine la confiance que les citoyens accordent au système de santé et à sa capacité de protéger leurs renseignements.

Exigences législatives

Le préambule de la LRMP énonce les principes fondamentaux sur lesquels reposent ses exigences :

> *ATTENDU QUE les renseignements médicaux sont personnels et de nature délicate et que leur confidentialité doit être préservée afin que les particuliers ne craignent pas de demander des soins de santé ni de divulguer des renseignements de nature délicate aux professionnels de la santé;*

ATTENDU QUE les particuliers doivent en toute justice avoir accès à leurs propres renseignements médicaux afin de pouvoir prendre des décisions éclairées en matière de soins de santé et de faire corriger les renseignements les concernant qui sont inexacts ou incomplets;

ATTENDU QU'IL est nécessaire d'agir de façon uniforme en ce qui a trait aux renseignements médicaux personnels étant donné que de nombreuses personnes autres que les professionnels de la santé obtiennent, utilisent et communiquent à l'heure actuelle ces renseignements dans des contextes différents et à des fins diverses;

ATTENDU QUE l'établissement de règles claires et certaines touchant la collecte, l'utilisation et la communication des renseignements médicaux personnels constitue un soutien essentiel aux systèmes d'information électroniques en matière de santé, lesquels systèmes peuvent améliorer tant la qualité des soins donnés aux patients que la gestion des ressources dans le domaine des soins de santé;

Plusieurs articles de la LRMP exigent que les dépositaires donnent aux personnes concernées accès à leurs propres renseignements médicaux personnels, qu'ils en assurent la sécurité et qu'ils en limitent la collecte, l'utilisation et la divulgation.

Droit d'examiner et de reproduire les renseignements

5(1) *Sous réserve des autres dispositions de la présente loi, tout particulier a le droit, sur demande, d'examiner les renseignements médicaux personnels le concernant que maintient un dépositaire et d'en recevoir copie.*

Obligation de prêter assistance au particulier

6(2) *Le dépositaire fait tous les efforts possibles pour prêter assistance au particulier qui présente une demande et pour lui répondre sans délai de façon ouverte, précise et complète.*

Restrictions applicables à la collecte

13(1) *Le dépositaire ne peut recueillir des renseignements médicaux personnels concernant un particulier que si :*

a) d'une part, il les recueille à une fin licite liée à une de ses fonctions ou activités;

b) d'autre part, la collecte des renseignements est nécessaire à cette fin.

Nombre de renseignements

13(2) *Le dépositaire ne peut recueillir que le nombre de renseignements nécessaires à la réalisation de la fin visée.*

Obligations générales des dépositaires

20(1) *Le dépositaire ne peut utiliser ou communiquer des renseignements médicaux personnels que dans la mesure prévue dans la présente section.*

Nombre de renseignements

20(2) *L'utilisation ou la communication par un dépositaire de renseignements médicaux personnels se limite au nombre minimal de renseignements nécessaires à la réalisation de la fin à laquelle ils sont destinés.*

Limite visant les employés du dépositaire

20(3) *Le dépositaire limite l'utilisation des renseignements médicaux personnels qu'il maintient à ceux de ses employés et mandataires qui doivent les connaître pour réaliser la fin à laquelle les renseignements ont été recueillis ou reçus ou une des fins qu'autorise l'article 21.*

Analyse

Notre bureau a constaté que la plupart des accès aux renseignements médicaux personnels par les employés de l'ORS ne font l'objet d'aucune documentation, et qu'il existe peu d'exigences claires les obligeant à consigner le moment et le motif de ces accès. Nous reconnaissons toutefois que certaines situations ne nécessitent pas la création d'une documentation distincte.

Par exemple, lorsque des professionnels de la santé accèdent à des renseignements médicaux personnels dans le cadre du traitement d'un patient, ils rédigent généralement des notes qui documentent leur évaluation et les soins prodigués. La preuve du motif de cet accès est donc disponible pour consultation et facile à justifier. Il n'est donc pas nécessaire de créer une documentation supplémentaire à ce sujet.

De même, lorsque des employés émettent des factures ou que des pharmaciens remplissent des ordonnances, ces types d'accès génèrent d'autres documents qui

indiquent clairement la raison de l'accès et ces documents sont souvent joints au dossier médical du patient ou y font référence.

