



Commission d'accès à l'information du Québec

Dossier : 1016308-S

Nom des organismes : Centre intégré universitaire de santé et services sociaux de l'Estrie – Centre hospitalier universitaire de Sherbrooke
et
Ministère de la Santé et des Services sociaux

Date : 6 janvier 2022

Membre : M^e Lina Desbiens

DÉCISION

ENQUÊTE en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*¹.

APERÇU

[1] La Commission d'accès à l'information (la Commission) a procédé à une enquête de sa propre initiative à la suite d'un article paru dans le journal *La Tribune*² selon lequel un infirmier auxiliaire du Centre intégré universitaire de santé et services sociaux de l'Estrie – Centre hospitalier universitaire de Sherbrooke (CIUSSS de l'Estrie – CHUS) aurait accédé à des renseignements personnels contenus dans des dossiers de nouveau-nés pour les communiquer à un tiers, et ce, sans le consentement des personnes concernées. Les parents des nouveau-nés ont été sollicités par ce tiers, notamment pour la souscription à des services financiers d'épargnes-études.

[2] L'enquête a été menée auprès du CIUSSS de l'Estrie – CHUS ainsi qu'auprès du ministère de la Santé et des Services sociaux (MSSS) qui est propriétaire du système informatique utilisé. Elle porte sur le respect des obligations prévues à la Loi sur l'accès, en lien avec les événements en cause,

¹ RLRQ, c. A-2.1, Loi sur l'accès.

² Article journal *La Tribune*, 20 mai 2017, page 11.

particulièrement sur les mesures visant à restreindre l'accès aux seuls renseignements personnels nécessaires à l'exercice des fonctions des employés, en lien avec les événements en cause.

[3] La Commission déclare la plainte fondée en partie, prend acte des mesures de sécurité déployées par le CIUSSS de l'Estrie-CHUS, de celles à venir de la part des deux organismes et rend les ordonnances appropriées.

Faits relatifs à l'incident de confidentialité

[4] L'enquête révèle que des renseignements personnels ont été communiqués par un infirmier auxiliaire du CIUSSS de l'Estrie-CHUS ayant accès au système Intégration CLSC (I-CLSC) dans l'exercice de ses fonctions³. Il s'occupait du soutien à domicile des personnes âgées en perte d'autonomie, des personnes en déficience physique de tous âges et des personnes en santé mentale, et ce, pour le réseau local de service de Sherbrooke (RLS)⁴. Il n'avait pas pour fonction de fournir des services à des nouveau-nés ou à leurs parents.

[5] Cet employé a accédé aux renseignements via la fenêtre Identification-Usager (l'index usager) du système I-CLSC. Cet index contient notamment les données démographiques des usagers, telles que nom, adresse, date de naissance. L'employé effectuait des recherches par dates de naissance récentes, choisies de manière aléatoire, dans l'index usager. Il allait ensuite consulter individuellement la fiche d'identification de chacun des dossiers qui apparaissaient pour faire la collecte des renseignements (noms des parents et numéros de téléphone). Par la suite, il communiquait cette information à sa conjointe, à l'emploi d'une entreprise privée, qui communiquait avec eux pour offrir un régime d'épargne-études. Ce stratagème a duré environ 10 ans.

³ Le I-CLSC est un système d'information sur la clientèle et les services des CSSS – mission CLSC, dont l'organisme propriétaire est le MSSS. Il permet la gestion de l'information clinique et administrative des CLSC et de certaines cliniques ambulatoires de centres hospitaliers. Il permet, entre autres, de gérer la demande de service, les interventions et la durée des interventions faites par les intervenants (infirmiers-auxiliaires, infirmières, travailleurs sociaux, etc.). Voir : <http://www.ti.msss.gouv.qc.ca/Familles-de-services/Actifs-informationnels/Integration-CLSC.aspx>.

⁴ À Sherbrooke, le RLS est composé du CSSS-IUGS (le regroupement de l'IUGS et du CLSC de Sherbrooke), du CHUS, des GMF et des cliniques médicales, des organismes communautaires, des pharmacies communautaires, l'entreprise d'économie sociale (COOP de services à domicile de l'Estrie), des résidences privées d'hébergement, des centres d'hébergement conventionnés et non conventionnés, des résidences publiques non institutionnelles, des centres de réadaptation CRE (déficience physique), Regroupement CNDE/Dixville (déficience intellectuelle), Jean-Patrice Chiasson - Maison St-Georges (dépendances), Villa Marie-Claire (jeunes mères en difficulté), du Centre Jeunesse et des partenaires du réseau municipal, scolaire et gouvernemental.

