Ministère de la Santé et des Services sociaux

Politique de gouvernance des renseignements de santé et de services sociaux du ministère de la Santé et des Services sociaux

Votre gouvernement

Québec

ÉDITION :
La Direction des communications du ministère de la Santé et des Services sociaux

Le présent document s'adresse spécifiquement aux intervenants du réseau québécois de la santé et des services sociaux et n'est accessible qu'en version électronique à l'adresse : **www.msss.gouv.qc.ca**, section **Publications**

Le genre masculin est utilisé sans aucune discrimination et dans le seul but d'alléger le texte.

Dépôt légal – 2025
Bibliothèque et Archives nationales du Québec
ISBN : 978-2-555-01155-7 (version PDF)

Politique de gouvernance des renseignements

Table des matières

Politique de gouvernance des renseignements

ACRONYMES LEXIQUE ET DÉFINITIONS

Principaux acronymes

LRSSS : Loi sur les renseignements de santé et de services sociaux (RLRQ, chapitre R-22.1), adoptée à la suite du projet de loi n° 3, Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives (2023, chapitre 5), et dont la majorité des articles sont entrés en vigueur le 1er juillet 2024 (décret 946-2024 du 5 juin 2024)

MSSS : ministère de la Santé et des Services sociaux

PST : Produit ou service technologique

Lexique et définitions

Renseignement :

Un « renseignement de santé et de services sociaux » (ci-après « Renseignement »), tel que défini à l'article 2 de la LRSSS, désigne trois types de renseignements :

- Tout renseignement qui concerne une personne et qui permet d'identifier cette personne, directement ou indirectement; **et** qui répond à l'une des caractéristiques suivantes :
  - Il concerne l'état de santé physique ou mentale d'une personne et ses facteurs déterminants, y compris les antécédents médicaux ou familiaux de cette personne.
  - Il concerne tout matériel prélevé sur cette personne dans le cadre d'une évaluation ou d'un traitement ainsi que tout aide suppléant à une incapacité de cette personne (p. ex. : *implant prothèse, etc.*).
  - Il concerne les services de santé ou de services sociaux offerts à cette personne (p. ex. : *nature de ces services, leurs résultats, les lieux où ils ont été offerts, etc.*).
  - Il a été obtenu dans l'exercice d'une fonction prévue par la Loi sur la santé publique[1].
  - Toute autre caractéristique déterminée par le règlement du gouvernement.
- Tout renseignement permettant l'identification d'une personne (p. ex. : *son nom, sa date de naissance, ses coordonnées, etc.*) qui est accolé à un « renseignement de santé et de services sociaux ».

[1] RLRQ, chapitre S-2.2.

- Tout renseignement permettant l'identification d'une personne qui est recueilli en vue de l'admission de cette personne dans un établissement ou de sa prise en charge par un organisme (p. ex. : *un renseignement recueilli en vue de l'inscription d'une personne dans une résidence privée pour ainés*).

Incident de confidentialité :

Un accès à un Renseignement ou toute autre utilisation ou communication d'un Renseignement non autorisé par la loi, la perte d'un Renseignement ou toute autre atteinte à sa protection (p. ex. : *un employé utilise des Renseignements à des fins personnelles pour vérifier l'état de santé d'un ami ou d'un membre de sa famille, la vente des Renseignements à des tiers, etc.*).

Organisme du secteur de la santé et des services sociaux :

Tout organisme visé à l'article 4 de la LRSSS, soit :

- Le MSSS.
- Santé Québec.
- Les établissements de santé et de services sociaux[2].
- La Régie régionale de la santé et des services sociaux du Nunavik.
- Les personnes ou organismes visés à l'annexe I de la LRSSS (p. ex. : *la Régie de l'assurance maladie du Québec, Héma-Québec, Corporation d'urgences-santé, etc*.).
- Les personnes et les groupements visés à l'annexe II de cette loi (p. ex. : *un cabinet privé de professionnels, une résidence privée pour personnes aînées, une ressource intermédiaire, une ressource de type familial, etc*.).
- Un prestataire de services ayant conclu une entente avec un organisme du secteur de la santé et des services sociaux pour la fourniture de services de santé ou de services sociaux.
- Un établissement d'enseignement de niveau collégial ou universitaire pour ses activités liées à la prestation de services de santé ou de services sociaux.
- Toute autre personne ou tout autre groupement déterminé par règlement du gouvernement.

Critère de nécessité :

Un Renseignement est nécessaire si l'objectif poursuivi est légitime, important et réel et que l'atteinte à la vie privée subie par les personnes concernées est proportionnelle à cet objectif.

[2] Soulignons cependant que, sauf exception relative à l'application des articles 38 et 38.1 de la Loi sur la santé publique (RLRQ, chapitre S-2.2), les dispositions de la LRSSS ne sont pas applicables à l'égard de l'établissement visé par la Loi sur les services de santé et les services sociaux pour les autochtones cris (RLRQ, chapitre S-5), c'est-à-dire au Conseil cri de la santé et des services sociaux de la Baie James. Cet établissement n'est donc pas un organisme du secteur de la santé et des services sociaux sous la LRSSS (voir le paragraphe 2° du décret 946-2024 du 5 juin 2024).

Le respect de ce critère doit être évalué préalablement aux étapes de la collecte, de l'utilisation et de la communication d'un Renseignement.

Le traitement d'un Renseignement sera autorisé si le Renseignement est considéré comme plus utile à l'organisme que préjudiciable à la personne concernée par le Renseignement.

Le consentement d'une personne ne peut permettre de déroger au critère de nécessité.

Politique de gouvernance des renseignements

1. MISE EN CONTEXTE

La présente politique de gouvernance est adoptée en vertu de l'article 105 de la LRSSS.

Elle vise à mettre en œuvre les principes de la LRSSS et du Règlement sur la gouvernance des renseignements de santé et de services sociaux[3], lequel est édicté par le ministre de la Santé en application de l'article 90 de cette loi.

2. CHAMP D'APPLICATION DE LA POLITIQUE

La présente politique s'applique :

- à l'ensemble des membres du personnel du MSSS et à tous les professionnels qui y exercent leur profession, y compris les étudiants, les stagiaires, les employés en prêt de services et les contractuels, lorsqu'ils recueillent, utilisent, communiquent, conservent ou détruisent des Renseignements dans le cadre de l'exercice de leurs fonctions ou de leur profession; ou lorsqu'ils ont autrement accès à des Renseignements détenus par le MSSS;

- à tout prestataire de services ou mandataire à qui le MSSS confie des Renseignements dans le cadre de l'exécution d'un mandat ou d'un contrat de services.

La présente politique vise tous les Renseignements détenus par le MSSS, y compris ceux dont la conservation est assurée par un tiers. Elle est applicable sans égard au support sur lequel les Renseignements sont consignés (p. ex. : *support papier, électronique, etc.)*, et ce, depuis leur collecte jusqu'à leur destruction.

3. RÔLE ET RESPONSABILITÉS À L'ÉGARD DES RENSEIGNEMENTS

3.1. Le responsable de la protection des Renseignements du MSSS :

- Veille à assurer le respect et la mise en œuvre de la LRSSS et de la présente politique au sein du MSSS.
- Conseille les directions du MSSS sur les questions relatives à la protection des Renseignements.
- Reçoit et traite les demandes visant l'exercice de certains droits par les citoyens sur les Renseignements détenus par le MSSS (p. ex. : *demande d'accès, demande de rectification, journalisation, etc*.).

[3] RLRQ, chapitre R-22.1, chapitre r. 2.

- Autorise les demandes de communication de Renseignements introduites par les directions du MSSS selon les modalités prévues à la section 6.1 de la présente politique (p. ex. : *en cas de communication de Renseignements à un tiers dans le cadre de l'exécution d'un contrat, ou lorsque la communication est prévue par la loi)*.
- Maintient le registre des communications visé à la section 6.2 de la présente politique.
- Maintient le registre des consentements visé à la section 11 de la présente politique.
- Prend les moyens nécessaires pour remédier à tout incident de confidentialité affectant les Renseignements et maintient le registre des incidents de confidentialité de la manière prévue par les lois applicables.
- Assure le traitement des plaintes concernant les Renseignements selon le processus prévu à la section 12 de la présente politique.
- Informe et sensibilise le personnel du MSSS sur leurs responsabilités en matière de protection des Renseignements et sur les meilleures pratiques à mettre en œuvre en cette matière.
- Met en place une offre de formation en matière de protection des Renseignements pour les membres du personnel du MSSS, et en assure la mise à jour.
- Prend les moyens nécessaires afin d'assurer la disponibilité des Renseignements (p. ex. : *réalise des sauvegardes et des tests de restaurations, etc*.).
- Préside les travaux du Comité sur la gouvernance des Renseignements du MSSS.

Au moment de l'entrée en vigueur de la présente politique, le responsable de la protection des Renseignements est monsieur **Marc-Nicolas Kobrynsky**, sous-ministre adjoint.

3.2. Le gestionnaire délégué aux données numériques gouvernementales :

- Autorise la communication de Renseignements à des fins de performance et d'appréciation des résultats ainsi que d'autres objectifs spécifiques[4], conformément aux critères et aux procédures prévus à la LRSSS.
- Tient un registre des autorisations de communication de Renseignements qu'il a accordées.
- Participe aux séances et aux travaux du Comité sur la gouvernance des Renseignements du MSSS.

Au moment de l'entrée en vigueur de la présente politique, le gestionnaire délégué aux données numériques gouvernementales est monsieur **Marc-Nicolas Kobrynsky**, sous-ministre adjoint.

[4] Article 80 de la LRSSS.

3.3. La personne-ressource en matière d'avis de restriction et de refus :

- Reçoit et traite les avis de restriction ainsi que les avis de refus, et en assure le suivi interne.
- Bloque les accès aux Renseignements à la suite d'un avis de restriction ou d'un avis de refus conforme.
- S'assure que la personne qui formule un avis de restriction ou un avis de refus est adéquatement informée des conséquences potentielles et des risques associés à sa démarche.

Au moment de l'entrée en vigueur de la présente politique, ces fonctions relèvent du directeur de la Direction de la valorisation et de la protection des données du MSSS, monsieur **Pier Tremblay**.

3.4. Directeur général des ressources informationnelles :

- Veille à l'application des normes applicables aux PST du MSSS.
- Supervise la mise en place et le maintien des mesures de sécurité propres à assurer la protection des Renseignements contenus dans ces PST.
- Assure le maintien du calendrier des normes PST, effectue les analyses et en assure le suivi afin d'en permettre la mise à jour continue.

Au moment de l'entrée en vigueur de la présente politique, le Directeur général des ressources informationnelles est monsieur **Mohamed-Nabil Ben-Abid**.