Lorsqu'un accès à des renseignements médicaux personnels est justifié, il devrait exister une trace documentée du motif de cet accès. Dans la majorité des cas, cette information se trouvera dans le dossier du patient. Cependant, si le motif de l'accès ne permet pas que la documentation soit conservée dans ce dossier, elle doit tout de même être consignée et conservée de manière à pouvoir être consultée.

Parmi les situations où cela est nécessaire, on peut penser à l'accès à des renseignements médicaux personnels à des fins de recherche, pour transmettre des renseignements démographiques à Santé Manitoba, pour offrir de la formation aux employés du dépositaire ou dans le cadre d'une vérification effectuée par le dépositaire.

Un fonctionnaire chargé de la protection des renseignements médicaux qui effectue une vérification devrait conserver des copies des vérifications réalisées, tenir une liste des dossiers consultés, expliquer le but de la vérification et préciser quels renseignements ont été examinés et pourquoi ils étaient nécessaires pour atteindre cet objectif.

Notre enquête n'a révélé aucun élément permettant d'établir le motif pour lequel le fonctionnaire de l'établissement a accédé aux renseignements médicaux personnels de l'une des personnes concernées. Cet accès allait à l'encontre de la politique en vigueur, puisque le fonctionnaire n'a pas consulté son gestionnaire. Rien n'avait été consigné concernant le motif de l'accès, l'étendue des renseignements consultés ou si l'ORS avait autorisé ou non cet accès.

Notre bureau reconnaît qu'il peut être difficile (voire impossible, dans certains cas) de documenter chaque utilisation de renseignements médicaux personnels. Toutefois, les dépositaires doivent être en mesure d'expliquer pourquoi une information a été consultée, afin de respecter leurs obligations en vertu de la LRMP. Ils devraient aussi redoubler de vigilance et d'efforts dans les situations où le risque d'atteinte à la vie privée est accru, par exemple lorsqu'un employé est aussi patient du dépositaire. L'absence de documentation dans des cas où celle-ci devrait normalement exister constitue un élément à prendre en compte lors de l'examen d'une plainte en matière de vie privée.

Documenter la collecte, l'utilisation et la divulgation des renseignements médicaux personnels permet aux dépositaires de s'assurer qu'ils respectent leurs obligations en vertu de la LRMP. La tenue de cette documentation leur permet également d'examiner de manière rigoureuse les accès de leurs employés aux renseignements médicaux personnels et de repérer tout problème éventuel.

Lorsque les dépositaires fournissent aux personnes concernées de l'information claire et pertinente sur l'accès à leurs renseignements médicaux personnels, cela renforce la confiance envers le système de santé et permet d'éviter que certaines personnes renoncent à consulter par souci de protéger leur vie privée.

Notre bureau conclut également que l'ORS n'a pas respecté les exigences de la LRMP, en ne documentant pas les accès aux renseignements médicaux personnels ni en fournissant suffisamment d'information sur l'autorisation et le motif de ces accès, ou d'assurance que la quantité minimale de renseignements avait été consultée.

6. Des employés demandent au fonctionnaire de l'établissement (et possiblement à d'autres) d'accéder aux renseignements médicaux personnels à leur place

L'un des motifs avancés par l'office régional de la santé pour expliquer l'accès du fonctionnaire de l'établissement aux renseignements médicaux personnels des personnes concernées est que certains employés communiquaient avec les responsables de la protection des renseignements médicaux pour leur demander de consulter des dossiers de patients auxquels ils n'avaient pas accès, ou auxquels ils ne savaient pas comment accéder.

Exigences législatives

La LRMP exige que les dépositaires mettent en place des garanties afin de protéger les renseignements médicaux personnels et de limiter l'accès de leurs employés à ce qui est strictement nécessaire.

> ***Obligation d'établir des garanties***
>
> ***18(1)*** *En conformité avec les exigences réglementaires, le dépositaire protège les renseignements médicaux personnels en établissant des garanties administratives, techniques et physiques satisfaisantes afin que soient*

assurées la confidentialité, la sécurité, l'exactitude et l'intégrité des renseignements.