[6] À cet égard, le CIUSSS de l'Estrie – CHUS précise dans ses observations⁵ qu'avant la réforme du réseau de la santé et sa création en avril 2015, soit pendant presque toute la période concernée par l'incident, les installations du RLS de Sherbrooke étaient des établissements juridiquement autonomes et distincts.

[7] Plusieurs plaintes de nouveaux parents qui avaient été sollicités pour des services financiers ou d'assurances ont été formulées envers l'hôpital Fleurimont (aujourd'hui le CHUS). Les enquêtes internes n'ont donné aucun résultat parce que les vérifications se limitaient au système ARIANNE qui était le système d'information clinique utilisé par cet hôpital. En fait, les plaintes étaient formulées dans un établissement qui n'était pas à l'origine de la fuite, alors que les actes reprochés ont été posés dans un autre établissement relevant du RLS de Sherbrooke, juridiquement indépendant. Il était impossible pour le CHUS de faire enquête dans un autre établissement avant 2015.

[8] Ce n'est qu'à la suite d'une plainte d'une famille d'accueil⁶, reçue après la fusion des établissements et la création du CIUSSS de l'Estrie – CHUS en avril 2015, que le service des archives a fait la recherche dans l'ensemble de ses installations du RLS de Sherbrooke, incluant l'ancien CSSS-IUGS. C'est là que le bris de confidentialité a été identifié, au sein de la mission CLSC. Des audits ont été effectués permettant ainsi d'identifier l'employé et de le sanctionner.

[9] Cet événement est le fruit d'un seul individu ayant agi en dehors de son rôle clinique. Cet infirmier auxiliaire a été congédié et a fait l'objet d'une radiation temporaire⁷ par le Conseil de discipline de l'Ordre des infirmières et infirmiers auxiliaires du Québec.

⁵ Cette description tient compte des observations du CIUSSS de l'Estrie - CHUS, *Précision en regard du stratagème utilisé*, 30 juillet 2021.

⁶ Information qui ne se retrouve pas dans le système ARIANNE.

⁷ Il a été trouvé coupable de ne pas avoir préservé le secret quant aux renseignements de nature confidentielle venus à sa connaissance dans l'exercice de sa profession, conformément à l'article 60.4 du *Code des professions*, et de ne pas avoir respecté les règles d'accessibilité aux dossiers prévues à la *Loi sur les services de santé et les services sociaux* et à la *Loi sur l'accès* contrairement à l'article 51 du *Code de déontologie des infirmières et infirmiers auxiliaires*. Conséquemment, il a fait l'objet d'une radiation temporaire de 15 mois pour chacun des chefs d'accusation, peine qui a été purgée de façon concurrente.

AVIS D'INTENTION ET OBSERVATIONS DES ORGANISMES

[10] Le 22 juin 2021, la Commission a transmis un avis d'intention aux organismes les informant qu'à la lumière des informations dont elle dispose au terme de l'enquête, elle pourrait conclure que le CIUSSS de l'Estrie - CHUS et le MSSS, qui partagent la responsabilité de la protection des renseignements personnels qui sont détenus dans le système I-CLSC, n'ont pas respecté :

- 1) L'article 62 de la Loi sur l'accès en ne prévenant pas suffisamment les accès non autorisés aux renseignements personnels des patients dans le module SIC Plus du I-CLSC, faisant en sorte qu'un infirmier auxiliaire au soutien à domicile a pu avoir accès à des renseignements personnels qui n'étaient pas nécessaires à l'exercice de ses fonctions;
- 2) L'article 63.1 de la Loi sur l'accès en n'ayant pas pris les mesures raisonnables :
 - a) Pour assurer la sécurité des renseignements personnels des patients qu'ils détiennent et prévenir l'utilisation non autorisée de ceux-ci, considérant notamment la quantité et la sensibilité des renseignements en cause;
 - b) Pour assurer la sécurité des renseignements personnels des patients en mettant en place un système de détection et de gestion des usages inappropriés.