3.5. Le personnel du MSSS :

- Prend connaissance de la présente politique et en respecte l'esprit, les dispositions et les procédures.
- Prend les mesures nécessaires pour protéger la confidentialité des Renseignements auxquels il a accès conformément à la section 5 de la présente politique.
- Accède seulement aux Renseignements lorsqu'il fait partie d'une catégorie de personnes autorisée au sens de l'Annexe A de la présente politique et que les Renseignements sont nécessaires à l'exercice de ses fonctions au sein du MSSS.
- S'assure que les Renseignements qu'il utilise sont à jour, exacts et complets afin de servir aux fins pour lesquelles ils ont été recueillis ou sont utilisés.
- Communique uniquement les Renseignements selon la procédure prévue à la section 6 de la présente politique.

- S'informe de la période de conservation établie pour les Renseignements qu'il détient dans ses fichiers et procède à leur destruction conformément aux modalités prévues à la section 7.1 de la présente politique.
- Informe son gestionnaire et le responsable de la protection des Renseignements du MSSS de tout potentiel incident de confidentialité affectant les Renseignements, et ce, dès que possible suivant la prise de connaissance de la survenance d'un tel incident potentiel.
- Effectue, dès son entrée en fonction, la formation en matière de protection des Renseignements mise à sa disposition par le MSSS.
- Assure la mise à jour annuelle de ses connaissances en cette matière.

4. UTILISATION D'UN RENSEIGNEMENT

Personnel autorisé. Seuls les membres du personnel ou les personnes qui font partie d'une catégorie prévue à l'Annexe A peuvent utiliser ou accéder aux Renseignements détenus par le MSSS lorsque cela est nécessaire à l'exercice de leurs fonctions.

Finalité de l'utilisation. Le personnel et les personnes visées par ces catégories peuvent uniquement utiliser les Renseignements :

- pour les fins pour lesquelles ils ont été recueillis;
- pour l'exercice des fonctions du ministre de la Santé, y compris ses fonctions relatives à l'organisation ou à l'évaluation des services de santé et des services sociaux;
- dans les cas prévus aux articles 62 à 65 de la LRSSS (p. ex. : *utilisation nécessaire à l'application d'une loi ou utilisation manifestement au bénéfice de la personne concernée, etc.*).

Utilisation sujette à autorisation. Un membre du personnel du MSSS qui est visé par une telle catégorie doit obtenir l'autorisation de son gestionnaire avant d'utiliser un Renseignement à une fin différente de celle pour laquelle le Renseignement a été initialement recueilli.

5. CONSERVATION D'UN RENSEIGNEMENT

Confidentialité. Tout membre du personnel du MSSS assure la confidentialité et l'intégrité des Renseignements détenus par le MSSS. Pour ce faire, le personnel :

- ✓ Ne révèle aucun Renseignement dont il a pris connaissance dans l'exercice de ses fonctions sans y être autorisé par un gestionnaire.
- ✓ Accède seulement aux Renseignements nécessaires à l'exercice de ses fonctions.
- ✓ S'assure que les Renseignements qu'il utilise sont complets, à jour et exacts afin qu'ils servent aux fins pour lesquelles le MSSS les recueille ou les utilise.

- ✓ S'assure que les Renseignements consignés sur un même support (p. ex. : papier, électronique, etc.) sont enregistrés selon les normes de la nomenclature du MSSS[5].
- ✓ Ne conserve, dans ses fichiers ou sur ses appareils personnels et appareils personnels amovibles, aucun Renseignement porté à sa connaissance dans le cadre de ses fonctions, sauf sur un support qui lui est fourni par le MSSS à cette fin.
- ✓ S'adresse à son gestionnaire ou au responsable de la protection des renseignements du MSSS pour toute question relative à la confidentialité ou à la période de conservation d'un Renseignement.

***Délai de conservation*.** Les Renseignements sont conservés pendant la période prévue au calendrier de conservation du MSSS[6] ou, au plus tard, pendant la durée nécessaire à la réalisation des fins pour lesquelles ils ont été recueillis ou sont utilisés.

***Disponibilité des Renseignements*.** Le responsable de la protection des Renseignements doit prendre les moyens nécessaires afin que les Renseignements détenus par le MSSS demeurent utilisables, même en cas d'incident affectant leur support.

Plus spécifiquement, il s'engage à :

- Réaliser des sauvegardes régulières dans lesquelles les Renseignements sont sauvegardés, ce qui permet de restaurer les Renseignements en cas de perte ou de corruption.
- Tester régulièrement les sauvegardes dans lesquelles des tests de restauration sont effectués périodiquement pour vérifier l'efficacité des procédures de sauvegarde.

6. COMMUNICATION D'UN RENSEIGNEMENT

La LRSSS autorise le MSSS à communiquer les Renseignements qu'il détient sans le consentement des personnes concernées dans certains cas d'exception, et ce, sous certaines conditions. La présente section expose certains cas de communication ne nécessitant pas l'obtention du consentement ainsi que les conditions et modalités afférentes à ces communications.

6.1. Modalités de communication

Note informative :

Les modalités prévues à la présente sous-section ne sont pas applicables aux communications devant être autorisées par le gestionnaire délégué aux données numériques gouvernementales du MSSS selon la procédure prévue aux articles 80 et suivants de la LRSSS ni aux cas de communication prévus à la section 6.3 de la présente politique.

[5] Il est possible d'adresser toute question relative aux normes de nomenclature du MSSS au Service de la gestion documentaire de la Direction de la valorisation et protection des données à l'adresse courriel suivante : gestion.documentaire@msss.gouv.qc.ca.

[6] Calendrier de conservation des documents - Documentation de l'intranet ministériel - MSSS

Demande de communication. La demande de communication de Renseignement doit être adressée au responsable de la protection des Renseignements du MSSS par le biais d'une demande écrite transmise à l'adresse suivante : msss.loirenseignement@msss.gouv.qc.ca.

La demande doit minimalement contenir :

- L'identification de la personne ou de l'organisme receveur des Renseignements.
- Une description des Renseignements visés.
- Une description de l'objectif poursuivi par la communication.
- Une justification de la nécessité et de la pertinence des Renseignements pour l'atteinte de cet objectif.

Évaluation de la demande. Le responsable de la protection des Renseignements du MSSS évalue la demande en fonction des critères légaux et des politiques internes du MSSS. Il s'assure notamment que :

- la communication est nécessaire et proportionnée à l'objectif poursuivi;
- les Renseignements communiqués sont pertinents à l'atteinte de cet objectif;
- la communication est limitée aux Renseignements qui sont strictement nécessaires à l'atteinte de cet objectif;
- les risques pour la vie privée des personnes concernées sont minimisés.

Autorisation. L'autorisation de communiquer le Renseignement est accordée par le responsable de la protection des Renseignements du MSSS.

Minimisation des Renseignements communiqués*.* Seuls les Renseignements strictement nécessaires à la réalisation de l'objectif poursuivi seront communiqués. S'il est possible d'utiliser ou de communiquer un tel Renseignement sous une forme ne permettant pas d'identifier directement la personne concernée, l'utilisation ou la communication doit se faire sous cette forme (p. ex*. : utiliser un code d'identification unique plutôt que les noms ou prénoms de la personne concernée*).

Format de la communication*.* La communication sera effectuée de manière à protéger au maximum l'anonymat de la personne concernée. Le responsable de la protection des Renseignements du MSSS peut donner des instructions pour assurer la protection des Renseignements lors de leur transmission.

6.2. Registre des communications

Note informative :

Le maintien du registre des communications est une obligation transitoire qui incombe au MSSS pour la période entre le 1er juillet 2024 et la date d'entrée en vigueur de l'article 103 de la LRSSS (qui est encore inconnue), le tout, conformément à l'article 265 de la LRSSS.

Responsable du maintien du registre. Le responsable de la protection des Renseignements du MSSS met en place un registre de communication, et doit y inscrire toute communication des Renseignements détenus par le MSSS, sauf une communication à la personne concernée ou à certaines personnes lui étant liées.

Informations requises. Chaque gestionnaire doit envoyer les informations suivantes pour chaque communication d'un Renseignement détenu par le MSSS à l'adresse msss.loirenseignement@msss.gouv.qc.ca afin qu'elles soient inscrites au registre des communications :

- La nature ou le type de Renseignement concerné (p. ex. : *un diagnostic médical, un résultat d'examen médical, une note médicale*).
- La personne ou le groupement ayant reçu la communication.
- La finalité et la justification de cette communication.
- La date et l'heure de la communication.
- L'identité de la personne qui a communiqué le Renseignement au nom du MSSS.

Utilisation du registre dans le MSSS. Le registre peut être consulté par toute personne visée par une catégorie prévue à l'Annexe A, à condition que le registre soit nécessaire à l'exercice de leurs fonctions.

6.3. Conditions et modalités applicables aux cas de communications nécessaires à des fins de sécurité publique ou de poursuite pour une infraction

6.3.1. Communication en cas de risque sérieux de mort ou de blessures graves[7]

Situation visée. Le MSSS peut communiquer un Renseignement qu'il détient sans le consentement des personnes concernées lorsqu'il existe un motif raisonnable de croire

[7] Article 74 de la LRSSS.

qu'un risque sérieux de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable et que la nature de la menace inspire un sentiment d'urgence.

Conditions de la communication. Pour qu'une telle communication soit légale, les conditions suivantes doivent être satisfaites :

Condition no. 1 : L'existence d'un risque sérieux de mort ou de blessures graves

La menace doit être claire et sérieuse, de manière à mettre en évidence la possibilité objective de la survenance d'un décès ou de blessures graves, y compris une disparition, un acte de violence, une tentative de suicide ou d'autres types de menace de même nature. Le concept de « blessures graves » vise autant les atteintes physiques que psychologiques qui sont de nature à nuire de manière importante à l'intégrité physique, à la santé ou au bien-être.

Ainsi, une personne raisonnable placée dans la même situation devrait elle aussi conclure à l'existence d'un risque sérieux. Inversement, l'existence de simples soupçons ou d'une crainte subjective est insuffisante.

Condition no. 2 : La menace doit viser une personne ou un groupe de personnes en particulier

La communication doit être faite en vue de protéger une personne ou un groupe de personnes spécifiques et identifiables d'un danger qui les menace. Inversement, la communication ne serait pas autorisée si l'identification de la personne ou du groupe de personnes menacées n'est pas possible, ou n'est pas assez précise.

Condition no. 3 : La menace doit avoir un caractère urgent

La nature de la menace doit susciter un sentiment d'urgence en raison, par exemple, de la gravité de la situation, de son sérieux ou des conséquences potentielles pour la ou les personnes concernées.