Garanties particulières
18(2) *Sans préjudice du paragraphe (1), le dépositaire :*

a) met en œuvre des dispositifs qui limitent le nombre de personnes qui peuvent utiliser les renseignements médicaux personnels qu'il maintient à celles qu'il autorise explicitement à cette fin;

b) met en œuvre des dispositifs visant à garantir que les renseignements médicaux personnels qu'il maintient ne puissent être utilisés que si :

(i) la personne qui cherche à les utiliser est bien l'une des personnes qu'il a autorisées à cette fin,

(ii) l'utilisation projetée est effectivement autorisée sous le régime de la présente loi;

c) met en œuvre des mesures visant à empêcher l'interception de renseignements médicaux personnels par des personnes non autorisées, s'il utilise des moyens électroniques pour demander la communication de tels renseignements ou pour répondre à des demandes de communication;

d) veille à ce que les demandes de communication de renseignements médicaux personnels auxquelles il répond contiennent suffisamment de détails pour identifier uniquement le particulier que les renseignements concernent.

Le règlement prévoit notamment ce qui suit :

Restriction d'accès et autres précautions
3 *Le dépositaire :*

a) veille à ce que les renseignements médicaux personnels soient conservés dans un ou plusieurs endroits désignés et fassent l'objet de garanties appropriées;

b) limite l'accès physique aux endroits désignés contenant des renseignements médicaux personnels aux seules personnes autorisées;

c) prend des précautions raisonnables pour protéger les renseignements médicaux personnels contre les incendies, le vol, le vandalisme, la détérioration, la destruction accidentelle, la perte et tout autre danger;

d) veille à ce que les supports amovibles servant à consigner des renseignements médicaux personnels soient entreposés de manière sécuritaire lorsqu'ils ne sont pas utilisés.

Accès autorisé

5 *Le dépositaire détermine les renseignements médicaux personnels auxquels chacun de ses employés et mandataires a accès.*

Orientation et formation des employés

6 *Le dépositaire donne des sessions d'orientation et une formation continue à ses employés et à ses mandataires au sujet des directives que vise l'article 2.*

Renseignements fournis par l'ORS

L'ORS a indiqué que, dans certains cas, des employés travaillant dans de plus petites cliniques ou ayant un accès limité aux renseignements médicaux personnels dans les systèmes de l'office communiquaient avec le fonctionnaire de l'établissement (qui agissait aussi à titre de gestionnaire de l'information pour l'établissement) afin de lui demander d'accéder aux renseignements médicaux personnels de patients en leur nom.

Des discussions plus approfondies ont révélé que cette pratique informelle découlait en grande partie d'un manque de connaissances techniques chez certains employés, qui ignoraient soit qu'ils pouvaient accéder à un système donné, soit où trouver certaines informations dans ce système.

Analyse

Lorsqu'un employé demande à un collègue de consulter des renseignements à sa place, cela soulève plusieurs enjeux potentiels. D'abord, si un employé n'a pas accès aux renseignements médicaux personnels dont il a besoin pour accomplir ses tâches, cette lacune devrait être portée à l'attention de l'ORS.

Cela permet à l'ORS de s'assurer que les employés ont un accès direct à l'information dont ils ont besoin pour accomplir leur travail, ou de leur offrir des indications afin qu'ils sachent où et comment trouver cette information.

Ensuite, si un employé n'a pas besoin de cette information pour accomplir ses tâches, les autres employés qui y ont accès ne devraient pas la lui transmettre, car cela contourne les garanties mises en place par le dépositaire pour protéger les renseignements médicaux personnels.

La LRMP et son règlement exigent des dépositaires qu'ils limitent non seulement les renseignements médicaux personnels qu'ils recueillent et utilisent à des fins autorisées, mais aussi les renseignements auxquels chaque employé est autorisé à accéder. Les dépositaires doivent mettre en place des processus pour prendre ces décisions et mettre à jour les droits d'accès des employés au besoin. Par exemple, le personnel infirmier ne devrait pas avoir les mêmes privilèges d'accès qu'un commis administratif, et ces privilèges doivent être réévalués chaque fois qu'un employé change de rôle au sein de l'organisation.

Les situations où un employé n'a pas accès aux renseignements médicaux personnels nécessaires à l'exécution de ses tâches et doit demander à un collègue d'y accéder à sa place devraient être extrêmement rares et faire l'objet d'une documentation claire précisant les raisons pour lesquelles cet accès est requis.

Le manque de formation des employés sur la façon d'accéder à certains renseignements et sur l'endroit où les trouver dans les différents systèmes de l'ORS a donné lieu à des situations où des employés, ayant un motif autorisé pour consulter l'information et disposant à leur insu des privilèges d'accès nécessaires, demandaient à un fonctionnaire chargé de la protection des renseignements médicaux de le faire à leur place. Cela pose problème, car le fonctionnaire chargé de la protection des renseignements médicaux se

retrouve alors à accéder à des renseignements médicaux personnels pour un motif qui dépasse le cadre de ses fonctions.