[11] Cet avis les informe également qu'en l'état actuel du dossier, la Commission pourrait ordonner aux organismes de :

- 1) Transmettre à la Commission, dans les 60 jours suivant sa décision, un plan de redressement visant à limiter l'accès à SIC Plus et le système I-CLSC aux seuls renseignements nécessaires aux employés dans l'exercice de leurs fonctions au sens de l'article 62 de la Loi sur l'accès. Ce plan devra proposer une solution à mettre en œuvre au plus tard à la fin de 2022;
- 2) Transmettre à la Commission, dans les 60 jours suivant sa décision, un plan d'amélioration des mesures de sécurité visant à réaliser des contrôles actifs de la sécurité des renseignements personnels et sensibles qu'ils détiennent et mettre en place des mesures visant à pallier aux vulnérabilités identifiées à la suite de l'incident;

- 3) Transmettre à la Commission, dans les deux ans suivant sa décision finale, une évaluation relative à l'ensemble des mesures déployées et propre à assurer la protection des renseignements personnels détenus dans SIC Plus de I-CLSC faite par un auditeur externe indépendant, dont l'identité devra être approuvée par la Commission. Cette évaluation devra notamment porter sur :
 - a) Les mesures relatives à l'accessibilité aux renseignements personnels détenus par les organismes, par son personnel et à la surveillance de celles-ci;
 - b) Les mesures de sécurité mises en place et propres à assurer la sécurité des renseignements personnels et à la surveillance de celles-ci.

[12] Conformément à l'article 129 de la Loi sur l'accès, la Commission a invité les organismes à présenter leurs observations écrites et à produire tous documents venant les appuyer.

[13] Le 8 octobre 2021, à la suite de la réception des observations des organismes, la Commission les invite à compléter les observations soumises pour expliquer :

- pourquoi tous les intervenants ayant accès à l'index-usager ont « la qualité pour le recevoir » parce que « ce renseignement est nécessaire à l'exercice de ses fonctions » (article 62 de la Loi sur l'accès);
- en quoi les mesures de sécurité adoptées sont raisonnables, compte tenu notamment de la sensibilité des renseignements, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

[14] À la demande des organismes, une rencontre s'est tenue le 8 novembre 2021 et les observations écrites s'y rapportant ont été transmises par la suite.

[15] À la lumière de l'ensemble des informations obtenues dans le cadre de son enquête et des observations des organismes, la Commission conclut que l'accès à l'index-usager du système I-CLSC accordé à l'employé à l'origine de l'incident de confidentialité respecte l'article 62 de la Loi sur l'accès. Toutefois, les mesures de sécurité adoptées à l'égard de ce système n'étaient pas propres à assurer la protection des renseignements personnels compte tenu, notamment, de la sensibilité et de l'utilisation des renseignements en cause. L'article 63.1 de la Loi sur l'accès n'a donc pas été respecté.

ANALYSE

1. Le CIUSSS de l'Estrie – CHUS et le MSSS sont assujettis à la Loi sur l'accès

[16] Le CIUSSS de l'Estrie – CHUS et le MSSS sont des organismes publics assujettis à la Loi sur l'accès⁸. Cette loi établit les règles relatives à la protection des renseignements personnels détenus par les organismes publics dans l'exercice de leurs fonctions, et ce, peu importe le support.

[17] Le I-CLSC est un système d'information sur la clientèle et les services des CSSS – mission CLSC, dont l'organisme propriétaire est le MSSS⁹. Il s'agit d'un actif décentralisé du MSSS, dont le déploiement s'est effectué à la grandeur du réseau de la santé il y a plus de 20 ans. Ce système permet la gestion d'une importante quantité de renseignements sensibles détenus à des fins de soins de santé.

2. Les renseignements visés sont des renseignements personnels sensibles

[18] La Loi sur l'accès prévoit que les renseignements qui concernent une personne physique et permettent de l'identifier sont des renseignements personnels. Ainsi, dès qu'un renseignement permet de faire connaître quelque chose permettant de distinguer une personne physique d'une autre, ce renseignement est personnel, et ce, peu importe sa forme ou son support.