Modalités de communication. La communication est permise conformément aux modalités suivantes :

Procédure : évaluation préalable et autorisation

1) Une évaluation préalable de la situation doit être réalisée par tout membre du personnel qui reçoit une demande de communication pour ce motif afin d'assurer que les conditions de la communication sont satisfaites.
2) Si l'évaluation préalable démontre que la situation remplit les conditions pertinentes, le membre du personnel doit en aviser son gestionnaire immédiat.
3) Le gestionnaire peut autoriser la communication s'il est d'avis que les conditions sont effectivement satisfaites.
4) Le gestionnaire en informe ensuite le responsable de la protection des Renseignements du MSSS dans les meilleurs délais.

Étendue des Renseignements communiqués. Seuls les Renseignements nécessaires et pertinents à la prévention de la menace identifiée peuvent être communiqués. L'étendue de la communication doit être proportionnelle à la gravité de la menace.

Destinataires autorisés :

- La ou les personnes exposées à la menace.
- Leur représentant.
- Toute personne ou tout organisme pouvant leur porter secours, notamment les services d'urgence (p. ex. : *police, pompiers, ambulanciers*) ou les professionnels de la santé et des services sociaux intervenant dans la situation.

Documentation et suivi. Le responsable de la protection des Renseignements du MSSS doit inscrire la communication dans le registre des communications visé à la section 6.2 afin d'assurer la traçabilité des Renseignements communiqués et le respect des obligations légales du MSSS.

Immunité de poursuite. Ni le MSSS ni les membres du personnel d'un organisme impliqués dans la communication ne peuvent être poursuivis en justice pour avoir communiqué de bonne foi un Renseignement en vue de protéger une personne ou un groupe.

6.3.2. Communication nécessaire à la poursuite d'une infraction[8]

Situation visée. Le MSSS peut communiquer un Renseignement sans le consentement des personnes concernées, lorsque le Renseignement est **nécessaire** aux fins d'une poursuite pour une infraction à une loi applicable au Québec.

Conditions de la communication. La communication peut être effectuée dans les cas et aux conditions suivantes :

- À la suite d'une demande officielle émanant du Directeur des poursuites criminelles et pénales (DPCP), lorsque les Renseignements sont nécessaires aux fins de la poursuite d'une infraction à une loi applicable au Québec.

- À la suite d'une demande d'une personne ou d'un groupement habilité par la loi à prévenir, détecter ou réprimer les crimes ou les infractions aux lois (p. ex. : un corps de police), et qui en fait la demande dans le cadre de l'exercice de ses fonctions.

- À l'initiative du MSSS lorsqu'il constate la commission d'un crime ou d'une infraction à une loi applicable au Québec et que les Renseignements sont nécessaires aux fins de la poursuite de ce crime ou de cette infraction (p. ex. : dans le cas où un membre du personnel du MSSS est victime d'un acte criminel dans le cadre de l'exercice de ses fonctions et que les Renseignements détenus par le MSSS sont nécessaires à la dénonciation du crime).

[8] Article 75 de la LRSSS.

Dans tous les cas, il appartient à l'organisme qui en fait la demande (soit le DPCP ou une autre autorité compétente) de s'assurer que la communication est conforme au droit applicable. Cela signifie que les règles relatives à la preuve continuent de s'appliquer à une telle communication et qu'un mandat de perquisition pourrait être requis.

Modalités de communication. La communication des Renseignements peut être effectuée dans le respect des modalités suivantes :

Procédure : évaluation préalable et autorisation

Dans le cas d'une demande du DPCP ou d'une autorité compétente

1) Le membre du personnel du MSSS qui reçoit la demande doit procéder à une évaluation préalable afin de vérifier que les conditions applicables à cette communication sont satisfaites.
2) Si l'évaluation préalable démontre que la situation rencontre les conditions pertinentes, le membre du personnel doit en aviser son gestionnaire immédiat ainsi que le responsable de la protection des Renseignements du MSSS.
3) Le responsable de la protection des Renseignements du MSSS doit s'assurer de la validité de la demande ainsi que de la nécessité et de la pertinence des Renseignements visés.
4) À la suite de son analyse, le responsable de la protection des Renseignements du MSSS confirme le bien-fondé de la demande à la direction concernée au sein du MSSS.
5) La direction concernée procède à la communication des Renseignements selon les paramètres de la demande du DPCP ou de l'autorité compétente, et en fonction des instructions du responsable de la protection des Renseignements du MSSS, le cas échéant.

Dans le cas de communication à l'initiative du MSSS

1) Tout membre du personnel du MSSS qui constate la commission d'un crime ou d'une infraction à une loi applicable au Québec doit procéder à une évaluation préalable pour s'assurer que les conditions pertinentes à la communication sont satisfaites.
2) Si l'évaluation préalable démontre que la situation rencontre les conditions pertinentes, le membre du personnel doit en aviser son gestionnaire immédiat ainsi que le responsable de la protection des Renseignements du MSSS.
3) Le responsable de la protection des Renseignements du MSSS doit
   - procéder à une évaluation interne pour confirmer que la situation répond effectivement aux conditions pertinentes;
   - déterminer, le cas échéant, l'étendue des Renseignements à communiquer afin d'assurer que la communication soit proportionnelle à la gravité du crime ou de l'infraction constatée;
   - imposer, le cas échéant, toutes les conditions pertinentes à la transmission des Renseignements.

Destinataires autorisés :

- les avocats du MSSS;
- le DPCP;
- une personne ou un organisme habilité par la loi à prévenir, détecter ou réprimer le crime ou les infractions aux lois.

Documentation et suivi. Le responsable de la protection des Renseignements du MSSS doit inscrire la communication dans le registre visé à la section 6.2 afin d'assurer la traçabilité des Renseignements communiqués et le respect des obligations légales du MSSS.

6.3.3. Communication nécessaire à une intervention policière[9] : NON-APPLICABLE

Note informative :

Le MSSS ne fait pas d'intervention adaptée ni ne fournit des services de santé et des services sociaux aux usagers.

7. DESTRUCTION ET ANONYMISATION D'UN RENSEIGNEMENT

Le MSSS ne peut conserver un Renseignement qu'il détient au-delà de la durée nécessaire à la réalisation des fins pour lesquelles il l'a recueilli ou utilisé, sous réserve d'un règlement pris en vertu du deuxième alinéa, de la Loi sur les archives[10] ou du Code des professions[11].

Pour assurer le respect de cette obligation, tout membre du personnel du MSSS qui détient un Renseignement dans ses fichiers doit le détruire ou l'anonymiser de la manière prévue aux sous-sections suivantes lorsque les fins pour lesquelles il détenait ou utilisait le Renseignement ont été accomplies.

7.1. Destruction

À l'expiration du délai prévu au calendrier de conservation pour un Renseignement[12], tout membre du personnel qui détient ce Renseignement doit déterminer si les fins pour lesquelles il détenait ou utilisait ce Renseignement ont été accomplies.

Si les fins n'ont pas été accomplies, il en informe son gestionnaire qui doit s'adresser au Directeur de la Direction de la valorisation et protection des données pour évaluer si une modification du délai prévu au calendrier de conservation pour ce Renseignement doit être faite.

[9] Article 76 de la LRSSS.
[10] RLRQ, chapitre A-21.1.
[11] RLRQ, chapitre C-26.
[12] Calendrier de conservation des documents - Documentation de l'intranet ministériel - MSSS.

Si les fins ont été accomplies, tout membre du personnel qui détient ce Renseignement dans ses fichiers doit :

- procéder à sa destruction d'une manière sécuritaire qui soit adaptée au degré de sensibilité du Renseignement et appropriée à son support (p. ex. : *support papier, électronique, etc.)* ou, à défaut, à son anonymisation de la manière prévue à la sous-section .2;
- conserver, dans ses fichiers, une preuve de la destruction et fournir cette preuve à son gestionnaire sur demande;
- consulter son gestionnaire ou le responsable de la protection des Renseignements du MSSS pour toutes questions relatives à la destruction ou l'anonymisation des Renseignements auxquels il a accès.

7.1.1. Modalités de la destruction selon le support du document

Renseignement sur papier. Tout membre du personnel doit obligatoirement procéder à la destruction du document qui comporte des Renseignements au moyen d'un bac de destruction sécuritaire. Un tel document ne peut, sous aucune considération, être déposé aux poubelles ou au recyclage ou autrement.

Lorsque le volume des documents à détruire est important et qu'ils ne peuvent être déchiquetés sur place, ils doivent être pris en charge par le Service de la gestion documentaire de la Direction de la valorisation et protection des données. Ce service prendra alors les dispositions appropriées pour les faire détruire dans un point central ou les confier à une entreprise de récupération munie d'équipements adaptés à la destruction de documents.

Dans ce dernier cas, le MSSS doit conclure avec cette entreprise un contrat de services à cette fin, dont le contenu obligatoire est prescrit à l'article 13 du Règlement sur la gouvernance des renseignements de santé et de services sociaux[13].

Renseignement sur un support électronique (p. ex. : dans le J). Les modalités de destruction applicables sont celles reconnues par le Sous-ministériat des services à l'organisation. Des outils logiciels comme *TreeSize* sont à privilégier pour analyser l'espace disque sur ordinateur et déterminer quels Renseignements occupent le plus de place sur un disque dur.

La présente sous-section ne s'applique pas aux Renseignements contenus dans les banques de données du MSSS. Seuls les pilotes et gestionnaires de ces banques de données peuvent modifier ou supprimer des Renseignements contenus dans les banques de données.

[13] RLRQ, chapitre R-22.1, r. 2.

7.2. Anonymisation

Le processus d'anonymisation constitue une alternative à la destruction des renseignements qui est reconnue et encadrée par la LRSSS et par le Règlement sur l'anonymisation des renseignements personnels[14] pris en application de l'article 73 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[15].

Cette loi prévoit qu'un renseignement est *« anonymisé »* lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances que ce renseignement ne permet plus, de façon irréversible, d'identifier, même indirectement, la personne qu'il concerne.

Toute direction du MSSS qui souhaite procéder à l'anonymisation de Renseignements comme alternative à la destruction doit s'adresser, au préalable, au responsable de la protection des Renseignements du MSSS.

8. JOURNALISATION

Droit à l'information des communications. Toute personne a droit d'être informée si des Renseignements la concernant, qui sont détenus par le MSSS, sont communiqués à d'autres personnes ou organismes.

Modalité d'exercice du droit à l'information des communications. Toute personne peut introduire une demande au responsable de la protection des Renseignements du MSSS pour obtenir de l'information relative aux communications dont ses Renseignements ont fait l'objet.