Un fonctionnaire chargé de l'accès à l'information et de la protection des renseignements personnels n'a pas du tout le même motif d'accès à des renseignements médicaux personnels qu'une infirmière. L'ORS autorise les accès en fonction de ces motifs, et met en place des garanties ainsi que des privilèges d'accès afin d'assurer une surveillance efficace et une application conforme des autorisations d'accès.

L'accès aux renseignements médicaux personnels de cette manière est, à première vue, contraire aux garanties mises en place par l'ORS. Ces garanties ont précisément pour but de permettre le suivi de qui accède aux renseignements, à quel moment et pour quel motif.

Ce manque de formation des employés a également mené à des situations où ceux-ci demandaient au fonctionnaire de l'établissement d'accéder à l'information à leur place. Dans ces cas, l'employé qui faisait la demande pouvait avoir l'autorisation d'accéder aux renseignements médicaux personnels, mais ce n'était pas le cas du fonctionnaire de l'établissement.

De plus, puisque l'accès a été effectué par le fonctionnaire de l'établissement et qu'il n'a pas été documenté, il est impossible de déterminer si l'employé ayant fait la demande était autorisé à consulter les renseignements médicaux personnels ni quel était le motif de l'accès.

La LRMP exige que les dépositaires offrent à leurs employés une formation continue sur leurs politiques et procédures. Cela doit inclure une formation régulière et à jour sur l'utilisation des divers systèmes nécessaires à l'accomplissement de leurs tâches.

Sans une formation adéquate sur les systèmes électroniques utilisés par l'ORS, les politiques et procédures liées à la sécurité de l'information dans ces systèmes ont peu d'utilité concrète. Si les employés ne comprennent pas le fonctionnement des systèmes, ils ne peuvent pas appliquer correctement les politiques et les procédures.

Notre bureau conclut que l'ORS n'a pas respecté son obligation de mettre en place des garanties administratives raisonnables.

Plus précisément :

- La formation offerte par l'ORS à ses employés était insuffisante, puisque ceux-ci ne possédaient pas les connaissances nécessaires pour repérer l'information dont ils avaient besoin tout en limitant leur accès aux renseignements non essentiels.

- Les politiques de l'ORS n'invitent pas les employés à signaler à leur supérieur les problèmes liés à leurs privilèges d'accès aux systèmes.

- L'ORS n'exige pas que les personnes disposant de privilèges d'accès documentent les moments où elles consultent ou partagent des renseignements médicaux personnels à des fins autorisées avec des collègues ayant des privilèges d'accès moindres.

7. Aucun mécanisme de surveillance des personnes responsables des vérifications

Les lignes directrices du ministre de la Santé en lien avec les documents concernant l'activité des utilisateurs exigent que les dépositaires mettent en place un processus de surveillance des employés chargés d'effectuer les vérifications. Autrement dit, les personnes responsables de vérifier l'utilisation des renseignements médicaux personnels doivent elles aussi faire l'objet de contrôles ciblés afin d'assurer que leur accès à ces renseignements est conforme à leur rôle et à leur autorisation.

Les vérifications ciblées des personnes chargées de surveiller les accès peuvent aider à détecter et à prévenir l'utilisation non autorisée des renseignements médicaux personnels. Dans le présent cas, l'ORS n'avait mis en place aucune politique ni procédure pour vérifier si les actions du fonctionnaire de l'établissement étaient autorisées. Aucun mécanisme ne permettait de surveiller les personnes responsables des vérifications.

Comme il est indiqué dans l'introduction du présent rapport, il s'agit d'une grave atteinte à la confiance lorsque l'employé chargé d'assurer la protection de la vie privée et de la sécurité des renseignements médicaux personnels est lui-même l'auteur de l'atteinte à cette vie privée.

Pour maintenir la confiance des citoyens envers la sécurité de leurs renseignements médicaux personnels et envers l'ensemble du système de santé, les dépositaires doivent

mettre en place des mesures cohérentes, rigoureuses et raisonnables afin d'assurer que tout employé ayant accès à ces renseignements les utilise de façon autorisée.