[19] En l'espèce, les renseignements visés par l'enquête sont les noms des nouveau-nés et leurs données démographiques, dont l'adresse des parents et leur numéro de téléphone. Il s'agit de renseignements personnels, puisqu'ils font connaître quelque chose sur quelqu'un et permettent également de distinguer cette personne par rapport à quelqu'un d'autre. De plus, ces renseignements sont détenus dans des dossiers de patients qui sont, par définition, d'une grande sensibilité et confidentiels.

[20] Plus particulièrement, ces renseignements sont détenus dans le système I-CLSC pour la prise en charge des nouveau-nés à la sortie de l'hôpital. Comme renseignements de santé, il s'agit de renseignements sensibles.

⁸ Article 3 et 7 de la Loi sur l'accès.

⁹ <https://www.msss.gouv.qc.ca/professionnels/documentation-sources-de-donnees-et-indicateurs/sources-de-donnees-et-metadonnees/iclsc/>

3. Obligations découlant de la Loi sur l'accès

[21] La Loi sur l'accès prévoit que les renseignements personnels détenus par un organisme public sont accessibles, sans le consentement de la personne concernée, à toute personne qui a la qualité pour le recevoir au sein de cet organisme seulement lorsque ce renseignement est nécessaire à l'exercice de ses fonctions.

[22] La Loi sur l'accès prévoit également qu'un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels et raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. Ces mesures de prévention, de détection et de contrôle doivent permettre de minimiser les risques.

[23] Plus particulièrement, la Loi sur l'accès prévoit qu'un organisme doit prendre les mesures visant à restreindre l'accès aux seuls renseignements personnels nécessaires à l'exercice des fonctions des employés :

62. Un renseignement personnel est accessible, sans le consentement de la personne concernée, à toute personne qui a qualité pour le recevoir au sein d'un organisme public lorsque ce renseignement est nécessaire à l'exercice de ses fonctions.

En outre, cette personne doit appartenir à l'une des catégories de personnes visées au paragraphe 4° du deuxième alinéa de l'article 76 ou au paragraphe 5° du premier alinéa de l'article 81.

[24] De plus, la loi prévoit que des mesures de sécurité propres à assurer la protection des renseignements personnels doivent être prises. Ces mesures doivent être raisonnables compte tenu, notamment, de leur sensibilité, comme en l'espèce :

63.1. Un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

[25] En l'espèce, le MSSS et le CIUSSS de l'Estrie - CHUS ont une responsabilité partagée quant aux renseignements détenus dans I-CLSC et aux mesures de sécurité prises. D'une part, le MSSS est responsable du système décentralisé et de sa configuration et, d'autre part, les établissements¹⁰ sont responsables des renseignements contenus dans le système, notamment des profils d'accès. Ils ont tous deux un rôle à jouer dans le respect des obligations prévues à la Loi sur l'accès.

a. Accès aux renseignements nécessaire à l'exercice de ses fonctions

[26] Concernant le droit d'accès de l'employé à l'index patient du I-CLSC, les organismes font valoir que les renseignements personnels qui s'y trouvent sont nécessaires à l'exercice de ses fonctions, à titre d'intervenant clinique de première ligne, et que cet accès respecte la Loi sur l'accès.

[27] La Commission est d'avis que l'employé pouvait avoir accès à l'ensemble des informations contenues dans l'index sans le consentement des personnes concernées, puisqu'elles étaient nécessaires à l'exercice de ses fonctions¹¹.

[28] En effet, le système I-CLSC, qui contient l'index-usager, fonctionne par établissement. L'index est accessible à tout intervenant de première ligne de cet établissement. Ainsi, l'employé n'avait accès qu'aux dossiers de l'établissement de sa région sociosanitaire et non à l'ensemble des dossiers de la province. Aucun accès n'est accordé à un intervenant en CLSC dont la fonction n'exige pas qu'il ait accès à ces informations, par exemple les aides en santé et services sociaux à domicile ou les auxiliaires familiales.

[29] Au CIUSSS de l'Estrie – CHUS, le logiciel I-CLSC est séparé en neuf bases de données régionales distinctes, soit autant d'index-usagers distincts, le tout, en conformité avec la division des RLS existants avant 2015 en Estrie.