Note informative

Pour la période entre le 1er juillet 2024 et la date d'entrée en vigueur de l'article 103 de la LRSSS (qui est encore inconnue), le droit à l'information des communications s'exerce par la consultation du registre des communications visé à la section 6.2 de la présente politique, conformément à l'article 265 de la LRSSS.

9. MESURES DE SÉCURITÉ

Le MSSS a mis en place des mesures de sécurité pour protéger les Renseignements. Ces mesures incluent notamment :

- Le contrôle et la surveillance des accès aux Renseignements.
- La mise en place de mesures de sécurité physiques et électroniques.
- La formation du personnel sur la protection des Renseignements

[14] RLRQ, chapitre A-2.1, r. 0.1.
[15] RLRQ, chapitre A-2.1.

Analyses et révisions

9.1. Analyse annuelle des catégories de personnes

Au moins une fois par année, le Comité sur la gouvernance des Renseignements du MSSS doit, à la réception d'une analyse produite à cet effet, s'assurer de la pertinence des catégories de personnes identifiées à la politique de gouvernance (Annexe A) et, le cas échéant, réviser celles-ci. Pour ce faire, le Comité s'appuie sur une revue des activités de traitement, des consultations avec les unités opérationnelles et une analyse des risques. Un rapport détaillé est produit à l'issue de chaque analyse.

9.2. Évaluation des mécanismes de journalisation et des mesures de sécurité

Au moins une fois par année, le Comité sur la gouvernance des Renseignements du MSSS doit, à la réception d'une analyse produite à cet effet, évaluer la conformité des mécanismes de journalisation et l'efficacité des mesures de sécurité propres à assurer la protection des Renseignements détenus et mis en place au MSSS et, le cas échéant, revoir ces mécanismes et ces mesures. Pour réaliser cette évaluation, le Comité examine les incidents de sécurité et se réfère aux meilleures pratiques. Un rapport détaillé est produit à l'issue de chaque évaluation.

9.3. Analyse mensuelle des accès

Le Comité sur la gouvernance des Renseignements du MSSS doit analyser, sur une base mensuelle, les accès aux Renseignements du MSSS ainsi que toute autre utilisation ou communications de ceux-ci. Cette analyse vise notamment à détecter les situations qui ne sont pas conformes aux normes applicables et, le cas échéant, à permettre la prise de mesures appropriées. Un rapport détaillé est produit à l'issue de chaque analyse.

10. ÉVALUATION DES PST

Le MSSS a mis en place un calendrier de gestion des PST[16] visant à assurer la continuité des opérations et à minimiser les risques liés à l'obsolescence ou à l'interruption de services technologiques. Ce calendrier, annexé à la présente politique, contient pour chaque PST :

- Le nom du PST.
- La date de cessation de la conformité du PST avec l'usage auquel il est destiné **ou** la date à laquelle cesse la prestation d'un PST que le MSSS utilise.
- Les prochaines actions prévues pour le PST, telles que les mises à jour, les migrations ou le remplacement.

Le Directeur général des ressources informationnelles tient et doit s'assurer de la mise à jour du calendrier de gestion des PST.

[16] Se référer à l'Annexe B.

11. REGISTRE DES CONSENTEMENTS

Le MSSS doit conserver une preuve de tout consentement qu'il reçoit conformément à l'article 6 de la LRSSS. Les preuves de consentement doivent être conservées dans un registre du MSSS.

Maintien du registre. Le responsable de la protection des Renseignements du MSSS est responsable de la mise en place et du maintien du registre des consentements.

Contenu du registre. Le registre des consentements comprend au minimum les informations suivantes pour chaque consentement :

- Identité de la personne concernée, soit le nom, le prénom et la date de naissance.

- Date et mode d'obtention du consentement, soit la date et l'heure de l'obtention du consentement, la forme du consentement obtenu (écrit, verbal, électronique), la preuve de consentement, et la référence aux documents associés, c'est-à-dire toute documentation pertinente (p. ex : formulaire de consentement, correspondance, etc.).

- Portée du consentement, dont la description détaillée et précise des fins pour lesquelles le consentement a été donné, y compris les restrictions éventuelles (p. ex. : *accès limité à certains intervenants, exclusion de certaines thématiques de recherche*).

- Modalités de retrait du consentement, telles que l'indication selon laquelle la personne a été informée de la procédure à suivre pour retirer son consentement.

- Identité de la personne ayant obtenu le consentement, c'est-à-dire le nom et la fonction de la personne ayant recueilli le consentement.

- Indication selon laquelle le consentement a été donné par un tiers, les motifs justifiant cette délégation et les informations relatives à l'identité de la personne ayant donné le consentement, soit le nom, le prénom et le lien avec la personne concernée.

12. PROCESSUS DE TRAITEMENT DES PLAINTES

Note informative
Il est à noter que ce processus de traitement des plaintes est applicable lorsqu'il s'agit de renseignements de santé et de services sociaux au sens de la LRSSS, mais aussi lorsque les renseignements concernés sont des renseignements personnels au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[17].

La personne concernée, son représentant autorisé, son représentant légal ou toute autre personne qui démontre un intérêt particulier pour une personne au sujet de laquelle le MSSS détient des Renseignements peut formuler une plainte selon le processus exposé ci-bas.

[17] RLRQ, chapitre A-2.1.

La plainte peut concerner l'un des sujets suivants :

a) l'accessibilité des registres du MSSS;
b) les relations avec le personnel du MSSS;
c) la conservation hors délais de Renseignements ou la destruction hâtive;
d) la collecte ou la communication de Renseignements non nécessaires;
e) la divulgation non autorisée d'un Renseignement;
f) l'utilisation d'un Renseignement sans le consentement requis;
g) l'obtention d'un consentement non conforme;
h) les autres types de plaintes concernant la protection des Renseignements.

12.1. Transmission de la plainte

Toute plainte doit être adressée au responsable de la protection des Renseignements du MSSS.

La plainte doit être produite par écrit, à l'aide de l'un des moyens suivants :

- par le formulaire « Déclaration d'une plainte PRP[18] »;
- par courriel au ***msss_incident_prp@msss.gouv.qc.ca***;
- par la poste à l'adresse suivante :
  Sous-ministériat à la performance
  Plainte protection des renseignements personnels
  930 chemin Sainte-Foy, 4e étage, Québec

La plainte doit minimalement contenir les informations suivantes :

- le nom et le prénom du plaignant ainsi que ceux de son représentant, le cas échéant;
- les coordonnées du plaignant et de son représentant, le cas échéant (courriel ou adresse postale, numéro de téléphone);
- le type de plainte;
- la date du ou des évènements;
- le détail de l'évènement;
- le moyen de communication privilégié pour assurer le suivi de la plainte (courriel, poste).

La date de réception de la plainte est consignée au dossier.

Un accusé de réception de la plainte est transmis au plaignant ou à son représentant avec le numéro de dossier interne.

[18] Formulaire en cours de développement au MSSS. Disponible prochainement.

12.2 Évaluation de la plainte

Recevabilité de la plainte

L'équipe responsable du traitement des plaintes procède à une préanalyse de celle-ci, dès sa réception. Un avis de recevabilité est transmis au plaignant ou à son représentant, selon le mode de communication préalablement identifié par le plaignant. L'avis de recevabilité inclut toute demande d'information manquante au traitement de la plainte.

Si la plainte s'avère frivole, vexatoire ou faite de mauvaise foi, elle doit être rejetée. Une lettre de non-recevabilité de la plainte est transmise au plaignant selon le mode de communication préalablement identifié par le plaignant. Il est à noter que la lettre de non-recevabilité comporte une description des motifs à son soutien et des modalités de contestation qui sont offerts au plaignant.

Le traitement de la plainte

À la suite de la confirmation de la recevabilité de la plainte, le conseiller responsable du dossier de plainte procède à l'analyse de la plainte ainsi que de toute documentation transmise à son soutien. Il fait les vérifications requises auprès des directions, des employés du MSSS et de toute autre personne concernée par l'évènement à l'origine de la plainte, et peut obtenir tous les documents ou Renseignements nécessaires à son analyse.

À la fin de l'analyse, le conseiller transmet au Responsable de la protection des renseignements du MSSS une ébauche de lettre de réponse et des suggestions d'actions à poser pour remédier à la situation énoncée dans la plainte.

12.3 Dénouement de la plainte

La réponse à la plainte

Le responsable de la protection des renseignements du MSSS analyse et approuve, avec ou sans modifications, le projet de lettre de réponse à la plainte et les suggestions d'actions à poser pour remédier à la situation concernée par la plainte.

La lettre de réponse est transmise au plaignant ou à son représentant, selon le mode de communication préalablement identifié par le plaignant.

L'analyse interne de l'évènement concerné par la plainte et les pistes d'amélioration à mettre en œuvre

Chaque plainte est portée devant le comité sur l'accès, la protection et la sécurité de l'information du MSSS. Lors d'une séance de ce comité, un sommaire de chaque plainte recevable ainsi que son dénouement est exposé. Le comité prend connaissance des suggestions d'actions qui ont été identifiées lors du processus de traitement de la plainte afin

d'évaluer comment elles peuvent être mises en œuvre pour diminuer les risques qu'un évènement de même nature ne se reproduise.

Le comité s'assure de la confidentialité et de la protection des Renseignements relatifs aux personnes concernées dans le cadre de ses travaux.

12.4 Contestation

Toute décision relative à une plainte est contestable soit auprès du Protecteur du citoyen ou de la Commission d'accès à l'information, selon le cas. Les coordonnées des deux organismes sont transmises au plaignant ou à son représentant lors de l'émission de la lettre de non-recevabilité ou de la lettre de réponse.

12.5. Les délais de traitement de la plainte

Accusé de réception : Un accusé de réception est transmis dans un délai de 5 jour ouvrable suivant la date de réception de la plainte.

Avis de recevabilité : Un avis de recevabilité de la plainte est transmis dans un délai de 10 jour ouvrable suivant la date de l'accusé de réception.

Lettre de réponse : Les lettres de réponse relatives aux plaintes recevables sont transmises dans un délai de 30 jours ouvrables suivant la date de l'avis de recevabilité de la plainte.

12.6 Délais de conservation

Le délai de conservation des Renseignements relatifs au traitement de la plainte est défini au calendrier de conservation du MSSS[19].

12.7 Le registre des plaintes

Un registre des plaintes est tenu par le responsable de la protection des renseignements du MSSS.

Le registre contient les informations suivantes pour chaque plainte soumise conformément au présent processus :

- La date de réception de la plainte.
- La nature de la plainte.
- La recevabilité et la décision.
- La date de la transmission de la lettre de réponse.
- Les délais de traitement du dossier de plainte.

[19] Calendrier de conservation des documents - Documentation de l'intranet ministériel - MSSS

13. PROCESSUS DE TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

Le processus de traitement des incidents de confidentialité à suivre est celui établi dans la *Politique de gestion des incidents de confidentialité* du MSSS[20]. La présente section est une reprise de cette politique.