Ces mesures doivent inclure l'examen de tous les accès aux renseignements médicaux personnels effectués par les employés chargés de vérifier les accès des autres employés et de faire la vérification des systèmes contenant ces renseignements.

Exigences législatives

Le règlement exige que les dépositaires créent et conservent des documents concernant l'activité des utilisateurs, conformément aux lignes directrices établies par le ministre de la Santé.

> ***Protection supplémentaire des systèmes d'information électronique en matière de santé***
>
> ***4(1)*** *Conformément aux directives du ministre, le dépositaire établit et conserve ou fait établir et conserver un document concernant l'activité des utilisateurs pour tout système d'information électronique qu'il utilise afin de maintenir des renseignements médicaux personnels.*

L'article 9 des lignes directrices du ministre de la Santé sur les documents concernant l'activité des utilisateurs prévoit l'obligation, pour les dépositaires, de mettre en place un mécanisme de surveillance des vérificateurs.

> ***9. Surveillance des vérificateurs***
>
> *Les dépositaires doivent établir un processus de vérification périodique des activités des administrateurs de système.*

Renseignements fournis par l'ORS

Le dépositaire a indiqué que les responsabilités du fonctionnaire de l'établissement comprenaient différents types de vérifications, notamment des vérifications liées à la protection de la vie privée et des vérifications d'assurance de la qualité, ainsi que le traitement des questions liées à la LRMP, comme les plaintes. Le fonctionnaire de l'établissement accomplissait également des tâches qui ne faisaient pas officiellement partie de son rôle, notamment accéder aux systèmes pour transmettre des renseignements médicaux personnels à des employés qui n'y avaient pas accès ou qui ne savaient pas où trouver l'information.

L'établissement et l'ORS n'ont mis en place aucun système officiel pour assurer le suivi de ces responsabilités. L'office n'a donc aucun moyen de savoir quand ces activités ont lieu ni quels dossiers sont consultés dans ce contexte.

Le fonctionnaire chargé de la protection des renseignements médicaux de l'ORS a commencé à assurer le suivi des vérifications effectuées par les responsables de la protection de la vie privée dans divers hôpitaux et cliniques relevant de l'office. Cependant, aucun processus officiel n'a été mis en place à cet égard, et il n'existe aucune directive précisant les étapes à suivre, la fréquence des vérifications, les personnes à auditer ou les personnes responsables de les effectuer.

Analyse

De façon générale, la question de savoir si un accès est autorisé repose en grande partie sur des éléments de preuve à l'appui. Cela fonctionne bien pour certains postes, notamment ceux liés aux soins directs aux patients (personnel infirmier, médecins, aides en soins de santé, etc.), puisque les accès autorisés sont généralement appuyés par des dossiers médicaux créés par le personnel soignant, et peuvent être corroborés par d'autres éléments comme le nom de l'employé, son poste ou ses quarts de travail.

L'accès aux renseignements médicaux personnels par les fonctionnaires chargés de la protection des renseignements médicaux est différent. Ces derniers sont responsables de s'assurer que les garanties mises en place par l'ORS protègent adéquatement les renseignements médicaux personnels.

Ils doivent également faire respecter ces garanties en vérifiant les accès aux renseignements médicaux personnels effectués par d'autres employés. La preuve du motif de ce type d'accès se trouve dans la vérification elle-même, et si les registres de ces vérifications ne sont pas conservés, il n'existe aucun moyen de surveiller ceux qui sont chargés de faire les vérifications.

Les lignes directrices exigent que les dépositaires mettent en place un processus de vérification des accès aux renseignements médicaux personnels effectués par les employés responsables des systèmes et des garanties. Or, l'ORS ne dispose d'aucun processus en ce sens et n'a aucun moyen de revoir de façon rigoureuse les accès aux

renseignements médicaux personnels effectués par les fonctionnaires chargés de la protection des renseignements médicaux et les gestionnaires de l'information.

Le fonctionnaire de l'établissement avait plusieurs motifs autorisés pour accéder à des renseignements médicaux personnels, mais aucun processus n'avait été mis en place pour consigner les accès liés à ces motifs. L'absence de documentation à ce sujet rendait la surveillance de ce fonctionnaire difficile, voire impossible, pour l'ORS.

Notre bureau conclut que l'ORS ne dispose pas d'un processus de surveillance des personnes responsables des vérifications, comme l'exigent les lignes directrices.