[30] À l'intérieur de chacune des bases de données du logiciel I-CLSC, des profils d'accès sont établis en fonction des besoins d'informations et des tâches à réaliser. À titre d'exemple, pour le RLS de Sherbrooke, la base de données I-CLSC locale compte un total de 72 profils d'accès différents. Ces profils sont répartis en 44 profils cliniques, 27 profils administratifs (secrétaires médicales, agentes administratives, commissaires aux plaintes, etc.) et un profil pilote/archiviste médical.

¹⁰ *Loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales*, RLRQ, c. O-7.2.

¹¹ Article 62 de la Loi sur l'accès.

[31] Toutefois, tout intervenant ayant un accès à I-CLSC a accès à l'index-usager de la région sociosanitaire où il intervient. C'est grâce à cet accès que l'employé a pu identifier les naissances de sa région, soit celle du RLS de Sherbrooke, bien qu'il n'intervenait pas auprès de cette clientèle.

[32] Les organismes soutiennent que l'accès à l'index-usager était nécessaire à l'exercice des fonctions de cet intervenant qui agissait en première ligne dans le réseau de la santé et qu'il ne devait pas se limiter aux seuls dossiers dont il a la charge.

[33] Ils indiquent que compte tenu du rôle de services de première ligne qu'offre un CLSC, selon la mission qui lui est dévolue par la loi, l'accès à l'ensemble des informations de l'index de I-CLSC est nécessaire à tout employé susceptible d'intervenir ponctuellement auprès de tout usager pour leur venir en aide rapidement.

[34] La mission d'un CLSC, définie par la loi¹², est d'offrir des services de santé et des services sociaux courants, en première ligne, à la population du territoire qu'il dessert. Pour ce faire, le CLSC doit s'assurer que les personnes qui requièrent des services pour elles ou pour leurs familles soient rejointes et que leurs besoins soient évalués et les services requis leur soient offerts ou, si cela est nécessaire, qu'elles soient dirigées vers les organismes ou personnes les plus aptes à leur venir en aide.

[35] Dans ce contexte, la Commission conclut que l'accès à l'ensemble de l'index-usager de sa région administrative, soit du RLS de Sherbrooke, qui a été accordé à l'employé responsable de l'incident de confidentialité était nécessaire à l'exercice de ses fonctions d'infirmier auxiliaire, à titre d'intervenant de première ligne dans un CLSC.

b. Les mesures de sécurité n'étaient pas propres à assurer la protection des renseignements personnels et n'étaient pas raisonnables

[36] L'enquête révèle que, malgré la présence d'outils limitant les droits d'accès aux renseignements personnels, un employé a collecté, utilisé et communiqué des renseignements personnels alors que cela n'était pas nécessaire à l'exercice de ses fonctions ni autorisé par la loi et par conséquent, en contravention de la Loi sur l'accès.

¹² *Loi sur les services de santé et les services sociaux*, RLRQ, c. S-4.2, art. 80.

[37] En effet, l'employé en cause a collecté, utilisé et communiqué des renseignements personnels auxquels il avait accès dans le but de les transmettre à sa conjointe, qui les a utilisés à des fins de sollicitation.

[38] Les mesures de sécurité de prévention et de contrôle en place n'ont pas permis de détecter cette situation qui a duré 10 ans, et ce, malgré plusieurs plaintes de parents. Dans ce contexte, la Commission conclut que les mesures de sécurité en place n'ont pas permis d'assurer la protection des renseignements personnels contenus dans le système I-CLSC et n'étaient pas raisonnables compte tenu, notamment, de la sensibilité des renseignements, du contexte d'utilisation et de leur quantité.

[39] Créé en 2015, le CIUSSS de l'Estrie – CHUS est responsable des renseignements détenus dans le système I-CLSC. Près de 5 000 personnes utilisent le logiciel I-CLSC au quotidien et les neuf banques de données regroupent plus de 1,3 million de dossiers d'utilisateurs.