La législation

Les articles 63.8 à 63.11 de la LAI, ainsi que les articles 108 à 110 de la LRSSS encadrent les incidents de confidentialité au sein des organismes publics. Leurs règlements déterminent la marche à suivre lorsqu'un tel incident survient. Il est important de noter que la Commission d'accès à l'information du Québec (CAI) doit être avisée dans les plus brefs délais lorsqu'un incident présente un risque de préjudice sérieux pour les personnes concernées. Ces dernières doivent aussi être avisées, sauf dans certaines circonstances prévues expressément par la loi.

Identification d'un incident de confidentialité

Aussitôt qu'un évènement lui est rapporté, le gestionnaire de l'unité administrative détermine s'il s'agit d'un incident de confidentialité. Un outil d'aide à la détermination si un évènement constitue un incident de confidentialité est présenté à l'Annexe D de la *Politique de gestion des incidents de confidentialité* du MSSS.

Pour qu'il y ait un incident de confidentialité, les deux conditions suivantes doivent s'appliquer obligatoirement :

1. Les renseignements qui font l'objet de l'incident sont des renseignements personnels ou de santé.

2. Ces renseignements personnels ou de santé ont fait l'objet soit :

a) d'un accès non autorisé;

b) d'une communication non autorisée;

c) d'une utilisation à des fins non autorisées;

d) d'une perte ou d'un vol dans des circonstances faisant suite à l'une ou l'autre des circonstances prévues aux paragraphes précédents.

Le signalement d'un incident de confidentialité

Un signalement doit être fait à la fois au gestionnaire de l'unité administrative et au responsable de la protection des renseignements personnels. Cette obligation s'applique à tout membre du personnel ou à tout tiers – y compris un fournisseur, un partenaire ou un consultant externe – auxquels le MSSS communique des renseignements personnels ou de santé, lorsqu'il y a un motif

[20] Politique en cours de développement au MSSS. Accessible prochainement.

raisonnable de croire qu'un incident de confidentialité impliquant un renseignement personnel ou de santé s'est produit.

Dès la réception du signalement, le gestionnaire de l'unité administrative doit, dans le cas où cela s'avèrerait possible, prendre les mesures adéquates pour contenir l'incident et limiter les dommages qui sont ou pourront être causés par l'incident.

La déclaration d'un incident de confidentialité

Le gestionnaire de l'unité administrative ou toute personne déclarante, remplit le formulaire de Déclaration d'un incident de confidentialité et le transmet au responsable de la protection des renseignements personnels à l'adresse courriel suivante : MSSS_incident_PRP@msss.gouv.qc.ca.

Dans le cas où certaines informations demandées ne seraient pas immédiatement disponibles et qu'elles ne sont pas indispensables pour traiter rapidement l'incident, elles peuvent être transmises ultérieurement, en avisant qu'il y a des informations supplémentaires à venir.

La collecte d'informations pertinentes

Le gestionnaire de l'unité administrative, avec la collaboration de l'équipe de protection des renseignements personnels, doit collecter les informations suivantes :

i. Le nom de la personne responsable de superviser la correction de l'incident.

ii. L'identification des renseignements qui ont été compromis.

iii. La nature et le détail entourant l'incident.

iv. Les contrats ou les ententes conclus avec des tiers, le cas échéant.

La nomination d'une personne responsable de superviser l'opération pour remédier à l'incident est primordiale. Cette personne fera le lien entre sa direction, les autres directions et l'équipe dédiée aux incidents de confidentialité de la Direction de la valorisation et protection des données (DVPD). Cette personne devra être disponible pour répondre aux diverses questions se rapportant à l'incident de confidentialité.

Une bonne connaissance de la nature de l'incident ainsi que du détail des circonstances l'entourant est essentielle et facilitera d'autant mieux l'identification des mesures de correction et de mitigation qui devront être prises. En plus d'identifier les détails de l'incident, il est crucial de déterminer s'il est toujours en cours ou s'il est définitivement interrompu. Dans bien des cas, l'apport provenant d'autres directions sera nécessaire.

Les contrats ou les ententes conclus avec des tiers permettront de statuer sur la propriété de l'actif concerné et celle des renseignements compromis. De plus, dans le cas d'un acte de malveillance, ils identifieront le statut d'emploi (contractuelle ou ministériel) de la personne ayant commis la violation de confidentialité. Dans tous les cas, la validité de l'entente ou du contrat doit être confirmée.

À la suite de la collecte des informations, le gestionnaire de l'unité administrative doit mettre à jour la Déclaration d'un incident de confidentialité.

Évaluation préliminaire du risque

L'unité administrative doit faire une première évaluation du risque à la vie privée, avec le soutien de l'équipe de la protection des renseignements personnels (PRP). Pour faire cette évaluation, il doit prendre en compte le niveau du préjudice et la probabilité d'occurrence du préjudice. Plus les renseignements personnels ou de santé sont sensibles ou confidentiels, plus le risque est potentiellement sérieux.

Pour faire une évaluation de la gravité du risque et du caractère sérieux de l'incident, on doit déterminer les éléments suivants :

1. La gravité des conséquences négatives ;
2. L'exposition éventuelle du public à ces conséquences négatives ;
3. La probabilité d'occurrence et ses conséquences négatives.

Voir l'outil d'aide à l'évaluation du risque à la vie privée en cas d'incident de confidentialité à l'annexe F de la *Politique de gestion des incidents de confidentialité* du MSSS.

Cette première évaluation contribuera à l'évaluation finale du risque qui sera réalisé par l'équipe de la protection des renseignements personnels de la DVPD.

Notion de risque à la vie et de risque relatif à la vie privée

Un risque consiste en une menace éventuelle ou concrète. Un risque à la vie privée consiste en une situation qui peut ou pourrait causer une perte ou un préjudice à une personne, et qui ne pourrait pas respecter ainsi son intimité ou sa vie personnelle.

Les principaux éléments constituant le domaine de la vie privée sont, notamment :

- L'origine de la personne.
- L'intimité du foyer.
- L'état de santé.
- L'anatomie et l'intimité corporelle.
- La vie conjugale et amoureuse.
- Les opinions politiques, philosophiques ou religieuses.

Une perte ou un préjudice n'est pas obligatoirement tangible. Les effets de l'atteinte à la vie privée peuvent être manifestes et externes ou être ressentis par un sentiment intérieur chez la personne concernée ou son entourage.

Actions correctives et préventives

Les actions correctives ou préventives doivent être prises dès que possible par le gestionnaire de l'unité administrative. Cela étant dit, il devra, en collaboration avec la PRP, solliciter d'autres directions du MSSS afin d'obtenir leur appui.

Les directions des technologies de l'information et des ressources humaines sont deux directions les plus interpelées à cette étape. En collaboration avec ses directions, le gestionnaire de l'unité administrative doit :

i. Appliquer les mesures correctives qui s'imposent afin de cesser l'incident.

ii. Adopter les mesures préventives qui lui paraissent appropriées afin d'éviter qu'un tel incident ne se reproduise, et ce, après les avoir validées auprès de l'équipe de protection des renseignements personnels.

L'application des mesures correctives devra se faire le plus rapidement possible. Si elles ne peuvent être appliquées dans les meilleurs délais, une solution alternative transitoire assurant la cessation de l'incident devra être identifiée.

L'identification et l'adoption de mesures préventives pour éviter qu'un autre incident du même genre se reproduise doivent aussi avoir lieu. Cependant, bien qu'elles puissent être mises en œuvre ultérieurement, ces mesures doivent l'être dans un très court délai après l'incident.

Tous ces moyens de gestion immédiats et futurs de l'évènement doivent être mentionnés dans la déclaration initiale de l'incident ou lors d'une mise à jour de celle-ci.

Validation de l'incident par l'équipe de protection des renseignements personnels de la DPVD

L'équipe de protection des renseignements personnels est chargée d'accompagner la direction déclarante et d'analyser les informations fournies au formulaire de Déclaration d'un incident de confidentialité, dans le but de :

i. vérifier et confirmer que l'incident de confidentialité est imputable au MSSS;

ii. s'assurer que les mesures correctrices et préventives prises ou prévues sont adéquates, et fournir des instructions pour y remédier;

iii. collaborer avec la Direction générale des ressources informationnelles (DGRI) ou toute autre direction qu'elle juge utile;

iv. déterminer la nature du préjudice causé par l'incident et décider de sa gravité;

v. transmettre à la CAI le formulaire de Déclaration d'un incident de confidentialité, le cas échéant;

vi. consigner l'incident au Registre des incidents de confidentialité.

Lors de l'analyse des informations fournies au formulaire de Déclaration d'un incident de confidentialité, les professionnels attitrés aux incidents de confidentialité de l'équipe de protection des renseignements personnels vérifient et valident la description ainsi que les particularités de l'incident soumises en incluant les mesures correctrices et l'analyse du préjudice, le tout en collaboration avec d'autres directions du MSSS.

Lorsque le préjudice est sérieux, le responsable de la protection des renseignements personnels transmet le formulaire de Déclaration d'un incident de confidentialité complété par l'unité administrative déclarante et le responsable de la protection des renseignements personnels du MSSS à la CAI.

Le registre des incidents de confidentialité est rempli pour tout incident de confidentialité déclaré, qu'il ait un préjudice sérieux ou non. Ce registre est obligatoire par la loi (art. 63.11 LAI et art. 110 LRSSS).

Évaluation du risque

Lorsque l'incident a été validé et qu'il est considéré comme imputable au MSSS, l'équipe de la protection des renseignements personnels doit évaluer le risque qui pèse sur la ou les personnes concernées du fait de l'incident.

À cette fin, l'équipe analyse l'évaluation préliminaire faite par l'unité administrative, pour ensuite évaluer notamment :

i. La sensibilité des renseignements concernés.

ii. Les conséquences appréhendées de leur utilisation.

iii. La probabilité qu'ils soient utilisés à des fins préjudiciables.

L'équipe de la protection des renseignements personnels détermine si la ou les personnes concernées s'exposent ou non à un risque plausible de préjudice sérieux. Pour ce faire, elle procède à une analyse de risques des facteurs de vie privée et peut utiliser l'évaluation des facteurs de risques relatifs à la vie privée (EFVP) réalisée, le cas échéant.

La notification de l'incident

En présence d'un risque plausible de préjudice sérieux. L'équipe de renseignements personnels avise de la survenance de l'incident de confidentialité ou de sécurité les personnes et entités suivantes :

<u>Avis à la Commission d'accès à l'information du Québec (CAI)</u>

L'avis à la CAI relève de la responsabilité de la Direction de la valorisation et protection des données (DVPD). Elle lui transmet les deux sections du formulaire de Déclaration d'un incident de confidentialité. De plus, à cet avis doit être jointe la copie de chacun des avis transmis à la personne concernée et, le cas échéant, l'avis public.