CONSTATATIONS

Notre bureau a terminé, en janvier 2021, ses enquêtes sur deux plaintes liées à l'accès non autorisé aux renseignements médicaux personnels de personnes concernées et a conclu qu'il y avait eu atteinte à la vie privée.

D'après l'analyse de notre bureau concernant les mesures prises par l'ORS pour traiter les atteintes à la vie privée, limiter les risques d'atteintes futures et assurer sa conformité à la LRMP, nous concluons ce qui suit :

1. L'ORS n'a pas respecté les exigences de la LRMP, du règlement et des lignes directrices, puisqu'il ne dispose d'aucune politique ni d'aucun processus pour effectuer et consigner les vérifications.

2. L'ORS n'a pas respecté sa politique sur la confidentialité des renseignements médicaux personnels lorsque le fonctionnaire de l'établissement a accédé aux renseignements d'une personne dans le cadre d'une vérification, puisque la politique de l'office exige une consultation préalable avec le gestionnaire ou l'obtention du consentement de la personne concernée. Il s'agit, en fin de compte, d'un manquement aux exigences prévues par la LRMP et le règlement, qui obligent les dépositaires à veiller à ce que ces renseignements ne soient utilisés que de façon autorisée, et uniquement par les personnes qui ont besoin de les connaître.

3. L'ORS n'a pas respecté la LRMP ni le règlement en ne reconnaissant pas le risque potentiel pour la sécurité des renseignements médicaux personnels, et en ne fournissant pas à ses employés une formation suffisante leur permettant d'identifier ce type de risque.

4. L'ORS n'a pas respecté l'obligation qui lui incombe en vertu de l'article 20, en tirant des conclusions qui ne respectent pas les exigences de la LRMP et en plaçant sur les plaignants le fardeau de prouver qu'il y avait eu atteinte à la vie privée. En conséquence :

    a. L'ORS a commis une erreur en concluant que l'utilisation des renseignements médicaux personnels des personnes concernées était autorisée.

    b. L'ORS n'a pas mené une enquête suffisamment approfondie sur les plaintes liées aux atteintes à la vie privée et n'a donc pas réussi à cerner les lacunes dans son processus ni à déterminer les garanties administratives supplémentaires nécessaires pour y remédier, comme l'exige l'article 18 de la LRMP.

5. L'ORS n'a pas respecté les exigences de la LRMP en omettant de documenter les accès aux renseignements médicaux personnels. Il n'a pas non plus fourni suffisamment d'information concernant l'autorisation d'accès, le motif de l'accès, ni la quantité minimale de renseignements consultés, comme l'exige la LRMP.

6. L'ORS n'a pas respecté son obligation de mettre en place des garanties administratives raisonnables. Plus précisément :

    a. La formation offerte par l'ORS à ses employés était insuffisante, puisque ceux-ci ne possédaient pas les connaissances nécessaires pour repérer l'information dont ils avaient besoin tout en limitant leur accès aux renseignements non essentiels.

    b. Les politiques de l'ORS n'invitent pas les employés à signaler à leur supérieur les problèmes liés à leurs privilèges d'accès aux systèmes.

c. L'ORS n'exige pas que les personnes disposant de privilèges d'accès documentent les moments où elles consultent ou partagent des renseignements médicaux personnels à des fins autorisées avec des collègues ayant des privilèges d'accès moindres.

7. L'ORS ne dispose pas d'un processus de surveillance des personnes responsables des vérifications, comme l'exigent le règlement et les lignes directrices.

MISE À JOUR DE L'OFFICE RÉGIONAL DE LA SANTÉ

Au cours de l'enquête, notre bureau a soulevé auprès de l'ORS les enjeux abordés dans le présent rapport, et l'office a commencé à y remédier. Nous sommes également demeurés en communication avec l'ORS pendant la poursuite judiciaire afin d'obtenir des mises à jour sur les changements apportés à ses politiques, procédures, formations et pratiques de vérification.

L'ORS a fourni les mises à jour suivantes :

- L'ORS prévoit consulter Santé numérique (DossiÉ).

- L'ORS a mis sur pied une équipe interdisciplinaire sur l'accès à l'information et la protection de la vie privée, composée de représentants de divers programmes, qui se réunissent pour discuter et approfondir leurs connaissances sur les questions de confidentialité, y compris les vérifications. Cette équipe offre également aux membres l'occasion d'en apprendre davantage sur les différents systèmes électroniques de santé utilisés au sein de l'ORS.