[40] Depuis 2015, un ensemble de mesures de sécurité sont en place, notamment :

- des profils limitant l'accès aux renseignements personnels par les employés;
- des mesures de sécurité physiques et technologiques protégeant les serveurs et les applications¹³;
- une catégorisation des actifs critiques;
- plusieurs politiques en vigueur¹⁴;
- un programme de formation continue pour les employés en matière de protection des renseignements personnels;
- un engagement à la confidentialité signé par tous les nouveaux employés;
- une campagne de sensibilisation annuelle à la protection des renseignements personnels .

¹³ Par exemple, une salle de serveurs centralisés redondante sur deux sites hébergeant la majorité des systèmes d'information critiques; l'hébergement virtuel des applications est sécurisé, mais certaines applications sont hébergées par le MSSS.

¹⁴ Gestion des dossiers; Politique en matière de communication des renseignements personnels dans le but d'assurer la protection des personnes; Accès et protection de l'information; Politique de sécurité de l'information du CIUSSS de l'Estrie – CHUS; Cadre de gestion de la sécurité de l'information.

[41] Il ressort des observations du CIUSSS de l'Estrie – CHUS que certaines mesures se sont ajoutées depuis la découverte du stratagème en 2016, dont diverses activités et outils de sensibilisation¹⁵ et l'amélioration des mesures de sécurité¹⁶ et de contrôle¹⁷.

[42] Toutefois, compte tenu de la sensibilité des informations contenues dans les bases de données I-CLSC et de l'incident à l'origine de la présente enquête, le CIUSSS de l'Estrie – CHUS informe la Commission qu'il doit prochainement mettre en place un processus de surveillance et d'audit par échantillonnage comme mesure supplémentaire de contrôle prospectif.

[43] Pour sa part, le MSSS explique que sa Direction des technologies de l'information travaille à mettre en place un indicateur paramétrable permettant de cibler tout volume de consultations de dossiers à l'index-usager jugé anormal. Cette mesure de veille permettrait d'agir plus tôt et de détecter des situations de non-conformité à la loi en matière d'accès à des renseignements personnels.

[44] Il ajoute que le dossier patient informatisé contiendra des fonctionnalités de journalisations « intelligentes » qui permettront de détecter des accès et utilisations non appropriés aux données par un utilisateur ayant accès au système. Par exemple, une de ces fonctions pourra vérifier automatiquement si les recherches et mises à jour d'index-usager par un utilisateur correspondent à ses tâches cliniques ou administratives (infirmière, psychologue, ergothérapeute, agent administratif, etc.).

[45] La Commission considère que l'ajout de ces mesures proactives supplémentaires de contrôle des accès est nécessaire. En effet, les mesures en

¹⁵ Formations à l'embauche et signature d'un engagement à la confidentialité (joint aux observations), capsules de sensibilisation au respect de la confidentialité et sécurité de l'information, participation aux semaines nationales de sécurité de l'information et campagnes bisannuelles de confidentialité, page dédiée à la sécurité de l'information sur l'Intranet de l'établissement, diffusion d'avis de sécurité et de guides encadrant les bonnes pratiques en matière de sécurité de l'information.

¹⁶ Notamment quant aux accès octroyés et au paramétrage des profils d'accès, du plan de continuité des affaires, des rappels de confidentialité sont présents lors de toute connexion à l'environnement technologique du CIUSSS de l'Estrie – CHUS et l'ensemble de la communauté interne est informé sur une base régulière de l'existence de processus de journalisation dans tous les systèmes de l'établissement.

¹⁷ Un mécanisme de vigie existe pour les accès à certains types de dossiers (ex. : événements médiatiques pouvant impliquer des usagers du CIUSSS de l'Estrie – CHUS ou de services offerts à des personnalités connues, etc.) assurant une journalisation prospective des accès dans I-CLSC et d'autres systèmes d'information clientèle. Ces démarches ont permis de détecter des bris de confidentialité qui ont fait l'objet d'enquêtes et de sanctions.

place au moment des événements à l'origine de l'enquête n'étaient pas raisonnables, car elles n'ont pas permis de détecter les accès, les utilisations et les communications effectués par l'employé en contravention de la législation, sur une période de 10 ans, malgré plusieurs plaintes de parents. La Commission prend en considération la sensibilité des renseignements de santé, la quantité importante des renseignements personnels contenus dans le système I-CLSC et le nombre élevé d'employés de première ligne y ayant accès. La Commission est d'avis qu'en raison des considérations particulières de ce dossier, des mesures de sécurité raisonnables doivent être à la fois préventives et permettre un contrôle proactif, *a posteriori*, du respect des obligations de protection des renseignements personnels.