La DVPD transmet toute information complémentaire à la CAI.

Avis à la personne concernée

La loi exige que la personne concernée soit informée de l'incident lorsqu'elle court un risque plausible de préjudice sérieux (art. 5 du règlement de la LAI et art. 13 du règlement de la LRSSS). Cet avis doit être communiqué par tout moyen jugé adéquat : courrier, appel téléphonique, courriel ou en personne.

L'avis doit être rédigé en termes clairs pour faciliter la compréhension par les personnes concernées et une validation des coordonnées devra être effectuée.

Il existe quelques exceptions à cette règle (avis à la personne). Dans de telles circonstances, un avis public est alors émis.

De plus dans certains cas, le MSSS doit procéder à la fois par avis à la personne et par un avis public. C'est le cas, par exemple, lorsqu'il ne détient les coordonnées que d'une partie des personnes concernées. Dans cette situation, des avis à la personne seront transmis aux personnes identifiées, et un avis public sera diffusé pour celles dont les coordonnées sont inconnues.

Il est aussi prévu aux articles 63.8 LAI et 108 LRSSS que si le fait de transmettre un avis avait pour effet d'entraver une enquête menée par un organisme habilité par la loi à prévenir, détecter ou réprimer une infraction aux lois, il ne devrait pas y avoir d'avis à la personne concernée. Cependant, dès que cette condition n'existe plus, l'avis est transmis.

Avis public

L'avis public doit être fait en application des exceptions édictées aux règlements de la LAI (art. 6) et de la LRSSS (art. 14). Cet avis peut être fait par tout moyen raisonnable qui permettra à joindre la ou les personnes concernées, par exemple une publication dans un journal ou les médias sociaux, la diffusion à la radio ou à la télévision. De plus, elle doit inclure les mêmes informations que l'avis à la personne concernée.

Le règlement est exclusif pour les cas d'utilisation d'un avis public au lieu d'un avis à la personne concernée. Voici les trois exceptions :

I. Ne détiens pas les coordonnées de la personne concernée : le MSSS procède par avis public, mais il doit, si le nombre de personnes concernées est limité, faire effectuer des recherches pour retrouver les coordonnées. À noter que ces recherches doivent être documentées. Si le MSSS retrouve les coordonnées de certaines personnes, il doit transmettre des avis à ces personnes concernées.

II. Cas de difficulté excessive : il peut s'agit d'une situation où le nombre de personnes concernées est très volumineux, où les ressources humaines ou financières ne sont pas proportionnelles au risque encouru, ou encore où la transmission des avis aux personnes concernées risque de nuire au déroulement normal des activités du MSSS. Dans tous les cas, le MSSS doit en faire la preuve.

III. Un risque de préjudice accru : il s'agit de situations où cela pourrait porter atteinte à la vie privée ou à la réputation de la personne concernée. Par exemple, une autre personne de la famille va chercher le courrier et prend connaissance de l'avis.

Le MSSS pourra décider de procéder à un avis public, même lorsqu'il n'y a pas de préjudice sérieux ou que celui-ci n'est pas obligé par la loi.

Tout avis public est publié dans la section accès à l'information de la page Internet du MSSS sur Québec.ca.

Avis à d'autres autorités

Lorsque l'incident implique des personnes concernées résidant hors du Québec, il est possible qu'une autre autorité régulatrice doive être avisée de l'incident. L'équipe dédiée à la protection des renseignements personnels doit faire les validations nécessaires et procéder à cet avis, et si requis, il doit en informer la CAI.

De plus, le MSSS peut aviser toute personne ou tout organisme susceptible de diminuer le risque de préjudice sérieux, en ne lui communiquant que les renseignements personnels nécessaires à cette fin, et ce, sans le consentement de la personne concernée. Cette communication doit être enregistrée dans le registre des communications du MSSS.

En absence d'un risque plausible de préjudice sérieux. Lorsqu'il a été établi qu'il n'y a pas de risque plausible de préjudice sérieux, l'équipe responsable de la protection des renseignements personnels inscrit l'incident dans le registre à cet effet, mais il n'a pas l'obligation de faire une déclaration à la CAI, un avis à la personne concernée ou un avis public.

En revanche, il est toujours possible de procéder à un avis, s'il est jugé nécessaire pour des raisons de transparence ou de gestion. Si tel est le cas, les raisons doivent être documentées au registre et jointes à la Déclaration d'un incident de confidentialité.

Documentation sur l'incident. Le dossier ouvert par l'équipe responsable de la protection des renseignements personnels doit être à jour et bien documenté pour référence ultérieure.

Le dossier doit inclure :

- La Déclaration d'un incident de confidentialité remplie par l'unité administrative et par l'équipe.
- L'analyse du préjudice.
- La preuve de toutes les transmissions à la CAI, lorsque requis.
- Une copie de la liste des personnes concernées.
- Une copie de l'avis à la personne concernée, la date et la méthode de sa transmission, lorsque requise.
- Une copie de l'avis public, la date et la méthode de sa transmission, lorsque requise.
- Tout autre document jugé pertinent.

14. FORMATION ET SENSIBILISATION

Tous les membres du personnel du MSSS doivent être adéquatement formés en matière de protection des Renseignements. Pour ce faire, une formation intitulée *Protection des renseignements de santé et de services sociaux* est déployée à la demande du MSSS sur l'environnement numérique d'apprentissage provincial (ENA-Provincial[21]).

***Caractère obligatoire de la formation*.** La formation doit obligatoirement être suivie par tous les membres du personnel du MSSS et tous les professionnels qui y exercent leur profession, y compris les étudiants et les stagiaires, les employés en prêt de services et les contractuels, et ce, dès leur entrée en fonction au sein du MSSS.

Objectifs pédagogiques de la formation. La formation a notamment pour but de permettre aux membres du personnel de développer les compétences requises pour assurer la protection et la confidentialité des Renseignements auxquels ils ont accès ou qu'ils utilisent dans le cadre de l'exercice de leurs fonctions au sein du MSSS.

Plus spécifiquement, la formation permet au personnel de se familiariser avec les comportements adéquats à adopter et les mesures à prendre pour favoriser la protection de la vie privée. À la fin de la formation, l'apprenant sera en mesure de démontrer qu'il

- est en mesure d'identifier les renseignements de santé et de services sociaux dans son milieu de travail;
- comprend les principes essentiels et les bonnes pratiques à mettre en œuvre pour assurer la protection des Renseignements, au moment de leur collecte à leur destruction;
- effectue un usage adéquat des Renseignements auxquels il a accès dans le cadre de son travail;
- peut respecter la règlementation en vigueur;
- dispose des moyens pour assurer la disponibilité, l'intégrité et la confidentialité des Renseignements dans le cadre de son utilisation d'outils informatiques ou technologiques.

Contenu de la formation. La formation aborde les thématiques suivantes :

- La définition du concept de renseignement de santé et de services sociaux.
- Les principes généraux en matière de sécurité de l'information.
- Le critère de nécessité.
- Les principes de la collecte de Renseignements, incluant la description des droits de la personne concernée dans le cadre de la collecte.
- L'accès aux Renseignements par les intervenants qui sont des professionnels au sens du Code des professions.

[21] Il est aussi possible pour des partenaires externes de suivre cette formation à travers le site de la FCP-Partenaires.

- L'accès aux Renseignements par les intervenants qui ne sont pas des professionnels au sens du Code des professions et les conditions réglementaires applicables en la matière.
- Le droit de la personne concernée de restreindre ou de refuser l'accès à ses renseignements et les modalités d'exercice de ses droits prévus par la LRSSS.
- L'utilisation adéquate des Renseignements.
- Les règles de sécurité concernant les codes d'accès.
- Les bonnes pratiques de communication d'un Renseignement, et les modes de communication appropriés selon les supports (p. ex. : *support technologique, papier, etc*.).
- Les règles applicables en matière de conservation et de destruction des Renseignements ainsi que les bonnes pratiques qui y sont associées.

Évaluation et attestation de réussite. Au terme de cette formation, les apprenants devront remplir un questionnaire d'évaluation dont la note de passage est fixée à 70 %. Il n'y a pas de nombre maximal d'essais pour réussir cette évaluation."

De plus, les apprenants se verront délivrer une attestation de réussite à l'achèvement des différents modules de formation ainsi que du questionnaire. Ils devront conserver une preuve de la réussite de cette formation et en remettre une copie à leur gestionnaire.

La réussite de la formation et la conservation de l'attestation de réussite sont des formalités obligatoires imposées à tous les membres du personnel du MSSS et à tous les professionnels qui y exercent leur profession, y compris les étudiants et les stagiaires, les employés en prêt de services et les contractuels.

15. LE SONDAGE

Le sondage est une activité de collecte de renseignements personnels ou de renseignements de santé et services sociaux. Dans certains cas, ces renseignements peuvent être des renseignements sensibles.

La responsabilité de la gouvernance des activités de sondage incombe au responsable de la protection des renseignements personnels pour le MSSS nommé en application de l'article 8 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Au moment de l'entrée en vigueur de la présente politique, le responsable de la protection des renseignements personnels pour le MSSS est monsieur **Marc-Nicolas Kobrynsky**, sous-ministre adjoint.

15.1. Demande d'autorisation d'un projet de sondage

Tous les projets de sondage qui impliquent la collecte de Renseignements doivent être transmis au responsable de la protection des renseignements personnels du MSSS à : msss_incident_prp@msss.gouv.qc.ca.

Tous les projets de sondage transmis pour autorisation doivent inclure :

- l'invitation à participer au sondage;
- le sondage (questionnaire);
- l'outil utilisé pour la transmission du sonda

15.2. Analyse et autorisation

L'évaluation du sondage est réalisée par le responsable de la protection des renseignements personnels du MSSS. Elle comporte une évaluation en deux volets, soit les considérations éthiques soulevées par le projet de sondage et la conformité du projet en matière de protection des Renseignements concernés.

Avis éthique. Le responsable de la protection des renseignements personnels du MSSS analyse les considérations éthiques liées au projet de sondage envisagé, incluant notamment la sensibilité des Renseignements collectés, les utilisations qui en seront faites et les personnes concernées par le sondage. Cette analyse doit être conclue par la production d'un avis sur l'aspect éthique du projet de sondage envisagé.