- Un examen des pratiques de vérification d'autres autorités sanitaires en milieu rural a été réalisé. L'ORS a indiqué qu'une des autorités sanitaires dispose d'un programme de vérification particulièrement rigoureux qu'il espère pouvoir intégrer à son propre programme de protection de la vie privée.

- L'ORS a offert une formation sur les vérifications dans le cadre de sa Journée de la LRMP sur les renseignements médicaux personnels 2021.

- Des liens rapides pour faire une demande d'accès à DossiÉ sont maintenant disponibles sur le site Web interne de l'office. De plus, l'ORS a revu les permissions d'accès des utilisateurs et en a créé de nouvelles afin d'offrir un niveau d'accès approprié selon les rôles précis au sein de l'organisation.

- L'ORS élabore actuellement un processus de consignation pour les situations exceptionnelles où des membres du personnel des services de soutien sont appelés à rechercher des renseignements médicaux personnels en dehors de la prestation de soins, mais ne peuvent pas enregistrer le motif de l'accès dans le système électronique de santé.

- L'ORS met à la disposition du personnel des guides de référence rapide, un système de gestion de l'apprentissage et la bibliothèque provinciale de référence sur les applications électroniques. Ces ressources offrent de l'information sur les différents systèmes électroniques d'information et les types de renseignements médicaux personnels qu'ils contiennent.

- L'ORS élabore actuellement des politiques qui reflètent plus clairement ses responsabilités lorsqu'un conflit d'intérêts est identifié.

- La politique de l'ORS sur la déclaration et l'examen des atteintes à la vie privée et des plaintes a été mise à jour. Elle n'indique plus aux employés de conclure automatiquement à l'absence d'atteinte à la vie privée lorsque le dépositaire est incapable de déterminer si un accès était autorisé.

Notre bureau tient à souligner que des progrès importants ont été réalisés pour remédier à plusieurs des problèmes relevés au cours de notre enquête. Bien que les mesures prises par l'ORS ne règlent pas entièrement les enjeux soulevés, nous reconnaissons que le travail se poursuit.

RECOMMANDATIONS

Pour satisfaire aux exigences de la LRMP, les dépositaires doivent instaurer une culture organisationnelle axée sur la protection des renseignements personnels. La protection de la vie privée doit être prise en compte et intégrée à tous les aspects du travail du dépositaire. La meilleure façon d'y parvenir est de mettre en place un programme de

gestion de la vie privée qui soit hiérarchique, global, stratégique, prospectif et ancré dans les principes de protection de la vie privée abordés dans le présent rapport.

À la lumière des constatations tirées de la présente enquête, l'ombudsman formule six recommandations visant à renforcer la protection des renseignements personnels et à consolider les pratiques organisationnelles en matière de vie privée au sein de l'ORS.

Pour donner suite aux constatations n^{os} 1 et 7, l'ombudsman recommande :

> **Recommandation :** 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.

Les recommandations suivantes visent à améliorer les processus de protection des renseignements personnels, les garanties et la formation des employés de l'ORS.

Pour donner suite à la constatation n^{o} 2, l'ombudsman recommande :

> **Recommandation :** 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.

Pour donner suite à la constatation n^{o} 3, l'ombudsman recommande :

> **Recommandation :** 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.

Pour donner suite à la constatation n° 4, l'ombudsman recommande ce qui suit :

Recommandation : 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.

Pour donner suite aux constatations nos 5 et 6, l'ombudsman recommande ce qui suit :

Recommandation : 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 : 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.

RÉPONSE DE L'OFFICE RÉGIONAL DE LA SANTÉ AUX RECOMMANDATIONS

L'ombudsman demande à l'ORS de répondre par écrit aux recommandations dans un délai de 45 jours suivant la réception du présent rapport. Comme ce rapport a été transmis par courriel au dépositaire le 31 décembre 2024, l'ORS devra faire parvenir sa réponse au plus tard le 14 février 2025. La réponse doit indiquer si l'ORS accepte chacune des recommandations. Si l'ORS ne les accepte pas, il devra en expliquer les raisons.

CONFORMITÉ DE L'OFFICE RÉGIONAL DE LA SANTÉ AUX RECOMMANDATIONS

L'ombudsman demande à l'ORS de fournir à notre bureau un plan de mise en œuvre des recommandations dans les 60 jours suivant leur acceptation.

Jill Perron
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