[46] Enfin, ces mesures de sécurité devront évoluer au rythme des développements technologiques.

[47] À ce sujet, la Commission comprend que le système I-CLSC est appelé à être remplacé dans les années à venir. En effet, le MSSS a informé la Commission qu'une initiative intitulée « Avenir I-CLSC » a été déposée aux instances compétentes pour proposer une solution de remplacement qui sera nécessaire d'ici la venue du Dossier de santé numérique. La solution transitoire devrait être déployée au cours de l'année 2024.

[48] La Commission invite le MSSS à s'assurer d'évaluer la conformité de cette solution dès les premières étapes et tout au long du projet. Elle rappelle le rôle que doit jouer le comité ministériel sur l'accès à l'information et la protection des renseignements personnels qui doit être informé et impliqué dans un projet de cette nature selon le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*¹⁸ :

7. Un organisme public doit informer le comité visé à l'article 2 des projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels.

Le comité suggère, parmi ces projets, ceux qui doivent être encadrés par des mesures particulières de protection des renseignements personnels. Ces mesures comprennent:

1° la nomination d'une personne chargée de la mise en œuvre des mesures de protection des renseignements personnels pour chaque projet;

¹⁸ RLRQ, c. A-2.1, r. 2.

2° l'évaluation, dès l'étude préliminaire du projet, des risques d'atteinte à la protection des renseignements personnels;

3° des mesures propres à assurer la protection des renseignements personnels pendant toute la période de réalisation du projet et son maintien lors de l'utilisation, de l'entretien, de la modification et de l'évolution du système d'information ou de prestation électronique des services visés;

4° la description des exigences de protection des renseignements personnels dans le cahier de charges ou le contrat relatif au projet, à moins que l'exécutant du contrat soit un autre organisme public;

5° la description des responsabilités des participants au projet en matière de protection des renseignements personnels;

6° la tenue d'activités de formation sur la protection des renseignements personnels à l'intention des participants au projet.

CONCLUSION

[49] À la lumière de ce qui précède, la Commission conclut que l'accès à l'index-usager du système I-CLSC accordé à l'employé responsable de l'incident de confidentialité à l'origine de la présente enquête respecte l'article 62 de la Loi sur l'accès. Toutefois, les mesures de sécurité adoptées à l'égard de ce système n'étaient pas raisonnables pour assurer la protection des renseignements personnels dans les circonstances au sens de l'article 63.1 de la Loi sur l'accès.

[50] La Commission prend acte des mesures que le CIUSSS de l'Estrie – CHUS a mises en place depuis l'incident.

[51] Elle prend aussi acte des mesures de contrôles prospectifs supplémentaires que le CIUSSS de l'Estrie – CHUS et le MSSS entendent déployer.

POUR CES MOTIFS, LA COMMISSION :

[52] **DÉCLARE** la plainte fondée en partie.

[53] **PREND ACTE** des mesures de sécurité déployées par le CIUSSS de l'Estrie – CHUS et de celles à venir de la part des deux organismes.

[54] **ORDONNE** aux deux organismes de transmettre à la Commission, dans les 60 jours suivant la réception de la décision, un plan d'amélioration des mesures de sécurité visant à réaliser des contrôles actifs de la sécurité des renseignements personnels sensibles qu'ils détiennent devant notamment comprendre :

- pour le CIUSSS de l'Estrie – CHUS, l'état d'avancement des travaux relatifs à la mise en place d'un processus de surveillance et d'audit par échantillonnage, incluant un échéancier de réalisation de leur mise en place complète prévue en 2022;
- pour le MSSS, l'état d'avancement des travaux relatifs à la mise en place d'un indicateur paramétrable permettant de cibler tout volume de consultations de dossiers à l'index-usager jugé anormal, incluant un échéancier de réalisation de leur mise en place complète.

[55] **INVITE** le MSSS à s'assurer d'évaluer la conformité de la solution de remplacement du système I-CLSC dès les premières étapes et tout au long du projet.

Original signé

M^e Lina Desbiens
Membre de la Commission, section de
surveillance