Avis de conformité en protection des renseignements personnels. Le responsable de la protection des renseignements personnels du MSSS analyse notamment la nécessité de recourir au sondage pour atteindre les objectifs poursuivis par le MSSS, la nécessité de chaque question qui sera employée pour recueillir des Renseignements, l'utilisation projetée des renseignements recueillis, la conformité du consentement qui serait obtenu, le lieu et le délai de conservation des Renseignements et la possibilité, pour les personnes concernées, de rectifier les Renseignements. Cette analyse se conclut avec la production d'un avis de conformité en protection de renseignements personnels.

Approbation. Le responsable de la protection des renseignements personnels du MSSS prend en considération l'avis de conformité en protection de renseignements personnels et l'avis éthique pour émettre son autorisation à la collecte de renseignement via le sondage proposé.

Suivi. Chaque demande d'autorisation de sondage est portée devant le comité sur l'accès, la protection et la sécurité de l'information du MSSS. Lors d'une séance de ce comité, un sommaire de chaque sondage ainsi que des avis de conformité et d'éthique rendus à son sujet sont exposés.

15.3. Délais de conservation

Le délai de conservation des Renseignements recueillis lors d'un sondage est défini selon le calendrier de conservation du MSSS.

15.4. Registre

Un registre interne des demandes de sondages est tenu par le responsable de la protection des renseignements personnels du MSSS.

Les éléments du registre incluent :

- La date de réception.
- La nature.
- La recevabilité et la décision prise.
- La date de la transmission de l'avis de conformité.
- Le délai de traitement du dossier.

Note

Cette politique de gouvernance est un document évolutif qui sera mis à jour au besoin.

Pour obtenir plus d'information sur la protection des Renseignements au MSSS, veuillez consulter le site Web du MSSS à l'adresse suivante : https://www.msss.gouv.qc.ca/.

Pour toute question relative à cette politique ou pour obtenir des informations supplémentaires, veuillez communiquer avec :

- La Direction de la valorisation et de la protection des données en écrivant à msss.loirenseignement@msss.gouv.qc.ca.
- Le Processus de traitement des plaintes et d'incidents de confidentialité en écrivant à msss_incident_prp@msss.gouv.qc.ca.

Politique de gouvernance des renseignements

Annexe A – Catégories de personnes autorisées

Catégories de personnes autorisées à avoir accès aux Renseignements détenus par le MSSS lorsque les Renseignements sont nécessaires à l'exercice de leurs fonctions au sein du MSSS.

Commentaires préliminaires :

- Les catégories exposées ci-dessous sont évolutives et peuvent être modifiées en fonction des besoins des différentes directions qui composent le MSSS. Pour toutes questions en lien avec ces catégories, ou pour faire une demande de modification ou de mise à jour, veuillez-vous adresser au responsable de la protection des Renseignements du MSSS à l'adresse courriel suivante : msss.loirenseignement@msss.gouv.qc.ca.
- L'accès aux Renseignements par les personnes mentionnées à ces catégories demeure encadré par le critère de la nécessité; et des mesures de sécurité physiques sont mises en œuvre pour en assurer le respect.
- Le genre masculin est utilisé sans aucune discrimination et dans le seul but d'alléger le texte.

Sous-ministériat	Direction principale / Direction générale	Direction / Direction adjointe	Catégorie de Renseignements accessibles	Fonctions ou titre
Sous-ministériat adjoint de la performance	Direction principale de la performance et Direction générale du système d'information de données	Direction de la diffusion de l'information de gestion	Renseignements nécessaires et dûment autorisés à l'analyse de la performance du système de santé	Coordonnateur
				Technicien en informatique
				Pilote d'orientation
				Analyste de la diffusion de l'information
				Stagiaire
				Analyste de données
		Direction de la qualité des données	Renseignements nécessaires et dûment autorisés à l'analyse de la performance du système de santé	Coordonnateur
				Pilote d'orientation
				Conseiller en pilotage
				Technicien en gestion de données
				Conseiller technique en collecte de données
				Conseiller en qualité des données et pilotage d'orientation
				Analyste de l'information
		Direction de l'environnement informationnel	Renseignements nécessaires et dûment autorisés à l'analyse de la performance du système de santé	Analyste en intelligence d'affaires
	Direction principale de la performance et Direction générale de l'orientation de performance	Direction de l'analyse et de l'intelligence artificielle	Renseignements nécessaires et dûment autorisés à l'analyse de la performance du système de santé	Coordonnateur
				Conseiller en information de gestion
				Analyste de données
				Technicien en informatique
				Conseiller en statistique et analyste de données
				Agent de recherche, géographie
				Analyste de l'information géographique
				Conseiller en intelligence d'affaires
				Conseiller à la coordination des projets et à la gestion des ententes

				Conseiller en intelligence artificielle et valorisation de données
				Stagiaire
				Analyste de données
	Direction générale de l'évaluation des programmes	Direction de l'évaluation de programmes	Renseignements nécessaires et dûment autorisés à l'analyse de la performance du système de santé	Conseiller en évaluation
Sous-ministériat santé physique et pharmaceutique	Direction générale de la pertinence et des services spécialisés	Direction des services spécialisés et soins critiques	Renseignements en matière de santé physique et pharmaceutique	Directeur général
				Conseiller stratégique de la cohérence des services spécialisés
				Coordonnateur stratégique, soins critiques et fluidité
				Conseiller stratégique – Alternatives à l'hospitalisation
				Conseiller en pertinence clinique
				Conseiller en amélioration continue
				Conseiller stratégique – Gouvernance de la pertinence clinique transversale
				Coordonnateur stratégique de la pertinence des activités cliniques
				Directeur des services spécialisés et soins critiques
				Coordonnateur stratégique Spécialités médicales
				Conseiller Intelligence d'Affaires
				Conseiller Sciences neurologiques
				Conseiller Cardiologie
				Conseiller COVID-longue et maladie de Lyme
				Conseiller santé rénale
				Conseiller Douleur chronique
				Conseiller en Maladies rares
				Conseiller Bariatrique
				Conseiller en douleur chronique et anesthésiologie

				Conseiller en chirurgie
				Conseiller Traumatologie et conseillère Soins intensifs
		Direction des laboratoires et de l'imagerie médicale	Renseignements en matière de santé physique et pharmaceutique	Conseiller en biologie médicale
				Technicien en administration
				Conseiller en biovigilance
	Direction générale des secteurs interdisciplinaires	Direction des affaires interdisciplinaires et affaires universitaires	Renseignements en matière de santé physique et pharmaceutique	Conseiller aux affaires universitaires
				Dentiste -conseil
		Direction santé mère-enfant	Renseignements en matière de santé physique et pharmaceutique	Directeur
				Directeur national santé des femmes
				Professionnel
				Adjoint exécutif
	Direction de la cancérologie et Direction adjointe du dépistage et de la surveillance		Renseignements en matière de santé physique et pharmaceutique	Directeur adjoint (Direction cancérologie/Direction adjointe dépistage et surveillance)
				Registraire du Registre québécois de cancérologie (Direction cancérologie/Direction adjointe dépistage et surveillance)
				Gestionnaire de banques de données (Direction cancérologie/Direction adjointe dépistage et surveillance)
				Analyste de données (Direction cancérologie/Direction adjointe dépistage et surveillance)
				Conseiller impliqué dans le contrôle de la qualité des données (Direction cancérologie/Direction adjointe dépistage et surveillance)

				Conseiller impliqué dans le contrôle de la qualité des données (Direction cancérologie)
Sous-ministériat aux services sociaux, à la santé mentale et à la réadaptation	Direction générale des services sociaux, de la santé mentale et de la réadaptation	Direction des services à la jeunesse	Renseignements en matière de services sociaux, de santé mentale et de réadaptation	Directeur général
				Adjoint exécutif
				Conseiller expert
				Conseiller ressources humaines et budget
				Médecin-conseil
				Directeur
				Coordonnateur
		Direction des services à l'adulte	Renseignements en matière de services sociaux, de santé mentale et de réadaptation	Directeur
				Coordonnateur
	Direction générale des services sociaux et à la communauté	Direction des services sociaux généraux, aux dépendances et à l'itinérance	Renseignements en matière de services sociaux, de santé mentale et de réadaptation	Directeur général
				Adjoint exécutif
				Conseiller ressources humaines et budget
				Directeur
				Adjoint exécutif
		Direction des services à la communauté	Renseignements en matière de services sociaux, de santé mentale et de réadaptation	Directeur (intérim)
				Adjoint exécutif
Sous-ministériat ressources humaines et négociation	Direction générale de la main-d'œuvre en santé et services sociaux	Direction de l'analyse stratégique en main-d'œuvre	Renseignements en matière de ressources humaines et négociation Renseignements en matière de ressources humaines et négociation	Coordonnateur et responsable des systèmes d'information sur le personnel du réseau
				Analyste senior en rémunération
				Analyste en informatique
				Pilote banque R22
				Actuaire
				Conseiller en planification de la main-d'œuvre
				Coordonnateur – Gestion budgétaire et financière

				Actuaire analyste en rémunération
				Économiste analyste en rémunération
				Actuaire chef d'équipe en planification de main-d'œuvre
				Analyste en exploitation des banques de données
				Consultant actuaire analyste en rémunération
				Actuaire chef d'équipe de la Fédération des médecins omnipraticiens du Québec (FMOQ)
				Consultant en informatique décisionnelle et architecture des données
Sous-ministériat des services à l'organisation	Direction générale des ressources informationnelles	Direction des opérations des ressources informationnelles	Renseignements en matière de services à l'organisation	Conseiller ou conseillère à la qualité des services et à l'amélioration des pratiques
				Coordonnateur des portefeuilles et des projets
				Coordonnateur en technologies de l'information (TI)
				Chargé en Systèmes d'information (SI)
				Expert Power-BI
				Administrateur de base de données (Windows SQL / Oracle)
		Direction des projets et gouvernance des ressources informationnelles		Administrateur de bases de données Application
				Analyse Architecture
				Pilote de systèmes
				Conseiller en architecture de sécurité de l'information
				Analyste en sécurité de l'information
				Coordonnateur de la gouvernance Ressources informationnelles
Sous-ministériat de la prévention et santé publique	Direction principale de la santé publique et	Direction des maladies infectieuses et de la vigie sanitaire	Renseignements en matière de prévention et de santé publique	Directeur général adjoint
				Directeur
				Personne affectée à la garde de protection en semaine et garde de 2e ligne en fin de semaine

	Direction générale de la protection			Conseiller en vigie sanitaire
				Coordonnateur de l'équipe d'épidémiologie
				Médecin-conseil
				Infirmier -conseil en protection de la santé publique
				Conseiller en immunisation
				Conseiller en maladies infectieuses
				Conseiller en prévention et contrôle des infections
				Médecin-conseil
				Conseiller en prévention et contrôle des maladies infectieuses
				Technicien en administration
		Direction de la santé environnementale et au travail	Renseignements en matière de prévention et de santé publique	Médecin-conseil
				Directeur
				Coordonnateur
				Conseiller en santé environnementale
				Conseiller en santé au travail
	Direction principale de santé publique et Direction générale de la prévention et de la promotion de la santé	Direction des populations vulnérables et marginalisées	Renseignements en matière de prévention et de santé publique	Directeur général
				Conseiller en prévention des surdoses
		Direction adultes et aînés	Renseignements en matière de prévention et de santé publique	Conseiller sur la stratégie prévention du suicide (105)
				Technicien en administration
				Coordonnateur
	Direction principale de santé publique	Direction des Affaires de la Direction nationale des soins	Renseignements en matière de prévention et de santé publique	Technicien nominal en administration

		et services de première ligne (DNSP)		Technicien principal en administration
	Direction générale des politiques en santé publique	Direction de la surveillance, mesure et suivi	Renseignements en matière de prévention et de santé publique	Conseiller en surveillance de l'état de santé
				Coordonnateur responsable de la mise en œuvre du Plan national de surveillance
				Responsable de la planification et de la réalisation des enquêtes sociosanitaires
Sous-ministériat des aînés et proches aidants	Direction générale du soutien à domicile et des services aux aînés	Direction du soutien à domicile	Renseignements en matière d'aînés et de proches aidants	Conseiller en développement d'information stratégique de gestion
				Conseiller en soutien à domicile
		Direction des services aux aînés et proches aidants	Renseignements en matière d'aînés et de proches aidants	Directeur
Sous-ministériat à la Protection de la jeunesse	Direction principale de la protection de la jeunesse et secrétariat aux services internationaux à l'enfance et	Direction de la grossesse pour autrui Hors Québec	Renseignements en matière de Protection de la jeunesse	Directeur général
				Directeur
				Chef d'équipe
				Conseiller
				Conseiller en gestion organisationnelle
				Technicien
				Technicien administratif et en bureautique et documentation

	Direction générale des affaires du secrétariat aux services internationaux à l'enfant			Étudiant
				Contractuel en GPAHQ
		Direction de la recherche des origines et des retrouvailles	Renseignements en matière de Protection de la jeunesse	Directeur
				Chef d'équipe
				Conseiller
				Technicien administratif
				Étudiant
				Agent de secrétariat
		Direction de l'adoption	Renseignements en matière de Protection de la jeunesse	Directeur
				Chef d'équipe
				Conseiller
				Technicien administratif
				Étudiant
				Agent de bureau
				Agent de bureau en droit
	Direction générale des affaires du Directeur nationale de protection de la jeunesse	Direction de la planification, du développement et des mandats transversaux	Renseignements en matière de Protection de la jeunesse	Directeur
				Chef d'équipe
				Conseiller
Bureau du sous-ministre	Direction générale de la gouvernance et des affaires institutionnelles	Direction des relations et des partenariats avec les Premières Nations et les Inuit	Renseignements nécessaires et dûment autorisés aux fins d'approbations et suivis requis	Directeur général
				Directeur
				Conseiller
				Conseiller stratégique
				Conseiller aux affaires autochtones
				Professionnel
				Technicien
				Agent de secrétariat
				Adjoint exécutif

				Consultant (selon les contrats)
		Direction de l'accès à l'information et de la propriété intellectuelle	Renseignements nécessaires et dûment autorisés aux fins d'approbations et suivis requis	Directeur général
				Directeur
				Conseiller
				Conseiller en accès
				Professionnel
				Adjoint exécutif
				Technicien
				Agent de secrétariat
				Étudiant
	Direction exécutive		Renseignements nécessaires et dûment autorisés aux fins d'approbations et suivis requis	Directeur
				Conseiller stratégique
				Adjoint exécutif
				Technicien
				Agent de secrétariat
	Secrétariat général		Renseignements nécessaires et dûment autorisés aux fins d'approbations et suivis requis	Directeur
				Conseiller stratégique
				Adjoint exécutif
				Technicien
				Agent de secrétariat

Annexe B - Calendrier de mise à jour des PST du MSSS

Le présent calendrier expose les différents produits ou services technologiques utilisés au sein du MSSS, avec les informations relatives à leur mise à jour respective. Il est à noter que l'intégration des banques de données dans la DSN sera faite selon le calendrier fourni par la Vice-présidence aux technologies de l'information (VPTI).

PST utilisé	Date de cessation de conformité du PST avec l'usage auquel il est destiné ou Date de cessation de la prestation du PST utilisé par le MSSS			Action
Dossier Santé Québec (DSQ)	À déterminer		À déterminer	À déterminer
Dossier Santé numérique (DSN)	À déterminer		À déterminer	À déterminer
GESCO (Gestion du courrier)	À déterminer		À déterminer	À déterminer
Maintenance et exploitation des données pour l'étude de la clientèle hospitalière (MED-ÉCHO)	À déterminer		À déterminer	À déterminer
Solution information du Réseau de services intégrés pour les personnes adultes (RSIPA)	À déterminer		À déterminer	À déterminer
Système d'information sur la clientèle et les services des CSSS - mission CLSC (I-CLSC)	À déterminer		À déterminer	À déterminer
Banque de données communes des urgences (BDCU)	À déterminer		À déterminer	À déterminer
Système d'information Adoption Québec Internationale (ADOQI);	À déterminer		À déterminer	À déterminer
Registre des enfants signalés	À déterminer		À déterminer	À déterminer
Système d'information clientèle pour les services de réadaptation dépendances (SIC-SRD)	À déterminer		À déterminer	À déterminer
Dossier Santé numérique (DSN)	À déterminer		À déterminer	À déterminer

Système d'information pour les personnes ayant une déficience (SIPAD)	À déterminer		À déterminer	À déterminer
Compilation des données de production des laboratoires de biologie médicale (CDLAB)	À déterminer		À déterminer	À déterminer
Registre canadien sur les insuffisances et les transplantations d'organes du Québec (RCITO)	À déterminer		À déterminer	À déterminer
Registre des évènements démographique (RED)	À déterminer		À déterminer	À déterminer
Système d'information sur les mécanismes d'accès aux services spécialisés – Chirurgie (SIMASS)	À déterminer		À déterminer	À déterminer
Système d'information et de gestion des urgences (SIGDU)	À déterminer		À déterminer	À déterminer
A08 (Suivi des demandes d'accès à l'information)	À déterminer		À déterminer	À déterminer
Coût par parcours de soins et de services (CPSS)-Infogestion	À déterminer		À déterminer	À déterminer
Greffe de cellules souches (Bases de données (BD) de suivi des greffes de cellules souches)	À déterminer		À déterminer	À déterminer
J36 (Système de données du recensement)	À déterminer		À déterminer	À déterminer
L09-Centralab	À déterminer		À déterminer	À déterminer
M25 - SBF – R (Système budgétaire et financier régionalisé)	À déterminer		À déterminer	À déterminer
M34 (Référentiel territorial)	À déterminer		À déterminer	À déterminer

Radio-onco (Bases de données (BD) des traitements de radio-oncologie)	À déterminer		À déterminer	À déterminer
Registre québécois du cancer (RQC)	À déterminer		À déterminer	À déterminer
SGAS (Système de gestion de l'accès aux services)	À déterminer		À déterminer	À déterminer
SI-PQDCS (Programme québécois de dépistage du cancer du sein)	À déterminer		À déterminer	À déterminer
SIRTQ (Système d'information du Registre des traumatismes du Québec)	À déterminer		À déterminer	À déterminer
SISPUQ (Système d'information des services préhospitaliers d'urgence)	À déterminer		À déterminer	À déterminer
G76 – AMEN (Gestion des aménagements)	À déterminer		À déterminer	À déterminer
SI-GMI (Système de surveillance et de vigie sanitaire des maladies à déclaration obligatoire d'origine infectieuse)	À déterminer		À déterminer	À déterminer
Mécanisme d'accès à l'hébergement	À déterminer		À déterminer	À déterminer
REIAT (Rapport d'évènement indésirable associé à la transformation)	À déterminer		À déterminer	À déterminer
s08 (Service de la dette (gestion des emprunts))	À déterminer		À déterminer	À déterminer
SI Endo (Endoscopies)	À déterminer		À déterminer	À déterminer

Système d'information sur la sécurité des soins et des services (SISS)	À déterminer		À déterminer	À déterminer
Administration du programme de financement et de soutien professionnel (V15 – GMF)	À déterminer		À déterminer	À déterminer

Annexe C - Lois et règlements consultés

Le *Code des professions* (L.R.Q., c. C-26).

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1).

La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (L.R.Q. c. G-1.03).

La *Loi sur la santé publique* (L.R.Q., c. S-2.2).

La *Loi sur les renseignements de santé et de services sociaux* (L.R.Q., c. R-22.1).

La *Loi sur les services de santé et les services socia*ux (L.R.Q., c. S-4.2).

Le *Règlement d'application de certaines dispositions de la Loi sur les renseignements de santé et de services sociaux* (RLRQ, c. R-22.1).

Le *Règlement sur l'anonymisation des renseignements personnels* (G.O.Q. II, 2848).

Le *Règlement sur la gouvernance des renseignements de santé et de services sociaux* (RLRQ, c. R-22.1).

Documents consultés :

Ministère de la Santé et des Services sociaux, *Directive sur la destruction des documents renfermant des renseignements confidentiels*. Gouvernement du Québec. 2019.

Ministère de la Santé et des Services sociaux, *Directive sur la destruction des documents renfermant des renseignements confidentiels*. Gouvernement du Québec. 2019.

Ministère de la Santé et des Services sociaux, *Guide de classification : dépôt J.* Gouvernement du Québec. 2024.

Ministère de la Santé et des Services sociaux, *Plan de classification uniforme des documents du ministère.* Gouvernement du Québec. 2024.

Gouvernement du Québec. *Anonymisation des renseignements personnels.* Québec.ca. Consulté le 16 juin 2024. Anonymisation | Gouvernement du Québec (quebec.ca).

Politique de gouvernance des renseignements

Annexe D - Sites d'intérêt

Environnement numérique d'apprentissage : https://fcp-partenaires.ca/login/index.php

Formation continue partagée pour les partenaires de services hors réseau : https://fcp-partenaires.ca/login/index.php

Commission d'accès à l'information du Québec : https://www.cai.gouv.qc.ca/

Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité : https://www.quebec.ca/gouvernement/ministeres-organismes/institutions-democratique-acces-information-laicite

- Vous pouvez également écrire à l'adresse msss.loirenseignement@msss.gouv.qc.ca afin de faire une demande pour obtenir le guide de formation de la formation intitulée *La protection des renseignements de santé et de services sociaux.*

25-107-01W

Santé
et Services sociaux
Québec